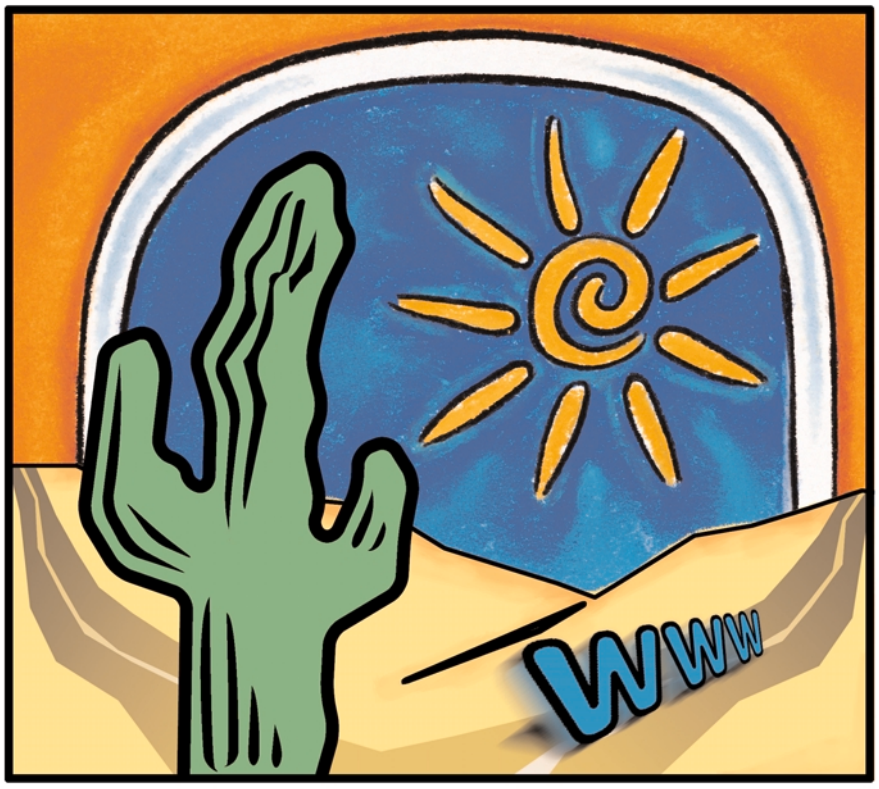
Governor's Office of Health Information Exchange

Arizona Health Information Exchange (HIE)

Appendix A

Arizona Health-*e* Connection Roadmap

April 4, 2006



"To facilitate the design and implementation of integrated statewide health data information systems that support the information needs of consumers, health plans, policymakers, providers, purchasers, and researchers and that reduce health-care costs, improve patient safety, and improve the quality and efficiency of healthcare and public health services in Arizona."

Arizona Health-e Connection Mission Statement

Arizona Health-*e* Connection Roadmap

April 4, 2006

Funded by St. Luke's Health Initiatives and BHHS Legacy Foundation

St. Luke's Health Initiatives
A Catalyst for Community Health

BHHS LEGACY FOUNDATION

With support and assistance by eHealth Initiative

eHEALTH INITIATIVE
Real Solutions, Better Health

Table of Contents

I. Executive Summary

A. Overview

Arizona recognizes that a statewide infrastructure to exchange health information electronically will improve the quality and reduce the cost of healthcare in Arizona by:

- Ensuring health information is available at the point of care for all patients
- Reducing medical errors to improve patient safety
- Avoiding duplicative medical procedures
- Improving coordination of care between hospitals, physicians, and other healthcare professionals
- Furthering healthcare research
- Enhancing public health and disease surveillance efforts
- Encouraging greater consumer participation in their personal healthcare decisions
- Enhancing the business environment for both small and large employers and reducing state expenditures by controlling healthcare costs

Through executive order, Governor Janet Napolitano requested that a wide range of interests determine a strategy to achieve a vision of 100 percent electronic health data exchange among payers, healthcare providers, consumers of healthcare, researchers, and government agencies, as appropriate. Hundreds of Arizonans representing diverse interests and geographies voluntarily contributed to the process and are enthusiastic about the possibilities of moving e-health forward. This Arizona Health-*e* Connection *Roadmap* is the result of that process.

The *Roadmap* articulates a path to improve the quality and reduce the cost of healthcare in Arizona. This path ensures that the needs of rural communities and small physician practices are accommodated.

The *Roadmap* identifies key decision points by focusing on the what, when, why and who – what action needs to occur, when the action needs to occur, why the action is necessary, and who (individual/group/organization) is required to complete the action. Many of the "how" questions are to be answered in the implementation phase and are not addressed in this *Roadmap*.

Choices identified in the *Roadmap* were considered from the perspectives of *urgency* and *feasibility*. Urgent initiatives bring relief to a problem in the healthcare system. They provide a high level of value to one or more constituent communities (such as patients, providers, and payers). Feasible initiatives include items likely to immediately succeed *as well as initiatives that are necessary prerequisites to achieve an urgent priority initiative*. Implementation of a feasible initiative does not necessarily provide a high level of standalone urgent value.

The *Roadmap* is constructed with initiatives that provide either a high level of urgent value or feasible value or both. Sequencing of the recommended initiatives was chosen to maximize impact and utility for the sum total of all initiatives. The *Roadmap* plan is designed to be scalable.

Although the *Roadmap* is a statewide plan and includes many elements of statewide coordination, some *Roadmap* initiatives will be implemented on a regional basis within the context of a medical trading area, or MTA. An MTA is usually a geographic area defined by where a population cluster receives its medical services. It is an area in which groups of physicians, hospitals, labs, and other providers work together to serve a population of consumers.

B. Health Information Technology and Health Information Exchange

The *Roadmap* advances an approach that recognizes a fundamental distinction between health information technology (HIT) and health information exchange (HIE). The combination of HIT and HIE approaches constitutes much of the *Roadmap*. This fundamental distinction simplifies the interrelationships between various components and clarifies the strategies necessary for e-health implementation.

Health information technology is a local deployment of technology to support organizational business and clinical requirements. HIT is technology implemented within the physical space of a doctor's office, laboratory, and hospital or virtually through a hospital system. Items such as electronic medical records (EMR) systems, administrative systems (such as billing), and workflow systems are examples of HIT systems.

Health information exchange is infrastructure to enable data sharing between organizations. Services are built once and used multiple times by many. Items such as a central Web site, healthcare terminology translation tools, a master patient index (MPI), authentication and authorization infrastructure, and applications to aggregate information from multiple sources are examples of HIE resources.

The Roadmap uses the following strategies for HIT and HIE. Specific recommendations presented in other sections of the Roadmap have been developed with direct consideration of these HIT and HIE strategies.

HIT *ROADMAP* STRATEGIES

- Partner with organizations already involved in HIT adoption
- Set and adopt standards (especially for integration with HIE)
- Provide guidance, direction, and education
- Provide incentives
- Identify barriers and propose solutions

HIE *ROADMAP* STRATEGIES

- Begin by developing HIE regionally
- Leverage existing information technology projects and databases
- Develop key statewide resources for data access and sharing

HIT products recognized as key include electronic medical records (EMRs), ePrescribing, and practice management systems (e.g., billing). High-priority HIE projects include a patient health summary, statewide Web portal, secure messaging and infrastructure, and a results delivery service (implemented on a regional basis).

The patient health summary has the most clinical value of all potential initiatives. It provides an assembled view of a patient's most pertinent medical characteristics, such as lab results and trends, allergies, and medications prescribed. The data, once standardized, can also serve as the basis of a personal health record. Since many patients are treated by more than one clinician, compilation of this data affords advances in safety, quality of care, continuity of care, and cost efficiency. Although the patient health summary will include continuity of care information, the *Roadmap* development team has intentionally refrained from using the term "continuity of care record (CCR)." CCR is a term recognized by many in the healthcare industry, but it is not a de facto national standard. The Arizona team found that use of the term CCR tended to confuse discussions because it means different things to different people.

The *Roadmap* makes a distinction between a "basic" patient health summary and an "enhanced" patient health summary. The basic patient health summary is envisioned as a pilot project that compiles information from several existing statewide data sources. It will provide clinical value but is limited in scope on the quantity, type, and standardization of data presented. An enhanced patient health summary is, by comparison, a more complete portrait of an individual's key clinical and administrative information. Several prerequisite activities, such as implementation of regionally based results delivery services, are necessary for realization of an enhanced patient health summary.

The regionally based results delivery service provides a standard mechanism for clinicians to request various types of clinical data (such as laboratory, radiology, etc.) and a standard mechanism for delivery of the results. It is especially important in that it will provide a stream of data to populate core infrastructure components and will also provide a sustainable revenue stream to offset many of the costs to develop and operate an e-health information exchange. Data gleaned from the results delivery service is essential to

establish items such as a directory of clinicians, a master patient index, and storage banks of "normalized" clinical data.

C. Finance

Funding for the Arizona Health-*e* Connection should be obtained from a variety of sources. The *Roadmap* recommends that different funding programs and parameters be considered for HIE, HIT, and a central coordination organization.

It is not necessary to invest large amounts of capital in a central organization to create a top-down funding structure for all Health-*e* Connection exchange activities. In fact, many projects should be funded on a case-by-case basis at an MTA level. In general, funding for the *Roadmap* should be value driven. Costs for ongoing operations should be borne by the organization(s) benefiting from the service. It follows that projects will be addressed when it makes economic sense to do so.

The central coordination organization is small and requires a modest amount of funding, estimated at $3 million to $4 million per year. Funding sources for this function could include grants and donations, state funds, in-kind donations of staff, and various transaction fees.

Regional HIE efforts will require start-up funding of about $1.5 million to $3 million per one million people (population) over the first two years. Like the central coordination organization, potential sources of funding include grants and donations, state funds, and in-kind donations of staff. Ongoing operational funding for a regional organization is obtained from a results delivery service via a self-funding model. The annual funding required to sustain a regional organization is estimated at $2.5 million to $4 million per one million people (population).

The *Roadmap* suggests that most HIT costs should be absorbed by the organization that is the primary user of the HIT system. In fact, many Arizona clinicians have already invested in such systems. A possible approach for clinicians who cannot afford a full EMR system is to offer a subset of those services through a Web-based system. It is believed that this more affordable option could be offered to clinicians for about $3,000 per clinician per year.

D. Legal

Implementation of the *Roadmap* requires that various legal issues be addressed. Arizona must ensure that the health information included in an e-health information exchange is confidential and secure. In addition, consumers must trust that their health information will be kept confidential. Rigorous confidentiality protection for the health information handled by an e-health information exchange is essential to the long-term success of the mission.

Specific legal issues to address include:

- Consumer control over their health information
- Appropriate handling of "special" health information that has greater confidentiality protection
- Appropriate handling of minors' health information
- Identification of those who will have access to e-health information in the exchange and for what purpose

E. Governance

A statewide governance body is needed to develop a uniform approach to legal issues and many other aspects of *Roadmap* implementation. The *Roadmap* recommends that a statewide nonprofit Health-*e*

Connection corporation be created to provide leadership, negotiate standards, and encourage cooperation and collaboration. This organization would strategically collect and distribute funding, help align financial incentives, develop statewide technical infrastructure when needed, and advocate for needed policy change. The governance body would consist of a governance board, board committees, full-time staff, a Council of Initiatives, and a Technology Advisory Council.

The governance board would maintain and refresh the vision, strategy, and outcome metrics underpinning the *Roadmap*. It would provide advocacy when needed and build trust, buy-in, and participation of major stakeholders statewide. In addition, the board would assure that equitable and ethical approaches are used in implementing the *Roadmap*. It might also raise, receive, manage, and distribute state, federal, and private funds. It would prioritize and foster interoperability for statewide and sub-state initiatives. Finally, it would implement statewide projects and facilitate local/sector projects.

The Health-*e* Connection board would include statewide stakeholder interests critical for *Roadmap* success, including clinicians, hospitals, payers, consumers, employers, and service providers (such as laboratories). Statewide representatives would be joined by representatives from each MTA to ensure integrated decision-making at the state and local levels.

Board committees, chaired by board members, would permit input by an even broader set of stakeholders, as well as content expertise in areas such as clinical problem-solving, technical architecture and standards, confidentiality and security concerns, and finance. Recommended standing committees include Clinician, Employer, Payer, and Consumer.

Participants of the many e-health initiatives in Arizona would be asked to join a Council of Initiatives to identify obstacles and solutions to enhance future interoperability of health information systems. The Council of Initiatives would be a forum for all interested e-health projects, including those with a more limited scale than an MTA. In addition, technical advisory boards would be forums to propose technical standards, policies, and solutions.

The Health-*e* Connection board should be supported by a full-time executive and supporting staff. Contractors may also be used to supplement the skills of full-time employees. The staff would execute strategic, business, and technical plans. Staff would also coordinate day-to-day tasks and deliverables, including establishing contracts and participation with local/regional initiatives.

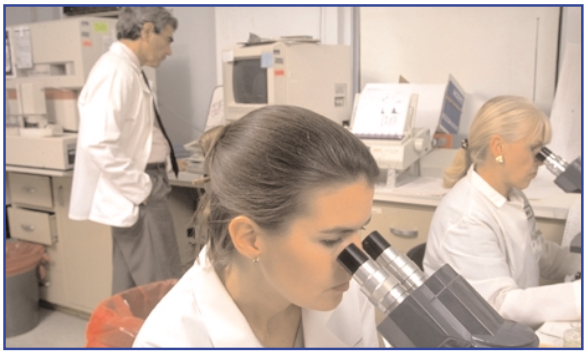
F. Transition Team

Even though the governance body is responsible for implementing the full *Roadmap*, a transition team will implement the governance body and the first deliverables. Transition is estimated to take about 12 months.

One of the most important goals of transition is to maintain the momentum established when developing the *Roadmap*. The first activity during transition is to finalize the transition structure, which includes obtaining commitments from the participants, identifying interim funding requirements, and acquiring the funding. Obtaining commitments from participants should take no more than one month. Identifying interim funding requirements and funding sources will occur over the following several months.

Once the participants commit to working on the transition, other activities will commence. These activities include:

- Establishing a statewide governance organization
- Establishing a practical strategy for statewide engagement in the Health-*e* Connection effort
- Implementing the first HIE initiatives
- Identifying and beginning to coordinate with current Arizona HIT initiatives
- Implementing the committees that will address the privacy, confidentiality, and legal issues
- Developing a marketing and education plan for *Roadmap* implementation



Key HIE initiatives to be implemented during the transition phase include developing a basic patient health summary, setting up a statewide Web portal with security infrastructure components, and establishing the first MTA information exchange with a results delivery service. The first results delivery service will immediately begin to develop a provider directory, establish a master patient index for the MTA, and launch the process of data normalization.

G. Wrap-up

There is no single method to undertake such a diverse task as creating an e-health infrastructure for Arizona. Stakeholders and participants in the process were able to reach a general consensus on the direction of the *Roadmap*. However, the timing of events, technologies chosen, financial strategies employed, and other factors ultimately will be received differently by each stakeholder. The *Roadmap* balances various competing priorities by advocating a representative governance structure, and it incorporates flexibility to adapt to lessons learned, technical advancements, and national standards as they emerge.

The process of implementation is incremental, long, and difficult. Dedicated commitment from multiple stakeholders is imperative. With persistence and diligence, however, Arizona can achieve Governor Napolitano's vision for e-health connectivity.

Finally, development of this *Roadmap* would not have been possible without the coordinated and concentrated contributions and efforts of many Arizona public and private partners, each with a sense of urgency and commitment to advance the *Roadmap* and its recommendations. Their knowledge, input, assistance, and spirit of dedication and teamwork were essential to successful completion of Governor Napolitano's Executive Order. The content presented in this *Roadmap* is a direct result of thousands of hours of volunteered time.

II. Introduction

The delivery and management of healthcare has extended beyond the walls of a single hospital or doctor's office and has resulted in healthcare information being located in a variety of institutions. Since patients and consumers often receive healthcare from more than one location, it is of paramount importance to move healthcare information with patients so that it is available wherever and whenever they receive care. Consensus has emerged within federal leadership and both the public and private sectors that health information technology (HIT) and health information exchange (HIE) play a key role in addressing the mounting challenges facing our nation's healthcare system. Several state governments are becoming engaged in the use of HIT and HIE to support policy goals and the improvement of healthcare delivery and outcomes.

There is no standard, widely accepted solution. Indeed, early experience suggests that successful efforts have different starting points, initial approaches, emphases, organizational forms, and evolutionary paths toward a common objective of a secure and ubiquitous information exchange. Consistent with U.S. Department of Health and Human Services (HHS) Secretary Michael Leavitt's maxim of "national standards, neighborhood solutions," state and local governments are beginning to collaborate and develop a consensus among diverse stakeholders on the vision, goals, and plans required to foster improved healthcare and outcomes through timely and appropriate healthcare information exchange. It is likely that as states begin to recognize the opportunities presented by HIT and HIE, more state leadership and initiatives will emerge.

On August 30, 2005, Governor Janet Napolitano issued Executive Order 2005–25 to develop the Arizona Health-*e* Connection *Roadmap* (see Appendix A: Governor's Executive Order). Under the Governor's Executive Order, the Health-*e* Connection Steering Committee is charged with developing a plan for Arizona to achieve statewide electronic health data exchange among insurance companies, healthcare providers, and consumers of healthcare, as well as exploring issues related to implementing electronic medical records. The *Roadmap* is consistent with the goals of President Bush and the HHS Office of the National Coordinator for Health Information Technology (ONC) to "achieve 100 percent electronic health data exchange between payers, healthcare providers, consumers of healthcare, researchers, and government agencies as appropriate."

Since the Call to Action Summit in October 2005, several activities to support the Executive Order have been made possible with the support of St. Luke's Health Initiatives and the BHHS Legacy Foundation in collaboration with the eHealth Initiative Foundation and its Health Information Exchange partners. Subsequent to the Call to Action, the 42-member Steering Committee, five task groups (Clinical, Financial, Technical, Legal, and Governance) with a total membership of more than 250, and a project management team collaborated for five months to create the *Roadmap* (see Appendix B: Organization Structure for *Roadmap* Creation). Under the leadership of the Steering Committee co-chairs, the activities in Figure I have been completed to create the *Roadmap*:

Figure I: Completed Activities

Project Activity	Impact
Weekly Project Management Meetings	• Increased awareness of activities and scope management • Obtained stakeholder input and collaboration • Initiated task group activities • Created the *Roadmap*
Arizona Briefing/ Assessment Paper	• Identified barriers and priorities • Established a baseline of information
Steering Committee Meetings (five meetings total)	• Established expectations and roles • Provided leadership for the process and a communication channel between the Governor and Steering Committee • Created Task Group charges • Provided guidance and approval of task group recommendations • Assured adherence to the Executive Order • Identified *Roadmap* Mission Statement and Values and Guiding Principles
Five Task Groups Meetings (17 meetings total)	• Identified urgent and feasible priorities • Developed recommendations for *Roadmap*
Task Group Leadership Meetings	• Provided synchronization among all task groups • Reviewed all task group work • Verified recommendations for feasibility and urgency

The Health-*e* Connection Roadmap articulates a path to improve the quality and reduce the cost of healthcare in Arizona. The *Roadmap* identifies key decision points by focusing on the what, when, why, and who — what action needs to occur, when the action needs to occur, why the action is necessary, and who (individual/group/organization) is required to complete the action. Specific values and guiding principles were identified at the onset of this initiative to guide the *Roadmap* development. The top-level values and guiding principles are listed in Figure II. The entire Values and Guiding Principles for Arizona Health-*e* Connection are listed in Appendix C: Process to Create the *Roadmap*.

Figure II: Arizona Health-*e* Connection Top-Level Values and Guiding Principles

- Create achievable, actionable, and practical initiatives
- Ensure that initiatives are consumer focused
- Provide technical basis for health data exchange
- Promote sustainability
- Increase the quality and performance of healthcare in Arizona
- Assist in healthcare research

The *Roadmap* reveals the recommended actions and key milestones to achieve in the next five years to accomplish the goals stated in the Executive Order. The overall goal is to achieve early adoption of a statewide e-health information infrastructure that will improve the quality and reduce the cost of healthcare

in Arizona. Other key benefits include improved care safety and patient self-management and improved surveillance and response to public health problems.

Full achievement of the goals requires interoperable health information systems combining a) health information sufficiently standardized to be machine usable; b) health information technology that can send, receive, route, assemble, and interpret such standardized information when and where needed; c) health information technology that includes automated decision support for better self-care, patient care, and public health; and d) health information exchanges that establish the legal and technical infrastructure to securely, confidently, and efficiently move the information between authorized users.

Healthcare, business, and government leaders throughout Arizona are excited and enthusiastic about the opportunity to improve patient care and delivery through health information exchange developed over a staged, multiyear plan. Through continued dialogue and collaboration among the diverse stakeholders in Arizona, supported by lessons now being learned in different parts of the country, the state has the opportunity to achieve significant gains in quality, safety, and efficiency through the effective and appropriate implementation of the *Roadmap* and become a national leader in e-health information exchange.

Recognizing the Challenges

Arizona clearly faces significant technical, privacy, and sociopolitical challenges in sharing health information statewide. By recognizing these challenges, the *Roadmap* provides strategies to negate the hurdles.

First, a wide variety of stakeholders are at the table with very different expectations. Stakeholders include government agencies, hospitals, physicians, dentists, nurses, pharmacies, labs, insurers/payers, a variety of associations, and consumer interests. The *Roadmap* process took all concerns into consideration in establishing priorities and developing initiatives.

In addition to the variety of stakeholders, stakeholders' adoption of HIT differs widely even among members of the same interest groups and the technology products being used are diverse. Because of the differences in the products and how they are used by various people or organizations, data standardization is lacking. The *Roadmap* acknowledges stakeholder diversity and takes into consideration the enormous amount of work required to remove the resulting ambiguities between the current data sources and to provide better guidance for future technologies that will be implemented.

Another related challenge is Arizona's geographic diversity. Each region has its own opportunities and challenges. For example, some rural areas of Arizona are fairly isolated without bandwidth to take advantage of many of today's technologies. Some consumers live on the borders of other states and receive medical services in those states. Also, some communities, such as Yuma, have close relationships with the medical communities in Mexico. The *Roadmap* takes into consideration the differences in each region.

Of course, there are the additional complexities of organizational policy, laws, regulations, and challenges in paying for implementation of the *Roadmap*.

With all of these and other issues to address, we must recognize that there is no panacea for the challenges ahead. The challenges are not insurmountable, but they must be understood and respected.

The *Roadmap* considers the following points to enable it to meet these challenges:

- Not all of the challenges have been identified; therefore, not all of the answers are available. The *Roadmap* is flexible to meet the challenges ahead

- Changes will occur in technology, medical science, and demographic factors that shape the overall demand for care. The *Roadmap* embraces changes in technology and leverages the future functionality and opportunities that become available to help address changes in medical science and demand patterns. In addition, older technologies will continue to be used and replaced only when participating organizations need additional functionality or have a financial incentive to do so

- Each stakeholder has different needs and different clinical and business processes. To meet these needs, vendors have developed many different but viable products for the market. There is no one-size-fits-all solution. Organizations must be able to use HIT products that address their needs, but also must be

able to exchange data with the rest of the healthcare community. Also, current standards will be changed and improved, and those changes will be absorbed to help with the seamless sharing of data

- The *Roadmap* leverages local interests that wish to implement local initiatives. It is in regional areas that patients are served and where the challenges are best met. The *Roadmap* encourages and supports local initiatives while providing guidance and infrastructure for sharing data among the various regions in Arizona

- The *Roadmap* reduces the disparities between the haves and the have-nots, whether this means those without broadband in their community or those who lack funds to pay for critical infrastructure or products. While the *Roadmap* does not have all the answers, it contains the ingredients needed to address these and other challenges going forward

- No single application determines success or failure of the *Roadmap*. Because of the enormous complexity of the environment and challenges, it is possible for a misstep to occur along the way. The *Roadmap* calls for work on key projects and objectives concurrently. Momentum and advancement will continue, even if one project encounters difficulties. The *Roadmap* also defines an infrastructure that enables reevaluation and permits necessary course corrections along the way

- Momentum developed while creating the *Roadmap* will be leveraged during implementation. Low-risk key products will be developed in the early stages of implementation. An interim transition organization will also be established to immediately begin implementing the *Roadmap*. The transition organization is tasked with establishing a permanent governance structure, among other things. This approach will provide the momentum needed to continue the goodwill and interest established while developing the *Roadmap*

- The *Roadmap* also seeks to leverage existing projects and initiatives under the strategic Health-*e* Connection umbrella. Many good things are happening in the Arizona Healthcare community and they should be encouraged, supported, and leveraged to further the goals and objectives of the *Roadmap*

In recognizing the complexities of the environment, the *Roadmap* takes a phased approach based on geography, functionality, and audience. The phased approach reduces risk and recognizes the challenges associated with location, the capabilities organizations require, and the various stakeholders involved.

While there are challenges, some are fading and the numbers of HIE and HIT initiatives are increasing. No challenge is identified as insurmountable in Arizona's quest to become a national leader in realizing the benefits of HIT and HIE.

III. Roadmap Fundamental Concepts

Several keys to understanding the *Roadmap* approach are presented in this section. The following three fundamental concepts are identified as crucial in creating Arizona's approach.

Fundamental Concept #1: Differences Between Health Information Technology and Health Information Exchange

The *Roadmap* approach is based on a distinction between health information technology (HIT) and health information exchange (HIE). This fundamental distinction simplifies the interrelationships between various components and clarifies the strategies necessary for implementation.

Health information technology (HIT) is the deployment of technology to support specific organizational business and clinical requirements. HIT is the technology within the physical four walls of a doctor's office, laboratory, or hospital or a virtual hospital system. Items such as electronic medical records (EMR) systems, administrative systems (such as billing), and workflow systems are examples of HIT systems.

Health information exchange is infrastructure to enable data sharing between organizations. Services are built once and used multiple times by many. Items such as a central Web site, healthcare terminology translation tools, a master patient index (MPI), authentication and authorization infrastructure, and applications to aggregate information from multiple sources are examples of HIE resources.

Specific recommendations presented in the *Roadmap* have been developed with direct consideration of the following HIT and HIE strategies.

HIT *ROADMAP* STRATEGIES

- Partner with organizations already involved in HIT adoption
- Adopt or, if necessary, set standards (especially for integration with HIE)
- Provide guidance, direction, and education
- Provide incentives
- Identify barriers and propose solutions

HIE *ROADMAP* STRATEGIES

- Begin by developing HIE regionally
- Leverage existing IT projects and rich data sources
- Develop key statewide resources for data access and sharing

Some items do not fit neatly in either the HIT or HIE category. Those items are identified as such when they are mentioned in the *Roadmap*. For example, ePrescribe systems typically have some components that fit the definition of HIE and some components that fit the description of HIT.

Fundamental Concept #2: Urgency Balanced by Feasibility Determines Timing of Roadmap Inclusion

A guiding principle of the *Roadmap* is to identify initiatives that are practical, achievable, and actionable. The *Roadmap* team recognized that it was not possible to do everything at once. Scarce resources (financial, human, time, etc.) demand that careful examination of all activities be conducted. In addition, it was necessary to identify and prioritize the proper activities to build and sustain project momentum and enthusiasm.

Choices identified in the *Roadmap* were considered from the perspectives of *urgency* and *feasibility*. Urgent initiatives bring relief to a problem in the healthcare system. They provide a high level of value to one or more constituent communities (such as patients, providers, and payers). Feasible initiatives include items likely to immediately succeed *as well as initiatives that are necessary prerequisites for achievement of an urgent priority initiative*. Implementation of a feasible initiative does not necessarily provide a high level of stand-alone urgent value.

The *Roadmap* is constructed with initiatives that provide either a high level of urgent value or feasible value or both. Sequencing of the recommended initiatives was chosen to maximize impact and utility for the sum total of all initiatives.

In the process of developing the *Roadmap*, several initiatives were placed in a grid showing their relative urgency and feasibility. Figure III lists key products and infrastructure components identified in the *Roadmap*. Certain items not identified as priorities from a clinical or business perspective were included in the grid based on their importance as infrastructure components that enabled the important products. The grid's horizontal axis lists the selections "Higher Feasibility" and "Lower Feasibility." The vertical axis lists the selections "Higher Urgency" and "Lower Urgency." The products and infrastructure components were placed in the grid based on their urgency and feasibility. From this grid, the timing of the products and infrastructure in the *Roadmap* was determined.

The grid presents priorities for Year One of the *Roadmap*. Items identified as lower urgency or lower feasibility in the grid increase in priority in later stages of the *Roadmap* as various prerequisite initiatives are implemented.

Fundamental Concept #3: Medical Trading Areas

Many HIE projects will be developed within the context of a medical trading area (MTA). An MTA is usually a geographic area defined by where a population cluster receives its medical services. It is an area in which groups of physicians, hospitals, labs, and other providers work together to serve a population of consumers. Within an MTA, the medical service providers or subsets of providers are often organized either formally or informally, and many are already exploring projects to enable them to share patient data.

Figure III: Urgency and Feasibility as Viewed in Year One of the Roadmap

	Higher Feasibility	Lower Feasibility
Higher Urgency	**Year 1 - 2**	**Year 3 -4**
	Web portal (statewide)	(Enhanced) Patient Health Summary - by MTA
	Statewide (Basic) Patient Health Summary	(Additional MTAs) - results delivery, provider directory, MPI, data normalization
	MTA results delivery	Encourage HIT adoption
	MTA provider directory	Statewide patient record locator
	MTA Master Patient Index (MPI)	
	MTA data normalization	
	Secure Infrastructure components	
	Secure messaging	
	Encourage HIT adoption	
Lower Urgency	**Year 3 - 4**	**Beyond**
	Statewide personal health record	Encourage HIT adoption
	Add public health functions	Add functions for oral health and other professionals

The greater metropolitan Phoenix area is an example of an MTA. The population of the Phoenix area is served by physicians, hospitals, labs, and other providers located in the same geographic area. Many providers have working relationships with each other to serve their patients and they often want an increased ability to share patient data in a secure and confidential way.
Because most data sharing will happen at a regional area with providers that already have relationships in serving consumers, it is much easier to develop trust between providers and it leverages the trust consumers have of their providers. Data-sharing agreements and data-use agreements will be much easier to develop and control at the local level.

MTAs are not specific to a large metropolitan population. Rural areas are included in this process. Arizona may develop several MTAs throughout the state to specifically serve rural providers and to account for the needs of all of Arizona's populations.

IV. Health Information Technology (HIT) Approach

A. HIT Adoption Strategies

The HIT adoption strategies may be summarized in five approaches: 1) partner with other organizations that already have HIT adoption programs; 2) adopt and, if necessary, set standards; 3) provide guidance, direction, and education; 4) provide incentives; and 5) identify barriers and propose solutions.

Partnerships

The statewide Health-*e* Connection governance body will partner with organizations that are already focused on HIT adoption strategies. The governance body will coordinate activities with these partners as the *Roadmap* is being implemented. A sample of the organizations include the Health Services Advisory Group (HSAG) and its efforts to implement the national Doctor's Office Quality–Information Technology (DOQ-IT) initiative, the Arizona Chapter of the Healthcare Information and Management Systems Society (HIMSS), the Arizona Health IT Accelerator (AHITA), and various medical associations. The governance body will partner with these and other organizations and continue the work of HIT adoption in Arizona in a concerted way.

For descriptions of DOQ-IT, AZHIMMS, and AHIT and how they propose supporting HIT adoption within the structure of the Health-*e* Connection *Roadmap*, see Appendix D: HIT Support Organizations.

Standards

Working with partners, the statewide governance body will adopt and set standards to ensure that HIT efforts will be able to exchange data with Arizona's HIE efforts. Arizona will adopt industry standards and certification programs if they meet Health-*e* Connection objectives.

As the *Roadmap* is being implemented, the statewide governance body may determine that the various national and industry standards or certification programs are not detailed enough to adequately ensure that data can be shared. If this is the case, the governance body will provide additional guidance in the form of localized standards for the Arizona HIT community. These localized standards will be developed with input from medical trading areas or strategic HIT partners, depending on the types of standards being developed.

Guidance, Direction, and Education

The statewide governance body will provide guidance, direction, and education to the community as part of the HIT adoption effort. Many of the potential partners working on HIT adoption provide a variety of services to the clinician community to encourage HIT adoption. The statewide governance organization will point people to these programs. One way is by developing a Web site that directs people to the class schedules, program descriptions, online tool kits, and other information and services dealing with HIT adoption. The Web site could provide bulletin boards, online chat rooms, collaborative work tools, and other resources to help the clinician community. In short, the statewide governance body will be a clearinghouse of the available services at the state and national levels.

The statewide governance body also will provide guidance on adopting federal policies and standards at the clinician level. A lot of information is available and it is difficult for people to understand the various requirements that have been developed.

For providers, health plans, and vendors that wish to do business in Arizona, the governance body can provide guidance on requirements for inclusion in the health information exchange. This will provide potential businesses with both the expectations and the opportunities available. This sets a level playing field with all businesses located or wishing to do business in Arizona.

Another area in which the statewide governance body can provide direction and guidance is in the open source movement and how it plays into Arizona's future plans. Many open source products are being developed for use in various aspects of healthcare provision. The governance organization should review

these developments and provide direction to the healthcare community.

HIT adoption would benefit by coordinated HIT classes in Arizona medical, nursing, and related field schools. As graduates enter the medical field, they will already be trained to use HIT and know some of its benefits. The new doctors will be technology savvy and will want to work in offices that were early adopters.

There are numerous other areas in which the governance body can become involved in providing guidance, direction, and education. Additional opportunities include vendor product ratings, pricing information, sample requests for proposal (RFPs), sample contracts, return-on-investment studies, readiness assessments, implementation plans, and HIE interface specifications. The governance body will work with various partners at appropriate times to provide help to clinicians in adopting HIT solutions.

Provide Incentives

The Governor's budget for FY 2007 includes $1.5 million for grant money to be distributed to HIT projects in rural areas. This is to be administered by the Arizona Government Information Technology Agency (GITA). There is other grant money for rural HIT projects at the local and national levels as well. The statewide governance organization will identify and make the clinician community aware of these and possibly provide training in how to apply for them. In essence, the governance body will be a clearinghouse, with information on the Web portal, for all available grants.
The statewide governance organization will work with its partners to explore other financial incentives for clinicians implementing HIT. Incentives may include various HIT tax credits, low-interest loans, raising money from foundations to redistribute as grants, etc.

For clinicians who cannot implement their own HIT solutions, Health-*e* Connection could provide data through a Web browser to encourage minimal adoption of HIT.

Identify Barriers and Propose Solutions

The statewide governance organization will work with its partners to continue identifying and proposing solutions to barriers. It will get involved in activities such as surveys of clinicians that gauge HIT adoption and identify barriers to adoption.

Other Opportunities

There are many other areas in which the statewide governance organization could become involved in HIT adoption. Over time, the governance body will identify areas based on experience that will have the greatest impact. See Appendix E for a list of sample HIT adoption strategies.

B. HIT Products and Functionality

During the *Roadmap* development process, key HIT product types were identified as priorities from a clinician point of view. The three priorities are (in no particular order):

- Electronic medical records
- ePrescribe
- Practice management systems (e.g., billing)

Because they were identified as important to the clinical community during the *Roadmap* development process, these key HIT products are a priority for adoption. The following descriptions of the product types also provide some justification for their being singled out as priorities for adoption.

Electronic Medical Records

Electronic medical records (EMRs), which refer to the capability to record, store, and retrieve patient medical records electronically, are central to improving the care process. This is particularly true with advances that allow portability, remote access, import, storage, and export of machine-readable electronic information (not just text), connection to other applications

such as billing and ePrescribing, and the inclusion of clinical decision support programs that alert clinicians to possible safety or quality problems.

ePrescribing

ePrescribing allows clinicians to order prescriptions electronically from a pharmacy, eliminating handwriting errors and errors related to manual retranscription into and out of paper forms. Many ePrescribing applications also help check medications against patient allergies, interactions with other medications, and insurance plan formularies and price lists. ePrescribe is a product that could have HIT and HIE implications and deployment.

Practice Management Systems

Practice management software is the most widespread electronic information management application in medical practices today. As payment systems for healthcare become more complex (narrow provider networks, multitiered health plans, medication formularies, preauthorization requirements, increased copayments and deductibles, and personal health savings accounts, among other developments), the ability of a practice to negotiate claims with payers and collect fees from patients requires increasing amounts of clinical information. This may be accomplished increasingly through the integration of practice management systems with clinical electronic medical records.

Other Products and Functions

Other products and functions were viewed as important to at least some segments of the healthcare community, depending on the organizations' roles and needs. Continuous encouragement of these products will also be encouraged when applicable. Other important functions included:

- Disease management
- Chronic care management
- Home healthcare reporting
- Real-time results from medical and therapeutic machines and instruments
- Task management
- Referrals
- Charge capture/right coding
- Decision support (alerts, best clinical practices, reminders, facilitate diagnoses)
- Patient education
- Drug-to-drug, drug-to-allergy alerts, etc.

Strategic HIT Systems

Certain HIT systems potentially have strategic value to the *Roadmap*. The strategic value depends on the application, but in general the applications either are data-rich resources for clinical information that might be shared or they provide functionality desirable to other Arizona stakeholders and could be shared to reduce the overall cost of the *Roadmap*. Examples of Arizona HIT systems with potential strategic importance are the state's immunization system, Arizona Health Query, Secure Integrated Response Electronic Notification (SIREN) system, and certain Arizona Health Care Cost Containment System (AHCCCS) data. There are also national data sources and services. SureScripts, a service that provides prescription fulfillment information from pharmacies, is one example. The *Roadmap's* approach to these potentially strategic HIT systems will be ascertained individually based on their strategic value and how they could be leveraged, if appropriate.

In addition, the governance body may determine that, for strategic purposes, it should develop an HIT system. For example, the governance body may determine that it should provide ePrescribing for those without HIT systems. This, in part, will help those that cannot afford or that face other barriers to implementing HIT systems.

V. Health Information Exchange (HIE) Approach

A. HIE Strategies

There are three strategies to develop a statewide HIE in Arizona: 1) begin by developing HIE regionally; 2) leverage existing IT projects and rich data sources; and 3) develop key statewide resources for data access and sharing.

Regional HIE

While the ultimate aim is sharing health data statewide, there are compelling reasons to start the process by developing the infrastructure regionally. The first reason is that medical delivery services are highly regional. A look at the total number of medical services provided to the population shows that the vast majority of services take place relatively close to the patients. Keeping the data close to where it is required enhances the speed and reduces the complexity of providing data to the patients' clinicians. Data-sharing and data-use agreements will be much easier to develop and control at the local level.

When taking on a project of this scope and magnitude, it only makes sense to implement it in portions. Dividing the work by geographic locations where groups already have established working relationships increases the likelihood of success.

Existing IT Projects and Rich Data Sources

Because healthcare projects, initiatives, and databases already exist in Arizona, they should be leveraged as part of the *Roadmap*. Early in the *Roadmap* development process, a high-level inventory was taken and many current initiatives with strategic value were identified. For example, Health-*e* Connection will partner with current initiatives to solve last mile and rural broadband issues.

Key Statewide Resources

Although Arizona will develop HIE regionally, certain resources should be provided statewide. For example, there should be one Web portal that provides access to data available from the various regions. Another example is a centralized patient locator service that can find all medical information about a patient throughout the state, regardless of region.

B. HIE Products and Infrastructure Components

The following sections identify and describe the major HIE products and required infrastructure components necessary to support statewide HIE.

Patient Health Summary

As Arizona works toward sharing health information statewide, many things need to be developed to make that goal a reality. In the process, there are short-term milestones that will add significant value to the quality of healthcare in Arizona. One of these is a patient health summary[1].

During the *Roadmap* development process, a patient health summary was identified as a product that would have the greatest short-term clinical impact on patients. Creating a summary will enhance continuity of care for patients, which impacts quality of care, potentially lowering costs and increasing communication between doctors providing the care. This will help reduce redundant and unneeded care while limiting delays in therapeutic care.

The patient health summary will provide a historic view made of data assembled from a variety of sources accessible to all clinicians on a 24-hours-a-day, seven-days-a-week basis via the Internet. It will contain a variety of information, including result trends, discharge summaries, and procedure reports. Nine types of information (topics) were identified as especially important. They are listed in Figure IV.

Figure IV: Topics of Information for Inclusion in the Patient Health Summary

Medications—prescribed
Medications—dispensed
Allergies
Immunizations
Lab results and trends
Other providers caring for patient (and contact information)
Cumulative medical problem list (from billing and or EMRs)
Insurance/eligibility and basic demographic information on patient
Hospital and emergency department discharge care summary

It is highly likely that the patient health summary will be developed in phases. The *Roadmap* makes a distinction between a "basic" patient health summary and an "enhanced" patient health summary. The basic patient health summary is envisioned as a pilot project that compiles information from several existing statewide data sources. It will provide clinical value but is limited in scope on the quantity, type, and standardization of data presented. An enhanced patient health summary is, by comparison, a more complete portrait of an individual's key clinical and administrative information. Several prerequisite activities, such as implementation of regionally based results delivery services, are necessary to realize an enhanced patient health summary. The enhanced patient health summary will be developed incrementally as the data becomes available and transformed on an MTA-by-MTA basis.

Statewide Web Portal

One milestone on the road to providing a patient health summary and eventual statewide sharing of patient data is developing a statewide Web portal. This will be among the first things to be implemented from the *Roadmap*. Providing a one-stop access point to statewide resources is an important roadmap component because clinicians and citizens will need to know only one Web address to obtain all of the information available to them. The Web portal will provide several important functions.

The Web portal will play a marketing and education role for implementing the *Roadmap*. Any news, updates to functionality, and other developments will be available on the Web portal. Another aspect of this role is providing clinicians and other providers with HIT adoption resources. Information about HIT standards, funding sources, and other pertinent resources will be available on the Web portal. The Web portal will be an important tool for increasing HIT adoption throughout Arizona and communicating to the general public.

In addition, the Web portal will be an access point for online services available now to clinicians and eventually to the public. In the beginning, Web links to services already available from other sources will be provided. For example, currently there are online public healthcare eligibility tools for both clinicians and potential clients. Having one place to find these types of services adds value to the healthcare community and those who want to use those services. As the *Roadmap* is implemented and services are developed, they will be made available through the portal.

Because confidentiality, privacy, and security are so crucial, the Web portal will provide secured access to health information exchange.

Results Delivery Services

An astonishing volume of personal health information must be sent routinely among clinicians, service providers such as laboratories and imaging centers, pharmacies, hospitals, insurance plans, public health authorities, and other parties. Most of this information is sent by paper or fax, with attendant problems in confidentiality, information loss, labor, and errors

created during transcription, sending, receiving, printing, copying, and filing.

Research indicated that one approach successfully employed by several locations is to establish a results delivery service and leverage that capability to build other important e-health components. The concept is to first develop a service that delivers results from labs and other providers to the ordering clinicians in the formats they require. Some clinicians want results on paper, others want them sent via fax, and others want the results sent in electronic format to their automated systems. If labs and hospitals have to establish only one electronic interface for all lab results and they do not have to provide delivery in various formats, then they should save money on delivering the results. The savings would fund sustainable operation of the results delivery and additional infrastructure components necessary to enhance the services.

The results delivery service will be expanded to receive results from all labs and similar providers. These providers include commercial labs, reference labs, imaging centers, outpatient facilities, inpatient facilities, emergency departments, and surgical centers. The results delivery service will develop electronic interfaces to create data streams containing the results from all of these providers. Examples of results in the data stream include blood tests, immunology, pathology reports, X-ray, CAT scan, mammography, transcribed reports, and other information. The service will deliver those results to the ordering physicians and to other authorized recipients.

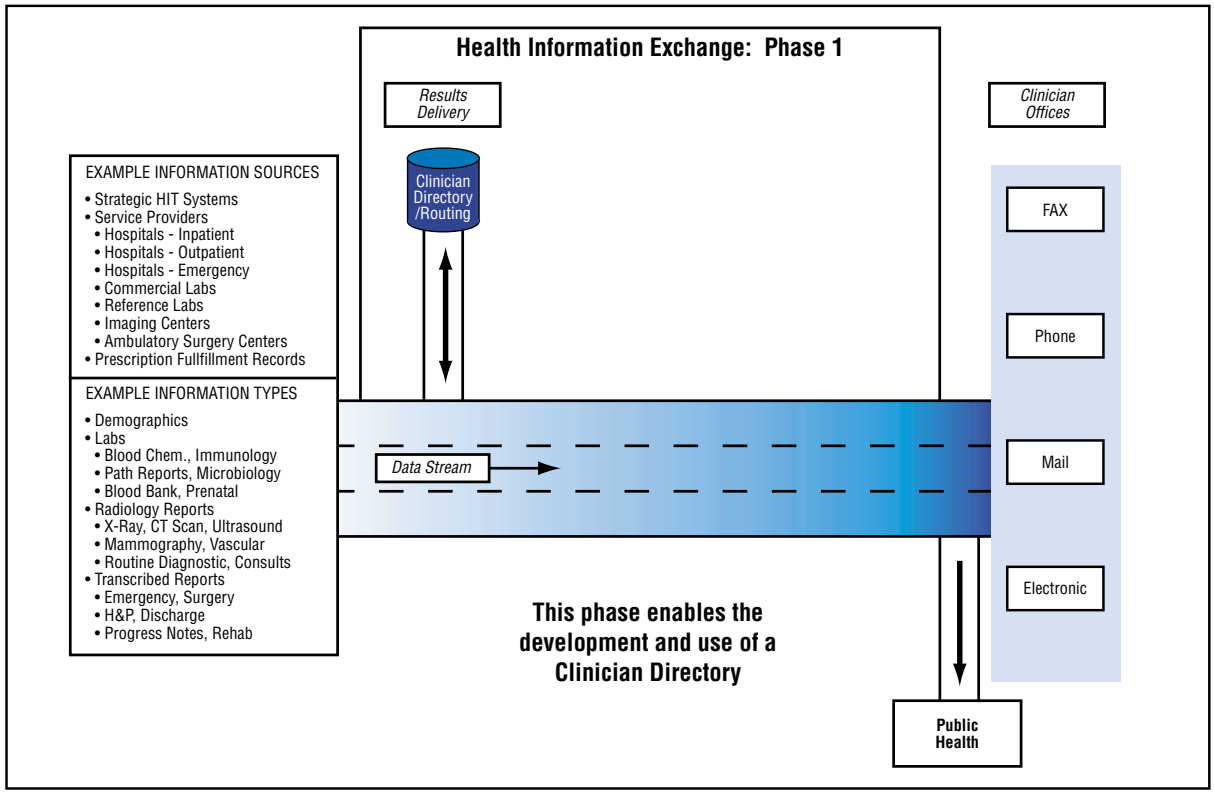
Over time, tools will be developed that glean data from the results to populate other important components necessary to provide a patient health summary. Also, data obtained via this mechanism will be instrumental in populating full electronic medical and health records.

The first important component that will be developed is a clinician directory. Information about the clinicians is necessary to deliver the results. Over time, the service may ask for additional data about the clinician to enhance the directory. During this process, the service will follow national and industry data standards to ensure that data is compatible with initiatives in later phases of the *Roadmap*. Appropriate information about these transactions can begin feeding public health systems.

One way to jump-start the clinician directory is to partner with the healthcare licensing or credentialing agencies and populate the provider directory with their data. The agencies may also be able to provide the administration services for clinicians accessing the data through the Web portal.

Beyond results delivery, the provider directory is important because it would help one clinician look up another clinician and find the appropriate address to send a message through the secure network. This could also be used to establish enhanced services such as a patient referral system. (For example, see Secured Messaging below.) Figure V provides an illustration of this first phase of results delivery.

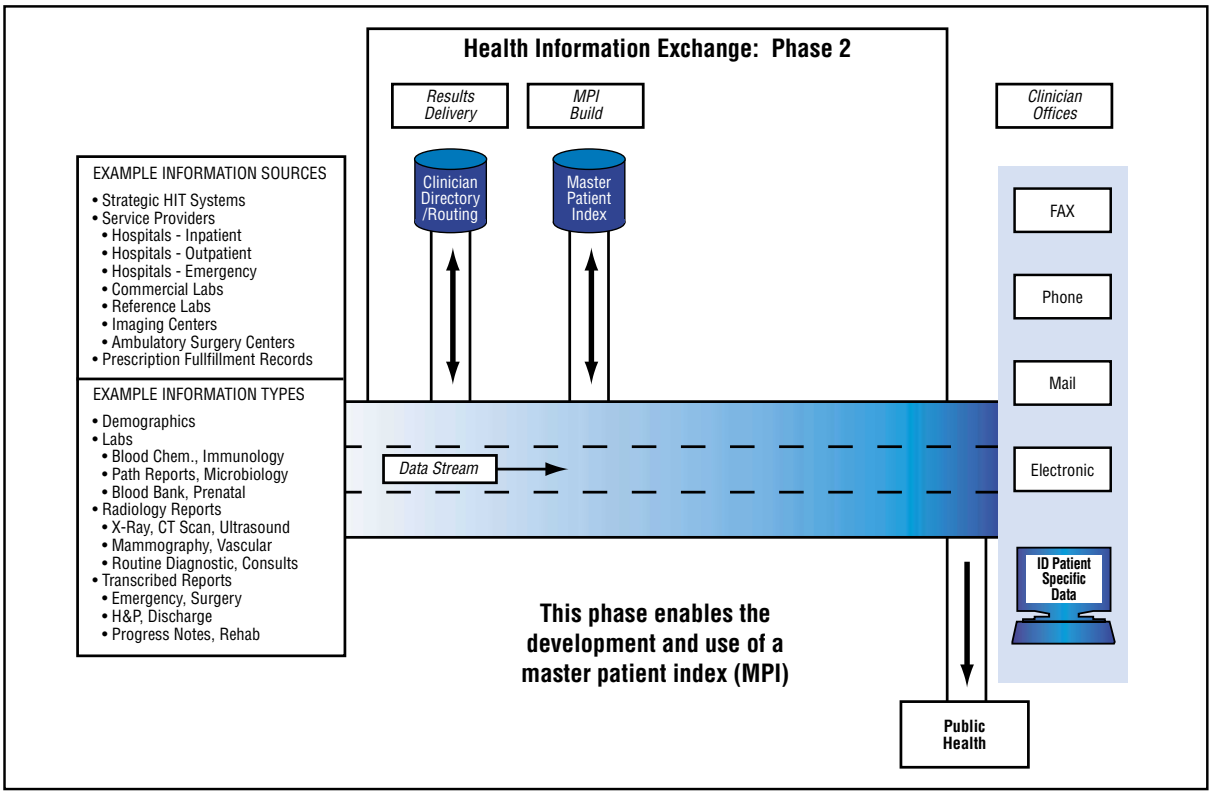
Figure V: First Phase for Results Delivery



The second component to be developed will likely be a master patient index (MPI). Again, data will be gleaned from the transaction and additional information will likely be requested to enhance the index. Data standards will be followed in creating the MPI.

The index is of utmost importance in that it a) enables the location of data about the patient and b) is required to connect data about the patient from various sources. Figure VI provides an illustration of this second phase of results delivery.

Figure VI: Second Phase for Results Delivery

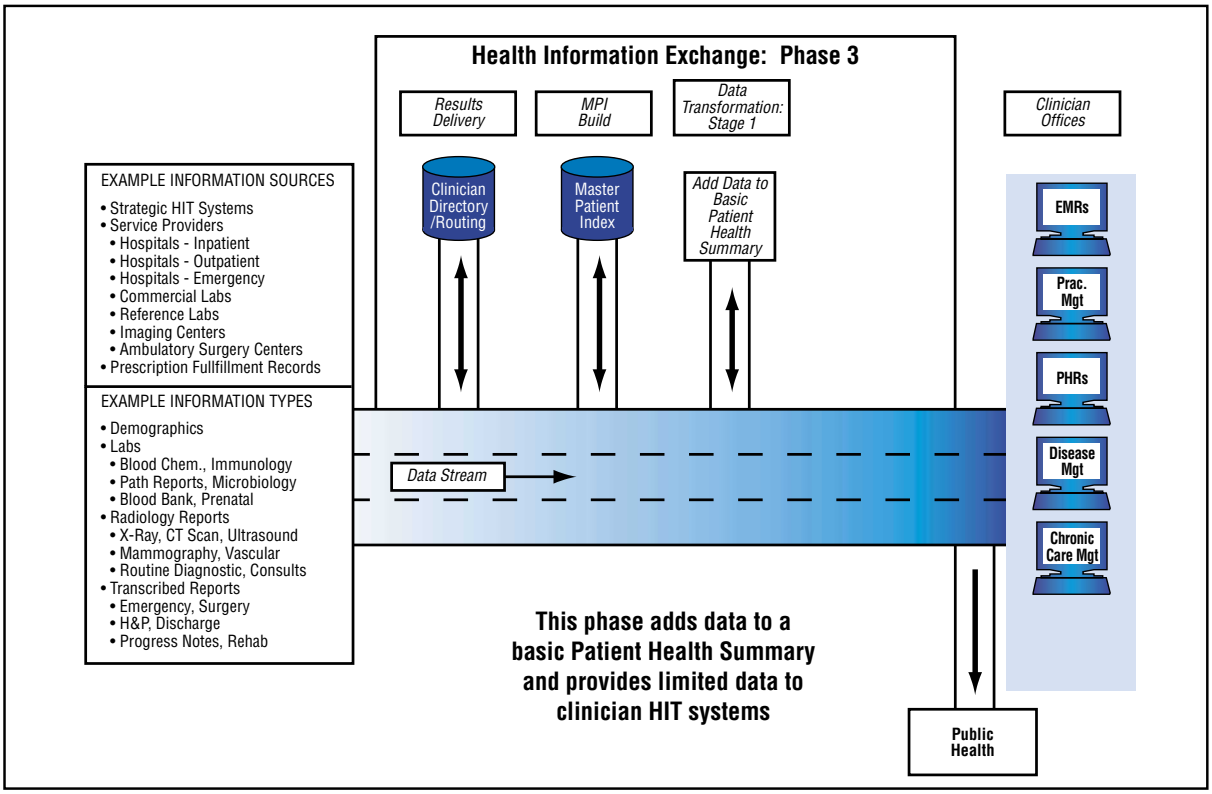


After the first two components are developed, the service will break down the lab and other clinical results into usable and shareable data that follow industry and national standards. This process, called data transformation (or normalization), is a key step in providing important clinical information and interfaces necessary for populating a patient health summary and, finally, comprehensive electronic health records.

An enormous amount of work will be required to convert the data stream into useable information. It will be a large and difficult task. Although many labs and others are already using the current industry standards, they are afforded much variation in implementing the standards.

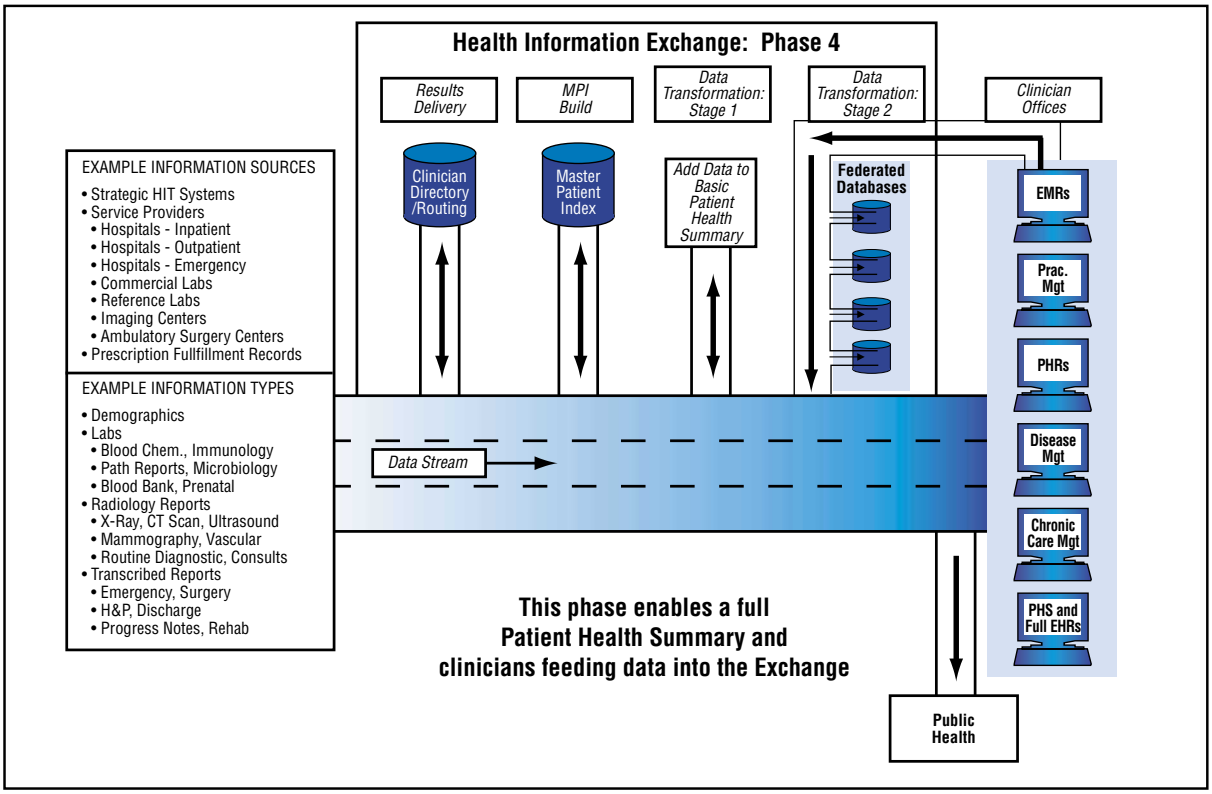
Once the data is standardized, it will be used to add information to a basic patient health summary. The patient health summary will be continually enhanced as data is transformed into shareable information. In addition, electronic interfaces that enable the seamless passing of data to the clinicians will continue to be developed. With these in place, the results delivery service can begin passing data into various HIT systems, including electronic medical records, practice management, patient health records, chronic care management, disease management, etc. Furthermore, more comprehensive data will be provided to public health systems. Figure VII provides an illustration of the third phase.

Figure VII: Third Phase for Results Delivery



In addition to continuing the work of transforming the data, the next task is to have clinicians share data that they created about the patient with other treating providers. This is important to the final goal of sharing health information statewide. There are multiple ways clinicians' information can be shared. It will likely be determined by the organizers of specific medical trading areas in conjunction with the statewide governance body in future phases of the *Roadmap*. Figure VIII provides an illustration of the fourth phase.

Figure VIII: Fourth Phase for Results Delivery



Results delivery services and other related activities will be developed within the context of a medical trading area (MTA). An MTA is usually a geographic area based on where a population cluster receives its medical services. It is also an area where groups of physicians, hospitals, labs, and other providers serve a geographic-based population of consumers. An MTA can be a metropolitan or rural area. The medical service providers or subsets of providers are often organized either formally or informally, and many are exploring projects that will enable them to share patient data.

Statewide Patient Record Locator

Ultimately, the central governance body will develop a patient locating service available through the statewide Web portal where providers with legal access will be able to obtain all appropriate medical data for their patients, regardless of the data's location in Arizona. The patient record locator will search the MPIs of MTAs. As the central governance body develops this capability, it will ensure that all appropriate data-sharing agreements are in place, along with all security controls and auditing functions.

Secured Messaging

Another priority identified by the *Roadmap* development process was the need for secured messaging between clinicians. This will enable timely and confidential communication between providers about a patient. This will be developed by leveraging communication tools that doctors are already familiar with, but those communications will go through a secure infrastructure that protects the data during transmission. The infrastructure developed for secured messaging will be leveraged for other services developed, as outlined in the *Roadmap*.

Public Health Alerts/Queries

Epidemics come and go, drugs and medical devices are recalled, and problems as diverse as water contamination, bioterrorism, or heat waves may have impacts on the health of thousands or millions of people. Public health agencies now rely on slow and inconsistent ways of receiving information about such problems. In addition, some agencies have a difficult time

disseminating clinical recommendations so that clinicians can use them to prevent illness and injury. As electronic systems permit automated reporting of surveillance information to public health authorities, facilitating alerts and clinical decision support, problems can be detected earlier and addressed rapidly by the entire health system. As the HIE infrastructure is implemented and earlier products are developed, public health capabilities will incrementally increase and the additional capabilities of alerts and queries will be addressed.

Personal Health Records

Personal health records permit patients to view, carry, and, in many cases, add to electronic documents containing their own important health information such as allergies, immunizations, and medication lists. Such records can serve various functions. At the simplest level they may facilitate providing information to clinicians, but they may evolve to help patients benefit from electronic health advice personalized to their own medical information (e.g., tailored to the medications a patient takes). Some records are created by patients; others are exported from records maintained by insurance plans or clinicians. There is now little standardization among the various personal health record formats, so they cannot electronically import or export information from different electronic medical records on a routine basis. While personal health records are currently products in some HIT solutions, it is recommended that a more comprehensive statewide approach to personal health records be addressed during later phases of *Roadmap* implementation.

Telecommunication Broadband and Last Mile Issues

A statewide electronic health information system depends on high-speed broadband connectivity between all points on the health network. But in the rural communities of Arizona, consistently available capacity does not exist in many areas. Broadband is defined as two-way communication of voice, video, and data at volumes of at least 1 megabit per second (Mbps). Broadband is available in only about half of the rural communities with a population of more than 500. Communities with fewer than 500 people have even less opportunity for broadband infrastructure because traditional models of broadband build-out have always depended on higher population density. The lack of broadband for rural healthcare providers will hinder their participation in the full implementation of Health-*e* Connection.

A number of organizations have committed to the ubiquitous availability of broadband across the state. The Governor's Council on Innovation and Technology (GCIT) recently established the Communications Infrastructure Advisory Committee (CIAC) to assume a leading role and center of influence to shed light on and help solve issues causing broadband disparities and deficits. The Arizona Telecommunications and Information Council (ATIC), the Arizona Technology Council (ATC), the Southern Arizona Tech Council (SATC), and the Greater Arizona eLearning Association (GAZEL) are addressing broadband availability. Because broadband is such a basic component of economic development, many business groups are also involving themselves in the discussions and issues.

The statewide governance organization will work closely with organizations seeking to resolve the broadband availability issue. Because of the close working relationship between Health-*e* Connection initiative and GITA, coordinating with CIAC and ATIC is relatively easy.

One way the *Roadmap* transition and governance bodies can assist in the discussion is to help identify where broadband deficits exist. Just identifying and uniting the various segments of the demand into a common voice can often create sufficient anchor tenancy for vendors to take notice and action. Demand aggregation is a major policy initiative promulgated by GITA other telecommunications advocacy groups.

Other Projects and Opportunities

Although some very specific milestones and projects are laid out above, this should not be seen as precluding any other projects or techniques that might be used as the *Roadmap* is developed. The *Roadmap* is developed specifically to take advantage of new ideas, changes in technology, and opportunities that may present themselves.

In fact, it is anticipated that various projects in the mid to latter stages of the *Roadmap* will use the HIE components developed in the early stages. For example, decision support capabilities, oral health functions, ePrescribe, integrated clinical/billing information flow for preauthorization and claims, and many other projects will most likely become feasible for implementation.

It is also recognized that changes in priorities may change because of changes in the economy, political climate, and other areas. While the focus has been on clinical data, the *Roadmap* is flexible enough to change gears and refocus efforts through the direction of the statewide governance body.

VI. Privacy and Security

A variety of federal and state statutes and regulations affect the formation of an e-health information exchange in Arizona. These include federal and state laws on medical record confidentiality, consumer rights, medical record administration, telemedicine, electronic signatures, fraud, abuse, and antitrust.

One of the legal challenges Arizona will face is to ensure that the health information included in an e-health information exchange is confidential and secure. For an e-health information exchange to be successful, consumers must trust that their health information will be kept confidential. Rigorous confidentiality protection for the health information handled by an e-health information exchange is essential to the long-term success of the mission.

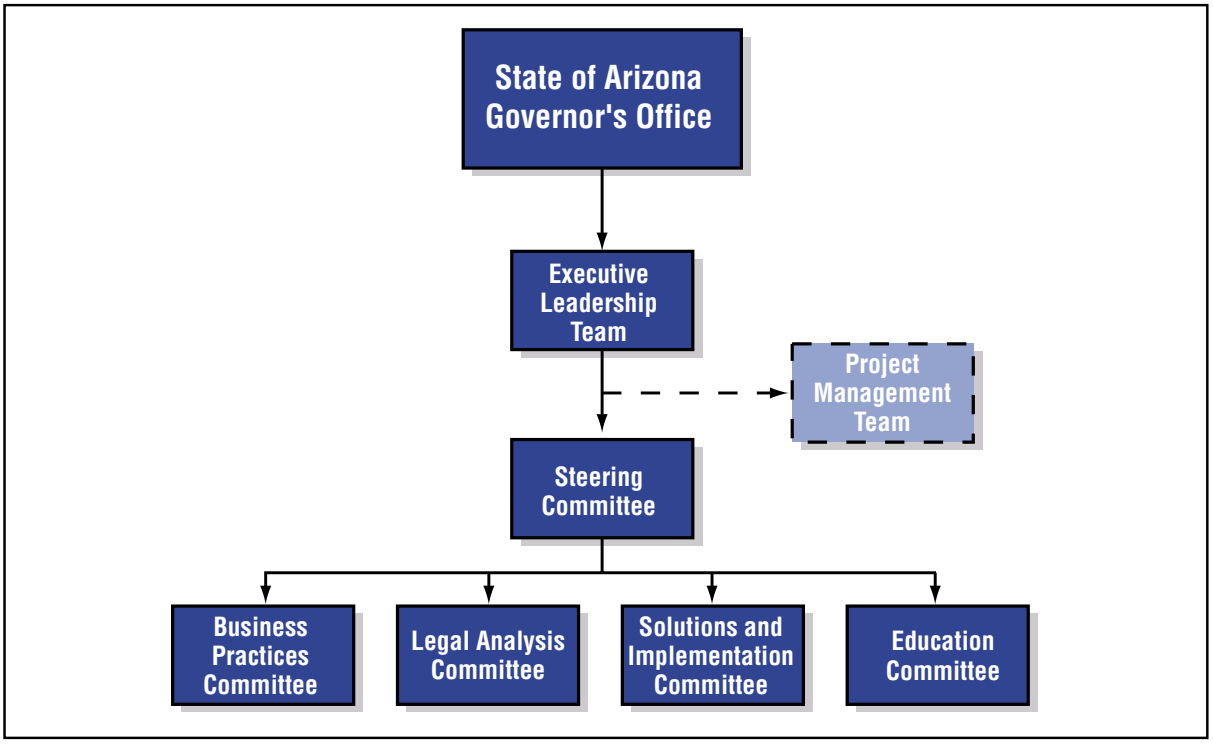
The resolution of many of these challenges will depend greatly on how the e-health information exchange is structured, the type of e-health information to be included, the types of participants in the exchange, and the reasons participants access the exchange. For example, many of these issues will be resolved differently if the exchange involves only limited information, such as medication information or a patient health summary, versus the statewide sharing of health information.

A. Arizona Health Information Security and Privacy Collaboration

In an effort to address the privacy and security issues that will arise during *Roadmap* implementation, the transition effort will leverage the process outlined in Arizona's response to the request from the U.S. Department of Health and Human Services and the National Governors Association for proposals to create a Health Information Security and Privacy Collaboration. The purpose of the Health Information Security and Privacy Collaboration is to identify barriers to e-health exchange in state privacy and security business practices and state laws and regulations, and to suggest methods of alleviating those barriers and encouraging harmonization of privacy and security practices to encourage e-health data exchange.

The Arizona Health Information Security and Privacy Collaboration (AzHISPC) structure (Figure IX) will

Figure IX: AzHISPC Organizational Structure



operate with functional oversight by the Health-*e* Connection Steering Committee. The Steering Committee will be assisted in this effort by four working groups: the Business Practices Committee, the Legal Analysis Committee, the Solutions and Implementation Committee, and the Education Committee.

B. Business Practices Committee

The Business Practices Committee will assess variations in organization-level business policies and practices related to the privacy and security of health information, and categorize them as barriers, best practices, or neutral with respect to interoperability.

C. Legal Analysis Committee

The Legal Analysis Committee will assess applicable privacy and security laws, regulations, and court cases to identify legal sources of barriers to sharing health information statewide. The group will be tasked with reviewing the barriers uncovered in the business policy assessment conducted by the Business Practices Committee and mapping those barriers to applicable privacy and security legal requirements. Members of the Legal Analysis Committee will also work with the Solutions and Implementation Committee (defined below) to ensure that laws are accurately and consistently interpreted throughout the process of formulating solutions, planning, and implementation. In addition to the responsibilities outlined above, the

Legal Analysis Committee will also be responsible for assisting the transition team in answering the legal challenges that arise during the transition phase. (See the Legal Challenges section.)

D. Solutions and Implementation Committee

The Solutions and Implementation Committee will review the assessment of variation of state laws, business policies, and legal requirements identified as barriers by the Business Practices Committee and the Legal Analysis Committee. The committee will develop an implementation plan to recommend policies that are consistent with federal and Arizona laws and will recommend any legislative or regulatory change necessary to reduce state law barriers to e-health data exchange.

E. Education Committee

This committee is expected to conduct outreach and educational sessions about the privacy and security issues involved in e-health data exchange. The committee will also direct other e-health exchange projects to collaborate with regional and national educational efforts as needed.

It is anticipated that the AzHISPC will continue for one year, as outlined in the HHS grant proposal and also as structured in the overall transition plan of the *Roadmap*. Once the governance organization is established during the first year of the *Roadmap*, the governance organization will be responsible for addressing privacy, security, and other legal challenges.

F. Legal Challenges Related to Privacy and Security

The e-health information exchange faces four significant challenges:

1. How will the e-health information exchange address consumers' control over their own health information?
2. How will the e-health information exchange handle "special" health information that has greater confidentiality protection?
3. How will the e-health information exchange handle minors' health information?
4. Who will have access to the e-health information in the exchange and for what purpose?

Challenge 1: How will the e-health information exchange address consumers' control over their health information?

E-health information exchanges across the country face the difficult task of determining how much control the individual consumer will have over his or her health information in the e-health information exchange. On the one hand, consumers legitimately want control over their own health information and want the right to choose whether to participate in a health information exchange.

On the other hand, seeking consumer consent before including health information in the e-health information exchange may mean that an individual consumer may not have the opportunity to consider including his or her information before that information is needed. For example, the person may be in a car accident and treated at an emergency department before the person has the opportunity to opt in to the system, so that person's information will not yet be available electronically to the emergency care providers. In addition, seeking consent of consumers will be an administratively difficult task and may pose substantial expense in implementing the system. Finally, permitting consumers control over participation will diminish the effectiveness of the information exchange in addressing important public concerns, such as using the information in the exchange for bioterrorism surveillance or to alert healthcare providers and public health officials to the beginning of a potential pandemic.

There is no easy answer to this challenge. Moreover, the balance between these positions changes, depending on what type of information is included in the exchange, who has access to the information in the exchange, and for what purposes the information will be available. For example, most consumers may be willing to include medication information in the exchange without consent, but may want the right to consent if a full-blown interoperable electronic health record is created. Similarly, some consumers may be willing to participate in the system if it is accessed only by physicians and hospitals for treatment purposes, but want to authorize access by health plans for purposes unrelated to paying claims for their healthcare.

Weighing the public policy issues above, the e-health information exchange has the following options:

- Seek consumers' consent to include their health information in the e-health exchange.
- Provide consumers the right to opt out of having their health information in the e-health exchange.
- Include all consumers' health information in the e-health exchange.

The Legal Analysis Committee will assist in determining the appropriate option for each e-health data exchange project in the *Roadmap*.

Challenge 2: How will the e-health information exchange handle "special" health information that has greater confidentiality protection?

Some types of health information have greater confidentiality protections than are found in the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, which forms the federal "floor" of confidentiality protection. For example, federal and Arizona laws related to communicable disease, genetic testing, mental health, and alcohol and substance abuse treatment information permit fewer types of uses and disclosures of health information without consumer consent than does the HIPAA Privacy Rule. One of the most challenging decisions facing the e-health information exchange will be how to handle this information. The e-health information exchange has a variety of options:

- The e-health information exchange could exclude communicable disease, genetic testing, mental health, and alcohol and substance abuse treatment information to provide greater confidentiality protection for that information. However, the exchange must examine whether this will be workable, given that this information (particularly communicable disease information) is integrated throughout medical information held by providers. Moreover, segregating that information means that it may not be available to healthcare providers, which may compromise the quality of care provided to the consumer.
- The e-health information exchange could include some sensitive information, but exclude other information that has the greatest restrictions on use and disclosure. For example, the e-health information exchange could include mental health information and communicable disease information (both of which may be disclosed for treatment, payment, quality improvement, research, and public health surveillance), but exclude alcohol and drug abuse treatment information held by federally assisted substance abuse treatment programs and genetic testing information (which may not be disclosed for these purposes without consumer consent). This

option may be workable, if providers holding genetic testing information and substance abuse treatment information can store that information separately from the e-health information exchange.

- The e-health information exchange could include the special information, but restrict the use of *all* information in the exchange to comply with the most restrictive laws. For example, the laws protecting special health information all permit disclosure of the information with consent. The exchange could seek consent to include an individual's information in the exchange, contingent on the individual's agreement to use and disclose all information for certain defined purposes. There are substantial downsides to seeking affirmative consent to include e-health information in the exchange, as explored in connection with the first challenge. Moreover, a consumer may wish all of his or her health information to be included in the e-health data exchange *except* alcohol and drug abuse treatment information; this option would thus force consumers to make a difficult choice between better quality of care and protection of more sensitive information.

- The e-health information exchange could determine a way to flag information that requires more confidentiality protection. This would alert providers that there is additional information in the system, but perhaps not allow access to this information without express authorization from the consumer.

- The e-health information exchange could ask the Arizona Legislature to amend laws to facilitate the e-health information exchange. For example, Arizona confidentiality laws might be amended so that *all* information is subject only to the restrictions in the federal HIPAA Privacy Rule. An alternative might be to reduce the amount of information subject to greater confidentiality restrictions. For instance, the communicable disease laws—which now protect information on all reportable diseases, including flu, measles, and mumps—might be amended to protect only communicable diseases that are stigmatizing to individuals, such as HIV/AIDS.

Challenge 3: How will the e-health information exchange handle minors' health information?

Minors have the right to consent to certain types of healthcare in Arizona, such as treatment for sexually transmitted diseases, HIV testing, alcohol and drug abuse treatment, and prenatal and other reproductive care. Minors also have the right to consent to *all* healthcare if they are emancipated, have been married, are homeless, or are in the military. While minors have the right to consent to healthcare and actually provide that consent, minors also have the right to control the health information related to that care and must authorize disclosure of that information to their parents or guardians. The e-health information exchange should determine how to satisfy the participants' legal obligations to protect minors' rights to control access to their health information. The exchange might consider the following options:

- The e-health information exchange might implement a mechanism for providers to flag information related to healthcare to which a minor consented, but that requires the minor's authorization for disclosure to parents or guardians.

- The e-health information exchange could exclude minors' health information from the system if that information relates to healthcare for which the minor has the right to consent (such as substance abuse treatment, HIV testing, and other types of specific healthcare). Excluding that information may have negative consequences if that information is significant to other treatment provided to the minor.

- The e-health information exchange could request the Arizona legislature to pass a law granting parents and guardians the right to see their children's health information, perhaps with exceptions to protect minors in cases of abuse or other circumstances. However, there are substantial policy reasons that counsel against this route, such as discouraging minors from obtaining treatment for sexually transmitted diseases or prenatal or reproductive care.

Challenge 4: Who will have access to the e-health information in the exchange and for what purpose?

For each e-health data exchange project in the *Roadmap*, the final challenge is to define who has access to the health information for that project and for what purpose. For example, it must be determined whether health plans and employer group health plans will have access to information in a patient health summary. This challenge is closely related to Challenge 1 on whether consumers will have the right to opt in or opt out of having their health information included in the e-health information exchange.

These four challenges — among others — are surmountable, but will require careful consideration based on the policy goals of the e-health information exchange, how the exchange is structured, the type of e-health information to be included, the types of participants in the exchange, and the reasons participants access the exchange.

VII. Finance

Funding for the Arizona Health-*e* Connection should be obtained from a variety of sources, depending on the function. This section considers the funding for HIE, HIT, and a central coordination organization. Each function requires a different approach. Recommendations for each function are listed in the sections below.

It is not necessary to invest large amounts of capital in a central organization to create a top-down funding structure for all Health-*e* Connection exchange activities. This is consistent with the proposed governance roles of the central organization. In fact, many projects will be funded on a case-by-case basis at a medical trading area level. It is anticipated that start-up funding efforts and possible sources for these regional HIE projects could be facilitated by the statewide organization to gain efficiency.

Finally, it is recommended that ongoing operational funding for the core MTA functions and central coordination organization applications be value driven, so that costs for ongoing operations are primarily borne by the organization(s) receiving benefit from the service. It follows that projects will be addressed when it makes economic sense to do so. A principal aim of the Arizona Health-*e* Connection is to create a sustainable business model with users paying for the products and services that they receive — which presumably will be less than what they pay today. As services that support information sharing are introduced and grow, so too will the required financial resource commitment and the complementary service revenues to offset the increased costs.

Costs presented in this section are estimates for the products, organization, and implementation envisioned for the Arizona Health-*e* Connection. They are based on similar products nationwide, research analysis, current level of discovery of the Arizona e-health landscape, and expert opinion. As the Arizona Health-*e* Connection is implemented, changes in scope will impact costing analysis.

A. Central Coordination Organization

A modest budget is recommended for the central organization to coordinate, facilitate, and standardize statewide efforts. As defined in the recommended governance structure for the Arizona Health-*e* Connection, the central organization is relatively small. It will provide staffing, implementation, and support for projects and services that benefit all organizations, making it difficult to assign value to specific organizations.

Since activities of the central organization are designed to promote the common good, funding should be obtained from a central source or sources. Options could include grants and donations, state funds, in-kind donations of staff, and transaction fees. Items such as a secure network, secure messaging, Web portal, clinician directory, and the patient health summary application should be funded centrally. The approximate annual amount of central coordination organization funding required is $3 million to $4 million.

B. Health Information Exchange

The first key HIE service to establish a funding stream is a medical trading area-wide results delivery service, which provides physicians with a single source to order clinical services, generate and confirm referrals, and receive clinical results. The clinical messaging service delivers clinical reports to the treating providers electronically, thereby reducing costs for the healthcare data provider and improving efficiency and utility for the recipient. This service is envisioned to a) be free of charge for the ordering physician and the "copy to" physician, and b) require the organization receiving the order and sending the result to pay the bulk of the costs to the MTA utility on a monthly basis for the service its receives. It is assumed that when the service is completely operational that the current more manual, less reliable results delivery and order processes would be discontinued and that the costs associated with them would be reduced or eliminated. It is further assumed that service levels would noticeably improve for customers and their patients.

The healthcare data providers send clinical reports electronically; the clinical messaging software converts them into a consistent, easy-to-use report format and delivers them to the treating provider. The intent is for new, fee-based services to replace paper-based reports now delivered to physicians by fax, postal mail, or courier. Phone call requests for status tracking information are reduced. Costs to send and receive clinical results are reduced (see Appendix F: Business Case for a discussion of benefits realized at Sonora Quest Laboratories as a result of implementing an electronic system).

Based on cost figures from other results delivery networks, Arizona can anticipate development costs of about $1.5 million to $3 million per one million people (population) over the first two years.

The proposed fees generated by the clinical results delivery service are critical to support the ongoing operations of the MTA and provide expansion of additional data-exchange services such as the MTA master patient index and data transformation (normalization). The cost to maintain each results delivery network and provide these expanded data-exchange services is about $2.5 million to $4 million per year per one million people (population), based on figures from other results delivery networks.

Studies to determine primary beneficiaries of a results delivery service have been initiated. It is believed that information source providers such as labs, hospital inpatient, outpatient and emergency services records, ambulatory surgery centers, imaging centers, etc., have been identified as beneficiaries of the service in the early work of the Clinical and Financial Task Groups. The extent of the benefits and identification of other beneficiaries will be thoroughly studied in future phases of each project.

Service fees may be charged to other organizations legally authorized to receive results on behalf of the patient, such as personal health record (PHR) entities, chronic care improvement programs (CCIP), and disease management (DM) organizations in or outside health plans, insurers, employers, and associations. Fees may be generated for these services based on the value of providing daily batches of information about their patients to their systems (PHR, CCIP, DM) on a per-patient basis.

The patient health summary is a special case as it relates to the decision to develop and sponsor the service to clinicians, care coordinators, emergency physicians, and other authorized users. The beneficiaries of this service, if built for the medical trading area or the central coordination organization, are most frequently the patients. It serves patients well in most cases involving their expressed need (a visit or a call) for medical care. Surveys have shown that in most cases, patients would like to have the clinician as fully aware of their previous conditions and clinical findings as possible. Therefore, the patient or the patient's financial sponsor or guarantor should fund the operation of the patient record summary system that provides this service. Thus, the costs of the system that provides the patient health summary, adds new patients, and provides for the addition and maintenance of clinical event reports, orders, prescriptions, and other records, and the record matching and integrity should be paid by those who benefit.

A financing mechanism for such a system includes a wide variety of financing approaches and formulas. An example is one that levies a fee for each person on the database each month and for the addition of more clinical data and the underlying service support. Thus, a base fee and an index of the degree of value for the additional information for each patient could be charged each month to the guarantor or sponsor of the person/patient. Past proposals have set base fees of between 5 and 10 cents per month, with the index raising the fee to 25 to 50 cents per patient per month at that index level.

The proposed strategy to select appropriate early applications that are easy for healthcare providers to use establishes the foundation for building toward a more comprehensive set of functions, thereby facilitating and expediting the transition of patients, providers, and payers to the benefits that HIT and HIE offer in improving health and healthcare delivery in Arizona. HIE projects provide support to HIT EMRs (interfaces), and HIT EMRs and ePrescribing provide support to HIE projects as patient health summaries are exchanged.

C. Health Information Technology

As envisioned in the HIE section, all clinical practices will receive certain free, basic-level HIE services. Some MTA organizations have offered very low threshold entry fees when referrals or secure messaging services were offered ($10 to $25 per clinician per month).

Figure X lists the proposed basic-level services for clinicians participating in an MTA.

Figure X: Basic-Level Services
Order/receive lab/radiology results Results viewing/printing Physician portal $0 per month per physician

Additional HIT costs should be borne by the organization that is the primary user of any given HIT system. In most cases this will be the clinical practice. Some HIE projects will most likely provide basic HIT extensions to their service offerings to clinicians and other service providers. These extensions can be found in MTAs like HealthBridge and Taconic's MedAllies and includes services such as practice-wide inbox and messaging, referrals, ePrescribing, dictation/transcription, basic charting (forms and templates) or progress notes, patient health summary, and scheduling. These services in many cases are integrated with the HIE software service or interfaced to make it appear seamless. The fees for these services are usually charged as a monthly subscription with transaction modifiers.

Many clinical practices will opt to fund their own deployments of HIT systems. According to the most recent Health Services Advisory Group (HSAG) survey, about 14 percent of Arizona physician practices already have invested in HIT systems and an additional 25 percent plan to invest in the next 12 months. Health and hospital corporations were not surveyed, although their percentage adoption rate of HIT is believed to be even higher. Incentives (such as tax credits, low-cost financing arrangements, and potentially others) should be explored to encourage additional HIT adoption.

An alternative approach for clinical practice will be to purchase, via a subscriber financial model, use of a central system to handle a subset of electronic medical record (EMR) functions. In effect, this is an "EMR-lite" offered through a Web-based system. This approach, commonly used for various business applications via the Internet, is also known as an application service provider model (ASP). If this approach were contemplated, collaboration on interface development and maintenance contracts should be considered, because there are considerable cost and time savings. This approach would also reduce risks of failure from collaboration, interface sharing, or joint development approaches.

The central coordination organization or the MTAs could develop and offer EMR-lite functions. It is also believed that certain vendors would be interested in competing for this work, if outsourcing the function is determined to be appropriate. In addition, it is possible that multiple outsource vendors could develop EMR-lite applications and market the service to clinical practices on a case-by-case basis. For this to occur, outsourced vendors must be required to adhere strictly to Arizona Health-*e* Connection interoperability standards.

Based on a survey of similar services offered nationwide, it is believed that EMR-lite functions could be offered to clinical practices on a tiered cost schedule. Figure XI lists an approximate cost schedule for additional EMR-lite functions.

Figure XI: Costs per Service Levels per Clinician

Intermediate Level of Services	Premium Level of Services
Basic services plus: ePrescribing (price based on number of formularies needed) Messaging/task management Drug-to-drug, drug-to-allergy alerts, etc. $30 to $75 per month per clinician	Basic/intermediate services plus: Referrals Charge capture/right coding Decision support (alerts, best clinical practices, reminders, facilitate diagnoses) Patient education $100 to $250 per month per clinician

D. Cost Summary

The following (Figure XII) summarizes cost estimates for the Arizona Health-*e* Connection as presented in this *Roadmap*. Ongoing and startup costs for HIE, HIT, and the central coordination organization are presented.

Figure XII: Summary of Cost Estimates for Arizona Health-*e* Connection

	Startup Costs	Ongoing Costs/Year
Central Coordination Organization	$3.0 - 4.0 M (year)	$3.0 - 5.0 M*
HIE	$1.5 - 3.0 M (2 years) per 1 million people (population)	$2.5 - 4.0 M per 1 million people (population)**
HIT	0	$3000/clinician***

* = partially self funded (Patient Health Summary)

** = self funded (Results Delivery)

*** assumes EMR-lite premium subscription

VIII. Governance

A. Background

Governance is the process by which an organization establishes strategic direction, makes major decisions, and remains accountable to its stakeholders. HIE involves cooperation, collaboration, and compliance from a large number of diverse participants (e.g., clinicians, health service providers such as hospitals and laboratories, employers and purchasers, health plans, health departments, and even patients themselves). Securing the trust and active engagement of stakeholders while achieving the goals of the Arizona Health-*e* Connection *Roadmap* requires a representative, effective, and resilient governance process.

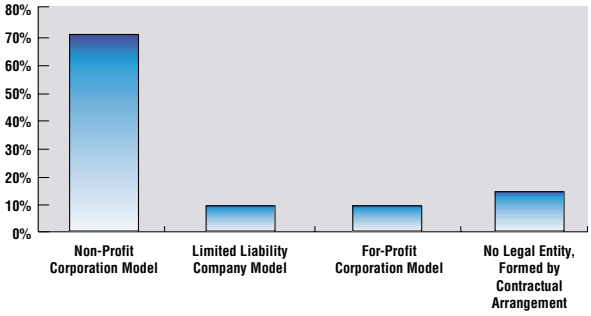
There is no single correct organizational structure for health information exchange efforts. Various models include government authorities, membership and non-membership nonprofit organizations, private for-profit firms, cooperatives, and contractual agreements with an academic institution, among others.

A 2005 survey conducted by the eHealth Initiative found that health information exchange efforts are maturing and some communities have developed multiple corporations to accomplish various parts of their missions (e.g., adding a wholly owned subsidiary limited-liability corporation to a nonprofit corporation). For initiatives that have created a formal legal organizational structure, 70 percent use a nonprofit corporation model (Figure XIII).[2]

The survey also shows a clear shift toward leadership by a neutral, multi-stakeholder entity, with 55 percent of respondents indicating that their initiatives are led by a multi-stakeholder organization.

Arizona's model establishes a clear mission, organizational principles, and governance structures to ensure sustainable adoption. One of the most important aspects of governance is coalition and trust building among the stakeholders.

Figure XIII: Nature of Health Information Exchange Initiatives



B. Getting Started

Discussions with key stakeholders, Steering Committee members, Governance Task Group members, and public meeting attendees indicated a strong preference for health information initiatives to be led by a neutral, diverse, and trusted governing body. Many other successful initiatives have come to the same conclusion. Given the fragmented and highly competitive nature of our healthcare system, building trust among these diverse entities requires a great deal of process and attention.

Although there is need for statewide leadership and coordination, much of the work will be done at the local and regional levels. Most of the day-to-day benefits of information exchange accrue inside individual medical trading areas. This is where stakeholders have the greatest need for one another's information and enjoy the trust enabled by face-to-face interaction. From both business case and governance perspectives, early exchanges and innovation are most likely to emerge at the local and regional levels.

Arizona has a good track record in developing successful and sustainable public-private collaborations, the structure proposed for Arizona's Health-*e* Connection initiative. The involvement of consumers is critical to the success the *Roadmap* implementation. To ensure buy-in, consumers will be integrated into existing and planned committees and task forces.

C. Governance Task Group Recommendations

The following Governance Task Group recommendations are detailed below:

- Mission statement
- Model governance structure for a statewide e-health information infrastructure
- Roles and responsibilities of a governance structure

Mission Statement

"To facilitate the design and implementation of integrated statewide health data information systems that support the information needs of consumers, health plans, policymakers, providers, purchasers, and researchers and that reduce healthcare costs, improve patient safety, and improve the quality and efficiency of healthcare and public health services in Arizona."

Statewide Governance Model

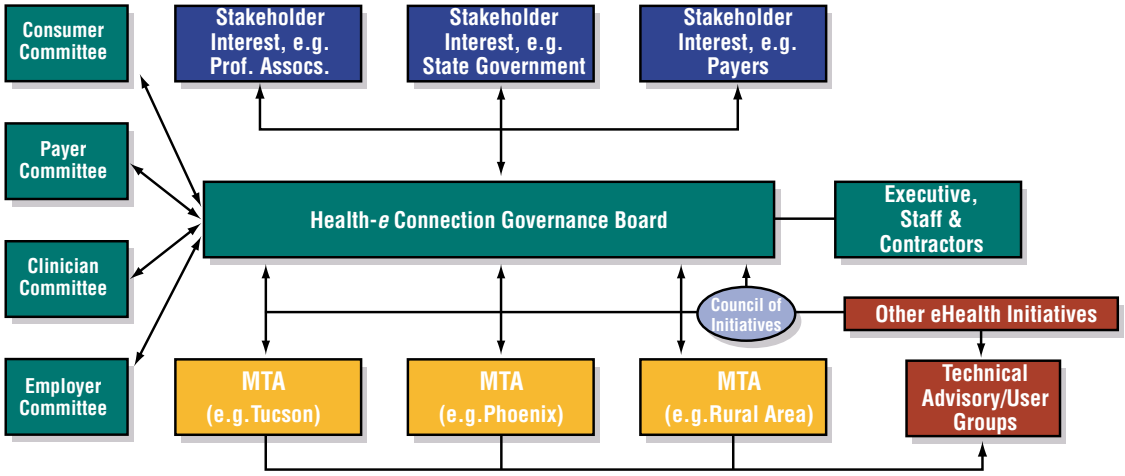
To accomplish the mission of the Arizona Health-*e* Connection initiative, a governing body is to be established that will:

- Include representatives of critical statewide stakeholder interests (e.g., government entities)
- Include representatives of local medical trading areas
- Promote interoperability and national standards
- Ensure security and privacy needs are met
- Allow those who contribute data to have a say in how data is used
- Be positioned to accept and spend both government and private funds
- Promote solutions that reach across geographical, demographic, and organizational boundaries
- Effectively attract and retain participants
- Clearly define roles and responsibilities of the public-private collaborative

A statewide governance body is needed to develop a uniform approach to all aspects of *Roadmap* implementation. It is recommended that a statewide nonprofit Health-*e* Connection corporation be created to provide leadership, negotiate standards, and encourage collaboration. This organization would strategically collect and distribute funding, align financial incentives, develop statewide technical infrastructure when needed, and advocate for needed policy changes.

A private-public, nonprofit organization is recommended to serve as a coordinating body, to provide leadership and guidance, and to drive collaboration. The organization could also assume key roles in areas such as providing funding, aligning financial incentives, developing technical infrastructure, and driving needed policy changes. It is recognized that no current organization fulfills these requirements. The adopted governance model is propelled by local and regional initiatives supported by a statewide process. The model consists of a governance board, board committees, full-time supporting staff, a Council of Initiatives, and technology advisory groups. The proposed structure is depicted in Figure XIV.

Figure XIV: Proposed Arizona Governance Structure



Governance Board

A board will be established to be the core entity of the governance body. It will maintain and refresh the coherent vision, strategy, and outcome metrics underpinning the *Roadmap*. It will provide advocacy and build trust, buy-in, and participation of major stakeholders. In addition, the board will assure equitable and ethical approaches in implementing the *Roadmap*. It may also raise, receive, manage, and distribute state, federal, and private funds. It will prioritize and foster interoperability for statewide and sub-state initiatives. Finally, it will implement statewide projects and facilitate local and sector projects.

The concept of a membership dues-driven, nonprofit organization was considered but discarded because the Health-*e* Connection corporation must represent all interests, regardless of whether individual organizations see fit to participate at any particular time. Instead, a small but committed board must be empowered to act aggressively on behalf of all state residents while balancing the interests of critical stakeholders. Similarly, the concept of a para-state organization (such as a government authority) was considered but discarded, given the need to assure substantial investment and ownership by both the public *and* private sectors, and the need for agile decisions and actions to implement a complex, ever-changing task.

It is recommended that the governing board consist of 15 to 20 members.

Statewide Stakeholder Representatives

The governance board will contain representatives from critical statewide stakeholder interests including:

- Employers
- Health plans/payers
- Healthcare clinicians
- Arizona state government agencies
- Consumers
- Public health
- Laboratories
- Pharmacies
- Hospitals

In some cases, associations can appoint representation of interests statewide. In other cases, it will be necessary for the Governor (e.g., government agencies) or existing board members (e.g., consumers) to select individual board members to represent particular stakeholder groups and to ensure that the board represents a diverse cross section of Arizona residents.

The bylaws of the Health-*e* Connection corporation will need to detail these selection processes. This will involve an additional level of detail and would be negotiated by the Transition Team discussed below.

MTA Representatives

Because the participation of statewide and regional (MTA) exchanges is crucial, each MTA health information exchange would also be represented on the board. MTA health information exchanges are distinguished from other types of e-health projects by being:

- A single entity for exchange of clinical information inside a geographic medical trading area on all patients, regardless of payer or provider system
- Open to all clinicians and service providers in the MTA who agree to necessary participation conditions
- Committed to collaborating with the Health-*e* Connections board and other MTA health information exchanges on statewide information exchange
- Committed to adopting statewide policies and standards
- Governed by structure that permits participation by local clinicians and service providers
- Able to assume the roles and responsibilities detailed in Figure XV

Board Committees

A modestly sized board cannot include representation from all important stakeholder groups and contain all the technical, clinical, legal, and policy expertise required. Board committees will be established to broaden both input into and expertise on the governance process. Each committee will be chaired by a board member.

Board committees will permit recruitment and input by an even broader set of stakeholders, as well as content expertise in areas such as clinical problem-solving, technical architecture, standards, finance, and confidentiality and security concerns. Four standing committees will represent clinicians, payers, employers, and consumers. In addition, technical advisory/user groups and a Council of Initiatives will address specific implementation issues confronting health information exchange initiatives.

Full-Time Staff

The Health-*e* Connection board should be supported by a full-time executive and supporting staff. Contractors may also be used to supplement the skills of the full-time employees. The staff would execute strategic, business, and technical plans. Staff would also coordinate day-to-day tasks and deliverables, including establishing contracts and participation with local and regional initiatives.

Council of Initiatives

Participants of the many e-health initiatives under development in Arizona (including those operating on a scale below the MTA level) could join a Council of Initiatives to help identify obstacles and common solutions for future interoperability of information systems. The council would send representatives to the board to contribute expertise and advice. It would also help select representatives to technical advisory/user groups.

Technology Advisory Groups

Technology advisory groups will provide MTAs and other interested parties a forum to explore technical standards, policies, and solutions to common problems facing multiple MTAs (e.g., user identity management and secure messaging). From these discussions, standards, policies, and solutions will be proposed to the governance board. In addition, the advisory groups will be a forum to openly share knowledge and solutions across projects and the larger Health-*e* Connections community.

Roles and Responsibilities of Proposed Governance Structure

The following (Figure XV) summarizes the responsibilities of each entity in the above diagram.

Figure XV: Roles and Responsibilities of Proposed Governance Structure

Governance Role	Responsibility
Governance Board	• Develop vision, strategy, outcome metrics, and technical and business plans • Build trust, buy-in, and participation of major stakeholders • Assure equitable and ethical approaches • Approve statewide policies, standards, and agreements • Balance interests and referee or resolve disputes • Raise, receive, manage, and distribute state, Federal, and private funds • Foster interoperability for statewide and sub-state initiatives • Implement statewide projects and facilitate local/sector projects • Provide financial and legal accountability, compliance, and risk management • Educate and market
Statewide Stakeholder Representatives	• Be credible representatives of their sectors • Offer needed participation in decisions and projects • Offer expertise and advice
Medical Trading Area (MTA) Representatives	• Serve as subset of e-health projects working toward exchange, including all willing participants in a geographic area • Recruit and build trust, buy-in, and participation of project participants; implement projects • Send credible representatives to the Statewide Board • Select representatives to technical advisory/user groups • Provide financial and legal accountability, compliance, and risk management for their initiatives
Board Committees	• Broaden the number of stakeholder representatives involved • Provide content expertise in specific areas of concern to the board • Serve as standing committees representing clinicians, payers, employers, and consumers
Executive, Staff, and Contractors	• Execute strategic, business, and technical plans • Coordinate day-to-day tasks and deliverables • Establish contracts and other relationships with local and sector initiatives • Provide industry knowledge • Measure and report meaningful outcomes • Establish participation agreements • Provide fiduciary and compliance accountability
Council of Initiatives	• Serve as meeting place for all interested e-health projects, including those with a more limited scale than MTAs • Offer shared learning and recruitment into projects serving Health-*e* Connection goals • Select one or more representatives to Statewide Board to contribute expertise and advice • Help select representatives to technical advisory/user groups
Technical Advisory/ User Groups	• Serve as forums to explore and propose technical standards, policies, and solutions to common problems facing multiple MTAs (e.g., user identity management and secure messaging) • Propose standards, policies, and solutions to Statewide Board • Openly share knowledge and solutions across projects and larger Health-*e* Connections community

IX. Transition Plan

The transition plan explains how the *Roadmap* will begin to be implemented during the first 12 months. It lays out the process for establishing the statewide governance organization, implementing early stages of the HIE infrastructure, and partnering with strategic HIT systems or initiatives. The transition also requires activities of the AzHISPC organization dealing with privacy, security, and legal questions in implementing the *Roadmap*. For more information about AzHISPC and its activities, see the section on Privacy and Security.

The first activity during transition is to finalize the transition structure, which includes selecting interim leaders, obtaining commitments from the participants, identifying interim funding requirements, and obtaining the funding. Obtaining commitments from participants should take no more than one month. Identifying interim funding requirements and securing the funds must then occur to avoid a vicious cycle of inactivity and discouragement. Transition participants will focus on:

- Establishing the governance corporation, draft strategic and business plans, and model participation agreements
- Developing a practical strategy for statewide and MTA engagement in the Health-*e* Connection effort
- Implementing early statewide HIE infrastructure (e.g., the secure portal)
- Identifying and coordinating with current Arizona HIT initiatives
- Developing a marketing and education plan for *Roadmap* implementation

Statewide Governance Organization

Critical transition activities are to incorporate and define bylaws for the governance body and ensure that core board members are recruited and appointed. It may also be necessary to position the board to operate effectively by arranging for interim executive staff and required contractors.

Once the governance body is established, it will develop a detailed strategic and business plan. The business model needs to be flexible enough to evolve to support changes in the healthcare industry (e.g., pay for performance) and changes in the local community (e.g., local business leadership changes as the initiative gains momentum). It is impossible on day one or even in year one to say what the sustainable model will be. The Health-*e* Connection approach is to plan, implement, and continuously evaluate and refine the model.

Another early task for the governance body is to develop model participation agreements to govern how the individuals or entities granted access to the e-health information exchange may access, use, and release the data in the exchange. These agreements will need to address a host of issues, such as authentication of users, security requirements for participating systems to ensure confidentiality of the information, the reasons participating individuals and entities may access data in the exchange, who has the right to grant access to consumers, and who has the right to amend information in the exchange. The agreements also will need to address the difficult issue of allocating risk and liability through indemnification and insurance provisions, and how participants will be sanctioned or disciplined for misuse of the system. The development and negotiation of these participation agreements will be time intensive because they must reflect participant consensus on a wide variety of issues. Final agreements will be developed as the e-health data exchange projects are refined.

Strategy for Statewide Engagement

It is important to engage various regions and audiences in Arizona to implement the *Roadmap*. One of the first activities is establishing an Arizona map of medical trading areas (MTAs), including demographic information (population, numbers of providers of various types, etc.) and taking account of cross-jurisdictional questions (e.g., Mexico, Nevada, California, etc.). The map will also include overlays of demographic information, such as the HHS Indian Health Service, the U.S. Department of Veterans Affairs, and professional association membership. The maps will become a part of the communication plan and will also be posted on the state portal. The goals are to help everyone recognize the scale of what is happen-

ing, establish the base for a full licensee/provider directory over time, and demonstrate progress.

Once the MTAs are identified and described by the overlay maps, the transition team will identify a viable approach for engaging MTAs, including a template of requirements to establish a formal information exchange. The transition team will approach groups that are currently organized and assist them in establishing a formal data exchange within their MTA.

HIE Initiatives

An important objective of the transition plan is to maintain the momentum that Governor Napolitano created when she asked for the creation of the *Roadmap*. Part of the strategy is to quickly implement some of the early HIE initiatives, including the development of a secure communications infrastructure. The activities for establishing a secure communications infrastructure include:

- Setting up a participation structure (e.g., hospitals, labs, payers, and other organizations that will benefit) and developing consensus about overall technical approach
- Identifying potential suppliers for the technical approach
- Developing technical designs
- Selecting project approaches for viable technical designs, including cost projections and funding possibilities
- Developing a Web portal strategy. Activities associated with creating the strategy include:
    - Identifying potential suppliers
    - Developing a conceptual design
    - Developing a project approach
    - Identify portal operation support
    - Obtaining funding
    - Implementing the portal

Perhaps one of the more challenging HIE initiatives during the transition phase is developing an MTA results delivery strategy. This includes identifying guidelines for regional governance, oversight mechanisms, and results reporting. It will also include funding strategies and a guidebook to establish the service.

HIT Initiatives

An important strategy to implement the *Roadmap* is to leverage strategic HIT systems. During the *Roadmap* development process, some HIT systems were identified as having potential strategic importance to the *Roadmap*. There may be additional HIT systems that could be leveraged. Therefore, an early HIT strategy is to identify and work with HIT systems that will help move the goals of the *Roadmap* forward. Activities related to this effort include:

- Conducting an HIT/HIE survey or inventory
- Determining information to publish on the portal for HIT adoption
- Establishing ongoing liaison with identified HIT projects
- Obtaining funding and staffing as necessary

Marketing and Education Plan

The following marketing and education items are the responsibility of the transition structure for the Arizona Health-*e* Connection. These responsibilities will most likely be absorbed into the permanent governance structure after it is established.

The responsibilities listed are critical to maintain project momentum and to generate additional enthusiasm at local and regional levels. In addition, it is critical to maintain resources to respond to public inquiries and public relations opportunities.

Activities to be listed in the marketing plan include:

- Developing standard presentations
- Advocating key implementation components (when needed)
- Establishing and training a speakers bureau
- Establishing media contacts

- Developing a media plan
- Distributing a quarterly newsletter
- Assisting the Governor's office (as requested) in the release of the *Roadmap*
- Reaching out to key stakeholders (especially rural constituencies)
- Maintaining a contact database
- Partnering with existing groups such as Doctor's Office Quality–Information Technology (DOQ-IT), Health Information and Management Systems Society (HIMSS), and Arizona Health Information Technology Accelerator (AHITA) for additional marketing coverage

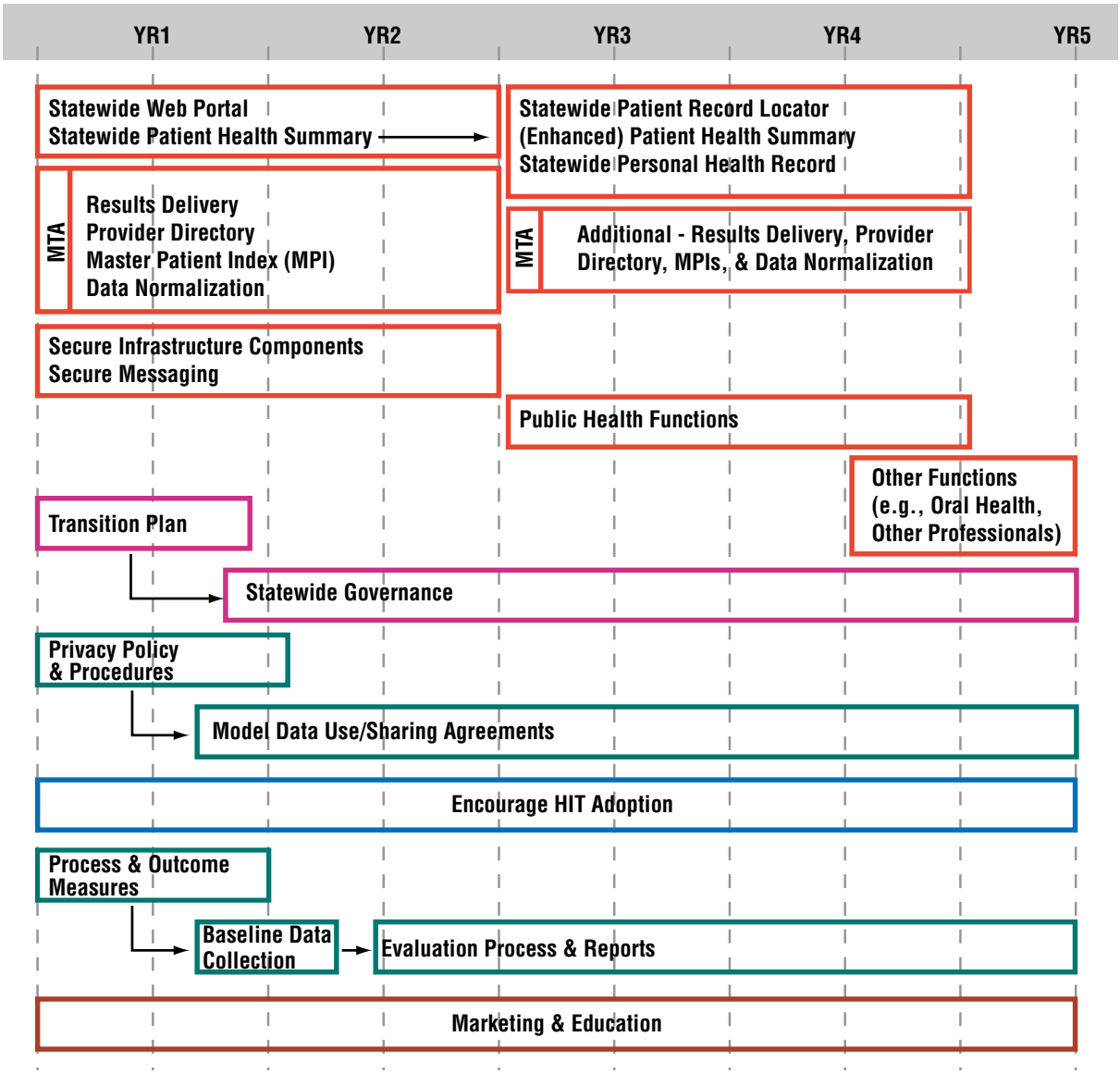
In addition to the marketing plan, an education plan needs to be developed to give specifics for participating in the initiative. Activities related to an education plan include:

- Organizing workshops for initial projects (such as results delivery)
- Assisting in coordinating grant and funding opportunities with statewide, regional, and local organizations
- Continuing to develop talent to serve as implementation leaders
- Supporting and exchanging industry knowledge such as lessons learned and best practices
- Assisting statewide, regional, and local organizations in obtaining assistance from national experts
- Advocating key implementation components (when needed)
- Developing materials to help communities and regions get started
- Expanding education opportunities by partnering with existing groups such as Doctor's Office Quality–Information Technology (DOQ-IT), Health Information and Management Systems Society (HIMSS), and Arizona Health Information Technology Accelerator (AHITA) for additional educational resources

X. Project Timeline

Roadmap implementation involves accomplishing many activities concurrently. In addition, some activities depend heavily on others. The following diagram (Figure XVI) provides a picture of the timing of activities in relationship to each other.

Figure XVI: Project Timeline



XI. Implementation Summary

The *Roadmap* contains actionable items that will enable Arizona to reach critical milestones on the road to fully sharing healthcare information throughout the state. Many specific activities will take place over the next five years to enable Arizona to exchange healthcare data statewide. The diagram on the preceding page shows a timeline of the most critical activities. The following chart (Figure XVII) highlights those same activities by year. Full implementation of these activities will enable Arizona to realize the benefits of electronic health data exchange and to be recognized as a national leader for its efforts to establish a virtually connected healthcare environment.

Figure XVII: Implementation Milestones by Year

Year	Milestones/Activities
1	• Establish Health-*e* Connection governance body • Develop statewide business plans • Develop model participation agreements • Identify and establish baseline measures of Health-*e* Connection outcomes • Identify and approach Arizona MTAs • Establish the first MTA information exchange with a results delivery service - Develop a provider directory - Begin a master patient index (MPI) - Begin data transformation • Develop Arizona's statewide Web portal with security infrastructure components • Pilot a basic patient health summary • Establish HIT adoption plan • Market and educate the healthcare community about Health-*e* Connection
2	• Provide guidance to first MTA information exchange for enhanced services • Establish other MTA information exchanges with results delivery services (including provider directories, master patient indexes, and data transformation) • Implement secured messaging • Obtain Health-*e* Connection outcome measurements • Encourage HIT adoption
3	• Establish and provide guidance to MTA information exchanges with results delivery services (including provider directories, master patient indexes, and data transformation) • Enhance the patient health summary with data from MTAs • Enhance public health functions • Obtain Health-*e* Connection outcome measurements • Encourage HIT adoption
4	• Establish and provide guidance to MTA information exchanges with results delivery services (including provider directories, master patient indexes, and data transformation) • Enhance the patient health summary with data from MTAs • Implement statewide patient locator • Develop statewide personal health record access • Obtain Health-*e* Connection outcome measurements • Encourage HIT adoption
5	• Enhance the patient health summary with data from MTAs • Add functions for oral health and other healthcare professions • Obtain Health-*e* Connection outcome measurements • Encourage HIT adoption

XII. Acknowledgements

Creation of the Arizona Health-*e* Connection *Roadmap* would not have been possible without the contributions of the following individuals. Their knowledge, input, assistance, and spirit of dedication and teamwork were essential to successful completion of Governor Napolitano's Executive Order. The content presented in this *Roadmap* is a direct result of literally thousands of hours of volunteered time.

Steering Committee

Co-Chairs:

Chris Cummiskey	Government Information Technology Agency
Beth Schermer	University of Arizona College of Medicine

Members:

Joe Anderson	Schaller Anderson
Reg Ballantyne	Vanguard/Abrazo Health Care
Betsey Bayless	Maricopa Health District
Bill Bell	Arizona Department Of Administration
Bruce Bethancourt, M.D.	Banner Health
Richard Boals	Blue Cross Blue Shield
Leslie Bromberg	Bromberg Consulting Inc.
Joe Coatsworth	Arizona Association of Community Health Centers
Benton Davis	United Health Care
Crane Davis	Arizona Pharmacy Association
Don Davis	Indian Health Service Plans
Jack E. Davis	Arizona Public Service
Mark El-Tawil	Healthnet
John Fears	U.S. Department of Veterans Affairs
Peter Fine	Banner Health
Susan Gerard	Arizona Department of Health Services
Bernard Glossy	Delta Dental
Wyllstyne Hill	Raytheon
Roger Hughes	St. Luke's Health Initiatives
Linda Hunt	St. Joseph's Hospital & Medical Center
Mark James	Honeywell Aerospace
Jack B. Jewett	TMC HealthCare
David Landrith	Arizona Medical Association

Celeste Null	Intel
Kathleen Oestreich	University Family Care/University Physicians Healthcare Group
Kathleen Pagels	Arizona Health Care Association
Sethuramen Panchanathan	Arizona State University School of Computer Science
Greg Pivirotto	University Medical Center Corporation
Rick Potter	Health Services Advisory Group
Patt Rehn, R.N.	Arizona Nurses Association
John Rivers	Arizona Hospital and Healthcare Association
Anthony D. Rodgers	Arizona Health Care Cost Containment System
Phyllis Rowe	Arizona Consumers Council
Michael Sherman	Salt River Project*
Richard Silverman	Salt River Project
Jim Sinek	Verde Valley Medical Center
Christina Urias	Arizona Department of Insurance
Wendy Vittori	Motorola
Michael Warden	Banner Health*
Amanda Weaver	Arizona Osteopathic Medical Association
Ronald S. Weinstein, M.D.	University of Arizona College of Medicine
Gerald Wissink	BHHS Legacy Foundation

*Substitute member

Executive Leadership Team

Chris Cummiskey	Government Information Technology Agency
Roger Hughes	St. Luke's Health Initiatives
Anthony Rodgers	Arizona Health Care Cost Containment System
Beth Schermer	University of Arizona College of Medicine
Anne Winter	Governor Napolitano's Office

Task Group Leadership Team

Clinical Task Group

Chair:	Bruce Bethancount, M.D.
Facilitator:	Seth Foldy, M.D.
Staff:	Andy Miller/Chris Muir

Technical Task Group

Chair:	Eric Dean
Facilitator:	Paul Biondich, M.D.
Staff:	Chris Muir

Financial Task Group

Chair:	Rick Potter
Facilitator:	Jay McCutcheon
Staff:	Elizabeth McNamee

Legal Task Group

Chair:	Kristen Rosati
Facilitator:	Bill Braithwaite, M.D.
Staff:	Andy Miller

Governance Task Group

Chair:	David Landrith
Facilitator:	Seth Foldy, M.D.
Staff:	Lorie Mayer

eHealth Initiative and Partners

Paul Biondich, M.D.
Bill Braithwaite, M.D.
Seth Foldy, M.D.
Janet Marchibroda
Jay McCutcheon
Katie Sawyer
Emily Welebob

Project Management Team

David Engelthaler
Lorie Mayer
Elizabeth McNamee
Andy Miller
Chris Muir
Kristen Rosati
Harvey Shrednick
Emily Welebob

Task Group Membership

Nancy Abell
Richard Adams
Ken Adler, M.D.
Rep. Amanda Aguirre
Desh Ahuja
Deniz Akinc
Sheena Albright
Sarah Allen
Anna Alonzo
Jason Attakai
Wade Bannister
Leila Barraza
Mary Jean (MJ) Barrett
Tim Barrett
Kevin Basso
Laura Bazzill
Scott Beatty
Lori Bedford
Mary Benhase
Wendy Benz
Mona Berkowitz
Ira Berkowitz
Bruce Bethancourt, M.D.
Tom Betlach
Jack Beveridge
Mark Bezjian

Kalyanramon Bharathan
Paul Biondich, M.D.
Rick Blankinship
Ken Bobis
William Bonfield, M.D., M.P.H.
Bill Braithwaite, M.D.
John Braswell
John Brimm, M.D.
Tom Brink
Leslie Bromberg
Kathy Byrne
Andrea Cabrera
Laura Carpenter
Michael Carter
Barry Cassidy, M.D.
Pete Cerchiara
Gordon Chagrin
Ricardo Chavez
David Clark
Susan Cobb
Barbara Cohen
Daniel Cohen
Darrell Contreras
Joshura Cork
Van Cosby
Jim Cramer
Bradford Croft, D.O.
Chris Cronberg
Robert Crossley
Sandra Davidson
Byron Davies
Jack Davis
Mary Davis Doyle
Eric Dean
Django Degree
Linda Deiley
Deborah Dennis
Matt Devlin
Kevin Dolan
Robert Dowd
Roger Downey
Andy Draper
Paula Dunn
Judith Effken
Mark Emery
Scott Endsley, M.D.
Dave Engert
Edie Faust
Bill Fink
Angela Fischer
Sharon Flanagan-Hyde
Jeff Flick
Seth Foldy, M.D.
Chris Fonner
Brian Foster
Don Foster
Richard Fox
Robin Furlong
Rita Gangi
Margaret Garcia
Amy Gelliffe, M.D.
Sue Gerard
Denice Gibson
Katy Gilbert
Michael Gleason
Michal Goforth
Nathan Goldberg
David Gregg Gordon
Janet Gordon Kennedy
Louis Gorman
Martin Goslar, Ph.D.
Kimiko Gosney, M.S.
Alan Grobman, M.D.
Julie Hale
Francine Hardaway
Phil Harrington
Kim Harris-Salamone
Eric Hedlund
Patricia Henrikson
Barbara Hess
Michelle Hindman
Joyce Hospodar
Jim Houtz
John Hoyt
Alison Hughes
Becky Hull
Minu Ipe
Carol Iverson
Doug Jaeger
Bruce Jameson
Karen Jiggens
Bill Johnson
Dana Johnson
Julie Johnson
Mary Beth Joublanc
Jack Keane
Michael Keeling
Kenneth Kelley
David Kempson
Leonard Kirschner, M.D.

Jeremy Klages
Glen Klineer
Penny Knochenhauer
Sharon Kocher
Ken Komatsu
Mary Kopp
Uday Kulkarni
Connie Lagneaux
David Landrith
William Larkin
Mary Jo Laufenberg
Jim Lauves
Chuck Lehn
Marc Leib, M.D.
Lee Lemelson
Steve Lieber
Denise Link
Thomas Lites
Nicki Lovejoy
Kathy Malloch
Jeannie Marino
Lorie Mayer
Joel McAldruff
Brian McAnallen
Mark McCourt
Lisa McCoy
Sue McCoy, R.N.
Jay McCutcheon
Mike McHale
Ted McKever
Elizabeth McNamee
Terry McPeters
J. McVey
Thomas McWilliams, D.O.
Manjula Mellacheruvu
Linda Melton
Laura Meyer
Chris Meyers
Joe Miglietta
Samuel Miller
Andy Miller
Darrell Mills
Bevey Miner
Mark Moehling
Susan Morley
Zach Mortensen
Bruce Mortenson
Chris Muir
Anita Murcko
Tina Naugle
John Nelson
Debbie Nixon
Susan Noack
Richard Noll
Laura Norquist
Celeste Null
Michael O'Hara
Christopher Oliver
Josh Padnick
Kathleen Pagels
Norma Peal
Gregory Pendergrass
Stan Person
Bonnie Petterson
Bill Pike
Debi Pomeroy
Richard Porter
Radi Ann Porter, R.N.
Tracy Post
Rick Potter
Deborah Prokop
Michael Prudence
Sally Reel
Patt Rehn, R.N.
Jay Resio
Chuck Revenew
Bart Rippenger, D.P.M.
John Rivers
Tony Rodgers
Anne Romer
Kristen Rosati
David Runt
Mary Rybka, R.H.I.T.
Scott Sadler
Russ Savage
Katie Sawyer
Sandra Schindler
Christopher Sedor
Enrique Serna
Paul Shannon
Ben Shao
John Sheldon
Michael Sherman
Harvey Shrednick
Jenn Simmon
Cynthia Smith
Steve Smith
Julie Smith David
Marshall Smith, M.D., Ph.D.
Jared Smout

Dan Soule
Sydney Standifird
Mike Stearns
Christine Steigerwald
Steven Steinberg
Sylvia Stock
Randy Stone
Pam Stott
Linsy Strait
John Swagart
Holly Swenson
Dave Syposs
Matt Taylor
Liz Temple M.P.A., J.D.
Marilyn Teplitz
Roy Teramoto
Kay Thompson
Micheal Toomey
Gail Ulan
Peach Unrast
Tom Updike, M.D.
Iris Villarreal
Geoffrey Walton
Jim Wang
Todd Watkins
Rita Weatherholt
Amanda Weaver
Jack Weiss, M.D.
Emily Welebob
Kathy Wells
Bruce Werber, D.P.M.
Liddy West
David Woodcock
Joe Yelanich
Lon Yo
Ping Zhang
Judy Zimmet

XIII. Appendices

Appendix A: Governor's Executive Order

Executive Order 2005- 25
Arizona Health-e Connection Roadmap

WHEREAS, on April 12, 2004 President Bush called for widespread adoption of interoperable electronic health records (EHRs) within 10 years and established the Office of the National Coordinator for Health Information Technology (ONCHIT); and

WHEREAS, ONCHIT issued a ***Framework for Strategic Action: The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care,*** (the "***Framework***") outlining four requirements for achieving the President's goal of widespread adoption of health information technology (HIT), including the need to: 1) develop interoperability standards; 2) support and encourage the development and use of EHRs and electronic data exchange infrastructure; 3) establish policies and regulation consistent with these goals and information security requirements; and 4) create an Internet-based architecture for nationwide health information exchange; and

WHEREAS, the ***Framework's*** goals are consistent with those of the State of Arizona to achieve 100% electronic health data exchange between payers, health care providers, consumers of health care, researchers, and government agencies as appropriate; and

WHEREAS, the federal Department of Health and Human Services (DHHS) estimates that savings of $140 billion per year, or close to 10% of total health spending in the United States, could be achieved through HIT by reducing duplicative care, lowering health care administrative costs, and avoiding errors in care; and

WHEREAS, the federal government intends to financially support local and statewide initiatives aligned with federal efforts to achieve the President's HIT goals; and

WHEREAS, Arizona recognizes that early adoption of a statewide e-health information infrastructure would improve the quality and reduce the cost of health care in Arizona by: 1) ensuring health information is available at the point of care for all patients; 2) reducing medical errors and avoiding duplicative medical procedures; 3) improving coordination of care between hospitals, physicians, and other health professionals; 4) furthering health care research; and 5) providing consumers with their own health information to encourage greater participation in their own health care decisions; and

WHEREAS, Arizona must control health care costs as a key to a long-term strategy of reducing state expenditures and enhancing the business environment for both large and small employers; and

WHEREAS, a statewide e-health information infrastructure must be organized and structured in a manner to protect the privacy and security of health information; and

WHEREAS, establishing an Arizona Health-e Connection Roadmap will guide legislative and regulatory actions, encourage coordinated efforts in the private health care sector, further public and private partnerships for the development of a statewide health information infrastructure, and maximize federal financial participation to support the goal of early adoption of an e-health information infrastructure;

NOW, THEREFORE, I, Janet Napolitano, Governor of the State of Arizona, by virtue of the authority vested in me by the Constitution and laws of this State, hereby order and direct as follows:

1. The Director of the Government Information Technology Agency ("GITA") shall convene a Call to Action Summit of health care industry executives, technology leaders, content experts, major employers, community leaders and interested government agencies within sixty (60) days of the execution of this Order to solicit input and participation in the creation of an e-health information infrastructure for Arizona.

2. There is hereby created a Steering Committee for Arizona Health-e Connection (the "Steering Committee"). The Steering Committee shall be chaired by the Director of GITA and shall comprehensively review issues surrounding the creation of an e-health information infrastructure in Arizona and develop guidance (to be known as the "Arizona Health-e Connection Roadmap") for the users of such infrastructure.

3. Members of the Steering Committee shall be appointed by, and serve without compensation at the pleasure of, the Governor. The Steering Committee shall include representatives from:
   - Major employers
   - Health plans
   - Physician community
   - Hospitals and hospital systems
   - Healthcare foundations and organizations involved in e-health information
   - Healthcare Associations
   - Arizona Health Care Cost Containment System
   - Arizona Department of Health Services
   - Arizona Department of Administration
   - Arizona Department of Insurance
   - Arizona Universities
   - Health information, privacy and security content experts

3. Task groups within the Steering Committee shall be formed to develop recommendations for:
   - Identifying existing e-health resources, including funding sources, to support the development of a statewide e-health information infrastructure;
   - Identifying technology options, and their advantages and disadvantages, for a statewide e-health information infrastructure;
   - Identifying options for serving consumer health information needs;
   - Ensuring health information privacy and security in electronic health information exchange;
   - Facilitating statewide adoption of electronic health record standards to enable health information exchange across the state and nationally; and

- Creating organizational and governance structures for a statewide e-health information infrastructure.

4. The Steering Committee shall explore funding options for the cost of developing the Arizona Health-e Connection Roadmap and the subsequent development of an e-health information infrastructure for Arizona.

5. No later than one hundred eighty (180) days following the Call to Action Summit, the Steering Committee shall submit to the Governor the Arizona Health-e Connection Roadmap, detailing recommended actions and key milestone dates to achieve within the next five years the goals stated in this Executive Order.

IN WITNESS WHEREOF, I have hereunto set my hand and caused to be affixed the Great Seal of the State of Arizona.

GOVERNOR

DONE at the Capitol in Phoenix on this 24th day of August in the Year Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.

ATTEST:

Janice K. Brewer
SECRETARY OF STATE

Appendix B: Organization Structure for *Roadmap* Creation

The organization structure used to create the Arizona Health-*e* Connection *Roadmap* consists of a Steering Committee and supporting task groups. The process is aided by an Executive Leadership Team, Task Group Leadership Team, and a Project Management Team. A listing of all *Roadmap* participants is in the Acknowledgments section of the *Roadmap*.

The **Steering Committee** is charged to comprehensively review issues surrounding the creation of an e-health infrastructure in Arizona and develop guidance for the users of such infrastructure. The Steering Committee is also charged to explore funding options for creation of the infrastructure. There are 42 members on the Steering Committee, including two co-chairs.

Representation on the Steering Committee is broad based and includes membership from the following organizations/sectors:

- Major employers
- Health plans
- Physician community
- Hospitals and hospital systems
- Healthcare foundations and organizations involved in e-health information
- Healthcare associations
- Arizona Health Care Cost Containment System
- Arizona Department of Health Services
- Arizona Department of Administration
- Arizona Department of Insurance
- Arizona universities
- Health information, privacy, and security content experts

Task groups were created to support the Steering Committee and to provide specific recommendations for Steering Committee consideration.

The five task groups established were:

- Clinical
- Technical
- Financial
- Legal
- Governance *

* The Governance Task Group is a subcommittee of the Steering Committee

Participation on the Clinical, Technical, Financial, and Legal task groups was open to all. An inclusive approach to task group membership provided a vehicle for all interested individuals and organizations to be represented. This approach proved successful and provided a rich variety of viewpoints and ideas. About 250 people signed up for task group participation.

Each task group was assigned a chairperson and a facilitator. The chairperson is an Arizona leader (and preferably a member of the Steering Committee). The facilitator is a nationally based expert obtained via an engagement with the eHealth Initiative. (www.eHealthInitiative.org).

An **Executive Leadership Team** provided day-to-day leadership of the project. The Executive Leadership Team, consisting of five members of the Steering Committee, provided guidance and support for the project staff on an as-needed basis. The team provides a channel between the Governor and the Steering Committee and is the Steering Committee's voice to the community. The team also ensures that the Steering Committee and task groups have appropriate resources.

The **Task Group Leadership Team** provided a key venue to continuously align progress and direction of each individual task group with the direction of the overall project. The Task Group Leadership team consisted of the chairperson, facilitator, and staff for each task group.

A **Project Management Team** orchestrated scheduling, logistics, and compilation of presentation materials for the entire process. The Project Management Team reports to the Executive Leadership Team.

Appendix C: Process to Create the *Roadmap*

This appendix discusses the process used to create the *Roadmap*.

The process was kicked off October 5, 2005, at the Governor's Call to Action Summit. About 300 people attended the summit. Attendees were encouraged to volunteer for one or more of the task groups at the summit. Formation of the Steering Committee was completed about a month after the summit. The process to create the *Roadmap* was discussed at the initial Steering Committee meeting.

The seven key steps in the process are below.

1. Steering Committee sets goals, objectives, principles, and policy.
2. Task groups make recommendations for the *Roadmap*.
3. Steering Committee reviews recommendations.
4. Executive Leadership and Project Management Teams synthesize recommendations into a ohesive document.
5. Draft *Roadmap* is presented to the Steering Committee for review and approval.
6. Once approved, the *Roadmap* is presented to the Governor.
7. Upon the Governor's direction, the *Roadmap* is implemented.

A more detailed description of each step in the process follows.

Step 1. Steering Committee sets goals, objectives, principles, and policy.

The Steering Committee is responsible for establishing the direction of the *Roadmap*. It developed and approved several documents instrumental in moving the project forward. The documents include the Arizona Health-*e* Connection Briefing Paper, a Values and Guiding Principles document, a Mission Statement, and charges for each of the five task groups.

The Arizona Health-*e* Connection Briefing Paper is a starting point for creation of the *Roadmap*. It provides a baseline of the e-health landscape from a national perspective and an Arizona perspective. Of special interest is a section that summarizes responses from a group of 27 Arizona leaders on the state of e-health in Arizona. The paper is available at http://www.azgita.gov/tech_news/2005/ehealth/Briefing.pdf.

The Steering Committee also provided a Mission Statement and a Values and Guiding Principles document for the *Roadmap*. These documents are in Figures XVIII and XIX.

Finally, the Steering Committee provided a Task Group Charge for each of the five task groups. The Task Group Charge document provides specific direction for deliverables from each group. The charges correlate to the Governor's Executive Order and are listed in Figure XX.

Figure XVIII: Mission Statement

"Facilitate the design and implementation of integrated statewide health data information systems that support the information needs of consumers, health plans, policymakers, providers, purchasers, and researchers and that reduce healthcare costs, improve patient safety, and improve the quality and efficiency of healthcare and public health services in Arizona."

Figure XIX: Values and Guiding Principles

ARIZONA HEALTH-*E* CONNECTION ROADMAP

VALUES AND GUIDING PRINCIPLES

The Health-*e* Connection *Roadmap* will articulate a path to improve the quality and reduce the cost of healthcare in Arizona. The *Roadmap* will be designed to identify key decision points by focusing on the what, when, why, and who—what action needs to occur, when the action needs to occur, why the action is necessary, and who (individual/group/organization) is required to complete the action. In addition, barriers to implementation must be identified to achieve the goals outlined in the *Roadmap*.

To aid in the *Roadmap* development process, specific values and guiding principles have been identified as critical ingredients of success and will serve as the foundation for a long-term strategy:

1. CREATE ACHIEVABLE, ACTIONABLE, AND PRACTICAL INITIATIVES.
   - Develop and implement short-term (one year or less) achievable, practical, and measurable initiatives as part of the *Roadmap* to show early progress, value, and momentum.
   - Develop mid-term and long-term recommendations for full implementation.
   - Provide recommendations that reach across geographical, demographic, and organizational boundaries

2. ENSURE THAT INITIATIVES ARE CONSUMER-FOCUSED.
   - Involve consumers from the start in the governance and advisory structure of an interoperable HIT environment, as appropriate.
   - Provide recommendations that will enable consumers to make more fully informed choices on their own healthcare with respect to value and quality of care.
   - Ensure that consumer health information security and privacy needs are met.

3. PROVIDE TECHNICAL BASIS FOR HEALTH DATA EXCHANGE.
   - Develop and implement a technical infrastructure that will support the federal initiative of interoperable, real-time electronic health data exchange based on national standards.
   - Ensure health information availability at the point of care for all providers and patients.

4. PROMOTE SUSTAINABILITY.
   - Develop and maintain a model for sustainability and continuous improvement that adapts to change and aligns the costs and incentives with the benefits related to health information technology and health information exchange.
   - Develop a governance structure that attracts and retains participants and defines roles and responsibilities of a public-private collaborative.

5. INCREASE THE QUALITY AND PERFORMANCE OF HEALTHCARE IN ARIZONA.
   - Identify metrics to measure performance from the perspective of patient care, public health, provider and payer value, and overall economic value.
   - Control healthcare costs to reduce state expenditures and enhance the business environment for both small and large employers.
   - Provide clinicians and other authorized healthcare professionals with clinical decision support to enhance decisions, avoid clinical errors, including medication errors and adverse events, avoid duplicative medical procedures, and assist in following recommended practices throughout the care delivery process.
   - Enhance and facilitate the use of patient care data for appropriate public health disease surveillance, outbreak detection, trending, and health protection efforts.
   - Collect and use scientifically valid data and information to assess the quality, performance, and cost of healthcare.

6. ASSIST IN HEALTHCARE RESEARCH.
   - Collect and use data and information for scientifically valid research and public health.

Figure XX: Task Group Charges

CLINICAL TASK GROUP

Leadership:

Chair:	*Bruce Bethancourt, M.D.*
Facilitator:	*Seth Foldy, M.D.*
Staff:	*Andy Miller/Chris Muir*

The exchange of electronic health information can improve the quality, safety, and efficiency of healthcare. There are imperatives that drive the formation of health information exchange networks to equally serve the provider, payer, and patient communities. Establishing clear priorities and articulating benefits for each community encourages active participation and gain sharing by all participants.

Executive Order Reference
Develop recommendations for facilitating statewide adoption of electronic health record standards to enable health information exchange across the state and nationally.

Clinical Task Group Is Charged With:

Initial Task:

- Define criteria (such as reach, feasibility, and impact) to prioritize key "product" types (such as a continuity of care record, ePrescribe, etc) to be implemented on the *Roadmap*.
- Identify and prioritize the key "product" types to be implemented on the *Roadmap*.

Upon Completion of Initial Task:

- Define use cases (real-world examples) that are appropriate for the first key "product" types identified.
- Identify key barriers to adoption and recommend strategies for working with the identified community to clear those barriers.

Clinical Task Group Shall Also:

- Coordinate with and give input to the Legal, Financial, and Technical Task Groups and Steering Committee.
- Present findings, analysis, and recommendations at the March 2006 Steering Committee meeting.

Figure XX: Task Group Charges (continued)

FINANCIAL TASK GROUP

Leadership:
Chair: *Rick Potter*
Facilitator: *Jay McCutcheon*
Staff: *Elizabeth McNamee*

An effective financial model is required to drive widespread adoption and diffusion of HIT and health information exchange. Financial incentives must be properly aligned, and a realistic business case and value proposition should be defined for e-health data exchange.

Executive Order Reference
Develop recommendations for identifying existing e-health resources, including funding sources, to support the development of a statewide e-health information infrastructure.

Financial Task Group Is Charged With:

Initial Tasks:

- Articulate the value of investment and the business case for investment in health information exchange.
- Examine approaches and successful examples of financial strategies to increase adoption of HIT and e-health data exchange from within Arizona and other regions.
- Propose finance strategies for funding HIT and e-health data exchange (start-up and long-term), including the appropriate role of public and private sectors.

Upon Completion of Initial Tasks:

- Identify specific financial actions required to support the first key "product" types (as identified by the Clinical Task Group and approved by the Steering Committee).
- Provide an estimate for total cost of implementation of the first key "product" types.
- Provide an estimate for total cost of implementation of the Arizona Health-e Connection Roadmap.

Financial Task Group Shall Also:

- Coordinate with and give input to the Clinical, Technical, and Legal Task Groups and Steering Committee.
- Present findings, analysis, and recommendations at the March 2006 Steering Committee meeting.

Figure XX: Task Group Charges (continued)

TECHNICAL TASK GROUP

Leadership:

Chair:	*Eric Dean*
Facilitator:	*Paul Biondich, M.D.*
Staff:	*Chris Muir*

A robust technical model is required for effective e-health data exchange. It is imperative to leverage current available technology and build on technical successes from other implementations to address e-health data exchange and business needs. A process to establish consensus must be created to ensure appropriate technical standards are applied.

Executive Order Reference
Develop recommendations for identifying technology options, and their advantages and disadvantages, for a statewide e-health information infrastructure.

Technical Task Group Is Charged With:

Initial Tasks:

- Discuss and document different options/examples of technical architectures used by health information exchange initiatives and the best uses of each.
- Complete an inventory of existing Arizona state technical infrastructure resources and increase understanding of what infrastructure resources can be leveraged.

Upon Completion of Initial Tasks:

- Recommend a process, inclusive of appropriate groups and organizations, to establish design guidelines for technology, including compliance with national standards to ensure e-health data exchange.
- Create technical requirements based on business and clinical use cases (as defined by the Clinical Task Group) required for the first key "product" types (as identified by the Clinical Task Group and approved by the Steering Committee)

Technology Task Group Shall Also:

- Coordinate with and give input to the Clinical, Financial, and Legal Task Groups and Steering Committee.
- Present findings, analysis, and recommendations at the March 2006 Steering Committee meeting.

Figure XX: Task Group Charges (continued)

LEGAL TASK GROUP (PRIVACY AND SECURITY)

Leadership:
Chair: *Kristen Rosati*
Facilitator: *Bill Braithwaite, M.D.*
Staff: *Andy Miller*

For an e-health data exchange to be successful, consumers must trust that their health information will be kept confidential and secure. There is thus a critical need to review federal and state laws affecting e-health data exchange, particularly those related to confidentiality, use, and disclosure of health information, and to anticipate new issues that may arise through e-health data exchange across multiple environments.

Executive Order References
Develop recommendations for identifying options for serving consumer health information needs; develop recommendations for ensuring health information privacy and security in electronic health information exchange.

Legal Task Group Is Charged With:

Initial Tasks:

- Document real and perceived legal barriers that could dramatically hinder an e-health data exchange for different purposes, including for treatment, payment functions, quality improvement, public health, and research.
- Make recommendations on whether health information with "special" protection will be included in the e-health data exchange (such as mental health information, alcohol and drug abuse treatment information, communicable disease information, and genetic testing information) and potential limits required on the use and disclosure of that special information.
- Understand consumer expectations for an e-health data exchange and make recommendations on the role of consumers in an e-health data exchange, including whether consumers will be permitted to opt out of having their information included in the exchange.
- Identify examples of best practices from other regions that can be applied to a variety of healthcare environments, that comply with HIPAA, and that represent consumer interests.

Upon Completion of Initial Tasks:

- Identify specific legal actions required for the first "product" types (as identified by the Clinical Task Group and approved by the Steering Committee), including whether statutory or regulatory amendments are needed.
- Identify practical strategies and solutions (not technical) for developing e-health data exchange that will ensure the secure and confidential transmission of medical information.

Legal Task Group Shall Also:

- Coordinate with and give input to the Clinical, Financial, and Technical Task Groups and Steering Committee.
- Present findings, analysis, and recommendations at the March 2006 Steering Committee meeting.

Figure XX: Task Group Charges (continued)

GOVERNANCE TASK GROUP

Note: The Governance Task Group is a subcommittee of the Arizona Health-e Connection Steering Committee. The task group will be staffed by Steering Committee members.

Leadership:

Chair:	*David Landrith*
Facilitator:	*Seth Foldy, M.D.*
Staff:	*Lorie Mayer*

A public-private collaborative structure is needed for the success of an electronic health information exchange organization that supports the development and implementation of a shared vision and plan for addressing healthcare challenges through information technology and health information exchange in Arizona.

Executive Order Reference
Develop recommendations for creating organizational and governance structures for a statewide e-health information infrastructure.

Steering Committee is charged with the following Governance tasks:

- Develop a draft shared vision statement, guiding principles, and operations of a statewide collaborative.
- Examine successful examples of governance strategies used by working health information exchange initiatives.
- Define a structure and approach that effectively attracts and retains participants and defines roles and responsibilities of a public-private collaborative.
- Discuss legal barriers and/or legal incentives associated with various governance models.
- Create a communication plan that conveys accurate and useful information, uses existing communication channels, creates new channels as needed, and presents information in a timely and effective manner.
- Coordinate with and give input to all four task groups.
- Present findings, analysis, and recommendations at the March 2006 Steering Committee meeting.

Step 2. Task groups make recommendations for the *Roadmap*.

Each task group was responsible for making recommendations to the Steering Committee based on its charge (see Figure XX). To accomplish this task, each task group conducted a series of meetings to discuss its charge, priorities, and alternatives and to reach general consensus.

By design, the Clinical Task Group was the lead group. It was the responsibility of the Clinical Task Group to determine priorities for the *Roadmap* based on urgency (see the *Roadmap* section on Fundamental Concept #2: Urgency Balanced by Feasibility Determines Timing of Roadmap Inclusion).

It was noted that the Clinical Task Group represented payers, providers, and patients in their deliberations of priorities. Although representation of providers in the task group was prevalent, it is believed the urgent priorities from the perspective of patients and payers were effectively represented.

The top priorities identified by the Clinical Task Group were:

- Create shared information access between professionals to
  - Support quality systems
  - Support continuity of care and access
  - Improve cost efficiency
  - Improve safety

- Add processes and interfaces for patient information access and communication (next priority), public health functions (next priority), research, and other functions (later priority)

These priorities were translated into *urgent* product types and presented to the Financial, Technical, and Legal Task Groups for *feasibility* analysis. The *urgent* product types determined by the Clinical Task Group are:

Initial Product:

- Historical, assembled view of a patient's high-value information from across all providers (continuity of care information)
  - Positive impact on all four top clusters (quality, safety, continuity of information, and cost efficiency)
  - Patient's high-value information includes medications prescribed, medications dispensed, allergies, immunizations, lab results and trends, other providers caring for patient (and contact info), cumulative medical problem list (from billing and/or EMRs), insurance/eligibility and basic demographic information of patient, and hospital and emergency department discharge information.

Other Products of Interest:

- ePrescribe

- Secure communication between users (providers initially)

- Decision support

In considering *feasibility*, it was the responsibility of the Technical, Legal, and Financial Task Groups to determine, "What needs to happen to implement the Clinical Task Group product-type priorities?" In considering this question, the task groups needed to balance factors such as:

- Were any prerequisite technical activities/ projects required?

- Importance of establishing early wins to maintain project momentum

- How would startup capital and sustainable funding be obtained?

Initiatives such as a results delivery service and the Web portal were determined critical during this phase of roadmap construction. These initiatives, for example, are both prerequisites for establishment of a patient health summary.

Regular meetings of the Task Group Leadership Team were conducted to maintain synchronization among the task groups. The meetings also served as a forum to vet conclusions and recommendations before they were forwarded to the Steering Committee.

The Clinical Task Group conducted five meetings, the Legal Task Group conducted two meetings, the Technical Task Group conducted three meetings, the Financial Task Group conducted three meetings, and the Governance Task Group conducted four meetings.

Step 3. Steering Committee reviews recommendations.

The Steering Committee approved high-level recommendations from the five task groups on March 8, 2006.

Step 4. Executive Leadership and Project Management Teams synthesize recommendations into a cohesive document.

The process of creating the *Roadmap* commenced March 8, 2006, upon approval of high-level recommendations by the Steering Committee and was completed April 3, 2006.

Step 5. Draft *Roadmap* is presented to the Steering Committee for review and approval.

A draft copy of the *Roadmap* was delivered to the Steering Committee March 28, 2006.

Step 6. Once approved, the *Roadmap* is presented to the Governor.

The Steering Committee approved the *Roadmap* on April 4, 2006.

Step 7. Upon Governor's direction, the *Roadmap* is implemented.

Appendix D: HIT Support Organizations

Doctors Office Quality-Information Technology Initiative (DOQ-IT)

The Doctors Office Quality-Information Technology Initiative (DOQ-IT) is a three-year national initiative of the Centers for Medicare & Medicaid Services (CMS) to promote adoption and effective use of information technologies in small- to medium-sized primary care practices. The national aim is to increase adoption of electronic health records by 5 to 6 percent within three years. At the state level, the Quality Improvement Organization (QIO) provides coordination of technical assistance activities of the DOQ-IT initiative. In Arizona, the Health Services Advisory Group (HSAG) is the state QIO responsible for DOQ-IT. HSAG is partnering with the Arizona Medical Board, the Arizona Medical Association (ARMA), the Arizona Academy of Family Physicians (AAFP), the Arizona chapter of the American College of Physicians (ACP), and the American Academy of Pediatrics (AAP) to promote EHR adoption. The Arizona DOQ-IT Web site is www.azdoqit.org.

The following recommendations were provided by DOQ-IT for implementing the HIT portion of the *Roadmap*:

- Convene health plans to establish a grant pool that could be managed by an HIT foundation
- Convene the banking and lending industry to establish common practices for lending for HIT
- Create state loan guarantees for HIT small practice loans
- Co-sponsor EHR University. Include the University of Arizona College of Medicine and the Arizona State University Bioinformatics Institute
- Organize statewide purchasing cooperative for small- to medium-sized practices
- Sponsor a speakers' bureau
- Sponsor town halls to introduce *Roadmap* and promote HIT adoption

Healthcare Information and Management Systems Society (HIMSS)

HIMSS is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of human health.

HIMSS supports HIT adoption and standards with a wide variety of educational events, conferences, Webinars, advocacy, and standards. Here is a listing:

CCHIT

HIMSS, AHIMA (American Health Information Management Association), and The Alliance (formerly National Alliance for Health Information Technology) have joined forces to launch the Certification Commission for Healthcare Information Technology (CCHIT). These three associations have committed funding and staff to support the commission during its organizational phase. CCHIT's mission is to accelerate the adoption of robust, interoperable HIT throughout the U.S. healthcare system by creating an efficient, credible, sustainable mechanism for the certification of HIT products.

Advocacy

As a partner of the Capitol Hill Telehealth and Healthcare Informatics Series, HIMSS convenes regular luncheon programs on Capitol Hill. Held on behalf of the Capitol Hill Steering Committee on Telehealth and Healthcare Informatics, it is designed to inform federally elected officials and their staffers on topics pertinent to HIT.

Standards

HIMSS has been assigned the role as secretariat to ISO TC/215, the technical committee of the International Organization for Standardization (ISO) for healthcare informatics, and other activities.

Physicians Adopting Computer Technology (PACT)

These are a series of conferences addressing the challenges and successes of EMR implementation held around the country for the independent physician practice.

Integrating the Healthcare Enterprise (IHE)

Integrating the Healthcare Enterprise (IHE) is a multiyear initiative that creates the framework for passing vital health information seamlessly—from application to application, system to system, and setting to setting—across the entire healthcare enterprise.

RHIO Federation

To begin supporting the development of regional health information organizations (RHIOs) and health information exchanges (HIE), HIMSS has launched the RHIO Federation to focus on three key areas of collaboration: chain of trust, business rules, and harmonization.

The HIMSS RHIO Federation's goal is to help foster the RHIO/HIE industry through education, outreach, and advocacy activities at the local, state, and federal levels. All Federation activities will be supported by 43 regional chapters through the RHIO Federation Chapter Liaison program. Federation liaisons and HIMSS' staff and membership of subject matter experts will be made available to RHIO/HIE initiatives nationwide to help them plan, develop, and maintain their business plans by connecting them to the right resources at the right time.

Arizona Health IT Accelerator (AHITA)

AHITA is a nonprofit organization that brings together technologists and physicians dedicated to helping other physicians select, implement, and finance EHRs. AHITA helps physicians by:

- Understanding the business of practicing medicine
- Understanding the technology
- Knowing how to facilitate beneficial change
- Being vendor neutral

A major part of AHITA's work is education. Working with Arizona DOQ-IT and Arizona medical associations (AAFP, AAP, ACP, Arizona Osteopathic Medical Association, and ARMA), AHITA is helping physicians get ready for electronic health records.

Appendix E: Sample HIT Adoption Strategies

The following is a list of potential approaches to encourage HIT adoption for consideration by the statewide governance organization. The list was developed by the task groups and the Task Group Leadership Team. There is no implied order or priority of the listed approaches.

PLANNING

- General assistance
- Standards, CCHIT, CDA, HL7, coding
- Arizona guidelines and materials
- Vendor and product ratings with comparisons and reports
- Pricing information
- Example RFPs and contracts
- Interregional network for information sharing

FINANCING

- ROI studies
- HIT tax credits, including credits for special populations and credits for utilization
- Low-interest loans
- Reimbursement for HIT integration with statewide HIE program
- HIT ASP services
- EMRs and other products as part of the HIE
- Grants from governments, foundations, and other sources
- Hospital HIT foundation

IMPLEMENTATION

- General assistance
- Example implementation plans
- Example network plans
- Example interface specifications
- Work process analysis templates
- Example procedures (e.g., change management)
- Network infrastructure
- Hardware procurement/replacement
- Design assistance
- User groups and chat rooms
- QIO staff support
- Joint ventures of HIT implementations
- HIT "Peace Corps"

EDUCATION AND ADOPTION

- EMR subsidies for medical schools
- Training programs (e.g., through community colleges and technical and medical schools)
- HIT education with CME credits
- Readiness assessment templates
- Training manuals
- SuperUser Network

Appendix F: Business Case for Electronic Orders and Results for Laboratory

Business Case for Electronic Orders and Results for Laboratory

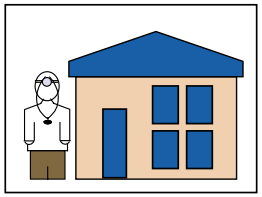
The business case enabling referring physicians to order laboratory tests and receive their results electronically is a compelling one. Without the electronic orders and results system, the reliance on paper documents caused numerous errors and delays in testing. The paper documents were incomplete and inaccurate because of illegible writing. In addition, vague orders were given, resulting in the wrong tests being performed. The ordering physician's office was impacted because this task was handled manually and relied on the office staff to provide the laboratory with all relevant information, including patient demographics, medical history, diagnosis, and medical necessity. If the information was not complete, the office or the patient had to be contacted directly for the required information. The manual paper process could cause delays in testing and require rework for the physician. The patient was inconvenienced by the need to complete missing data, by being billed incorrectly and, in worst cases, by having to return to the laboratory for a redraw. All data entry in the laboratory to initiate testing was manual, creating another possible error point, and costly to perform. Results were sent to physicians via courier, fax, or remote printing.

With the implementation of electronic orders and results, the laboratory receives accurate data from the ordering physician. The system has all requirements inherent in the system and prompts the staff for all demographics and testing information. The medical necessity logic is in the system, preventing billing errors and delays. The physician's office staff has an electronic record of the ordered tests for follow-up and the patient's demographics are the same as in the office system. The order is received by the laboratory directly into its system, which reduces manual data entry and errors due to inaccurate test requests or specimen requirements. Once the testing is reported, the results are immediately available electronically for the physician's office. There is no need to wait for courier delivery, faxes, or remote printing.

Overall, the electronic orders and results process reduces cost for both the ordering physicians and the laboratory because the orders are validated in the system and screened for errors, reducing rework and phone calls to clients. Quality improvements are seen in the laboratory because the correct tests and specimen requirements are adhered to; orders are electronically received, reducing data entry errors and improving turnaround time for testing. Results are sent directly to the physician's system electronically and are available for immediate review. This also reduces costs for courier delivery. Patients benefit because their orders are received correctly with all required data, reducing the number of redraws and requests for correct demographic information. The whole cycle, from test ordered to result to billing, is reduced through the electronic process.

The following two pages provide a view of the environment before and after implementation of an automated lab system.

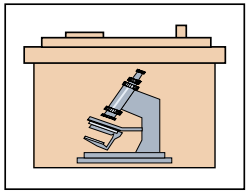
Business Case: Orders and Results
Laboratory Example
(Before)



Physician Practice

Orders

Results / Reports



Laboratory

Physician Practice
Assumptions & Implications

- **Physician requests lab testing via paper requisition or written script**
- **Patient sent to patient service center with laboratory requisition or script**
- **Some patients are drawn in physician's office and paper requisition or script accompanies specimen in transport to laboratory**
- **Specific lab tests codes not always used, especially on scripts, written description of requested tests on document**
- **Specimen requirements are offline, in a reference manual for physician's use**
- **No adherence to required data on paper documents, missing patient demographics and test information occurs frequently, delaying testing**
- **Lack of patient demographic information causes increased contact to physicians for correct information**
- **Physician's system must be updated manually to indicate lab tests ordered**
- **Medical necessity rules and ICD-9 requirements not automated**
- **Physicians are upset with increased calls to their offices for clarification and rework**

Health Information Exchange

Financial & Economic Beneficiaries

Service Level & Operations Beneficiaries

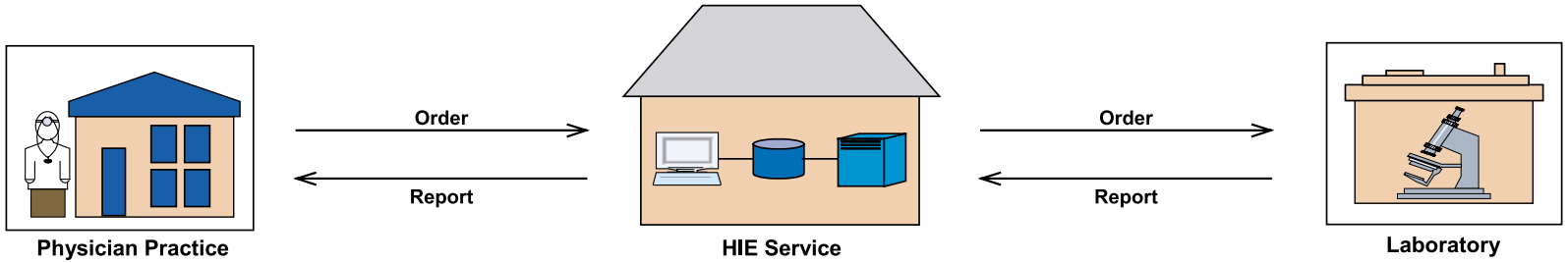
Quality & Safety Beneficiaries

Other Beneficiaries

Laboratory
Assumptions & Implications

- **Paper orders received either when patient presents or with specimen transported from physician's office**
- **If patient is present, the patient must complete a requisition in order to provide demographic data**
- **If patient is not present, the physician must be called or asked for additional written documentation**
- **Paper documents received can be illegible, indicate incorrect test codes, lack specificity, the physician is called for clarification**
- **If specimen sent directly to laboratory from physician's office, inaccurate or incomplete information on paper documents may cause incorrect tests to be performed or missed**
- **All manual data entry for laboratory processing**
- **Patient may have to be re-called and re-drawn due to inaccurate information on paper orders**
- **Results delivered by courier, fax or remote printer, no electronic interfaces to physician's systems**
- **Lab quality is impacted due to rework, delays in testing while awaiting information and increased turnaround time**

Business Case: Orders and Results
Laboratory Example
(After)



Physician Practice
Assumptions & Implications

- •Electronic orders increase accuracy for ordered tests
- •Easy, secure, access to orders, results and diagnostic tools online, from any internet connection via VPN
- •Secure method to share clinical information with other providers
- •Customized screens for test ordering, ICD9 lists
- •No investment in expensive equipment
- •Maintain patient clinical information, test history and trending data
- •Patient-centric database, can combine information from other sources, acts as an EMR
- •Medical necessity logic for compliant ordering
- •Reference manual online
- •E-Prescribing
- •Patient eligibility verification
- •CPU to CPU interfaces-more expensive, varies widely by vendor

Health Information Exchange

Financial & Economic Beneficiaries
Physicians, laboratories, payers, patients

Service Level & Operations Beneficiaries
Physicians, laboratories, patients, payers

Quality & Safety Beneficiaries
Patients, physicians, laboratories, payers, health agencies

Other Beneficiaries
Health agencies, government agencies, specialty groups, RHIO's

Laboratory
Assumptions & Implications

- •Increased accuracy in ordering, reduces missed tests, wrong tests ordered
- •Patients to not have to be re-drawn due to missed or incorrect tests
- •Reduction in labor for specimen processing
- •Reduces turn-around time due to minimal input for lab testing, tests distributed to lab departments quickly
- •Results sent electronically to client, no in-house printing or courier delivery, results available for viewing as soon as finalized
- •Reduced number of calls to client services because information available real time by physician and questions regarding test requirements available online
- •Medical necessity logic in system reduces calls to physicians for additional information
- •Patient eligibility performed by physician office reduces rejections from laboratory payers
- •Data mining capabilities, Hedis reporting, trend data

XIV. Glossary

Application Service Provider (ASP)—A business that provides computer-based services to customers over a network. The most limited sense of this business is that of providing access to a particular application program (such as medical billing) using a standard protocol such as HTTP.

Arizona Department of Health Services (ADHS)—State department involved in a wide array of activities designed to promote and protect the health of Arizona citizens. Some of the services overseen by ADHS are the state's Mental Health program, Assistance and Licensure offices, community and family health, epidemiology and disease control, and Office of Vital Records.

Arizona Health Care Cost Containment System (AHCCCS)—Arizona's Medicaid program. AHCCCS contracts with health plans and other program contractors, paying them a monthly capitation amount prospectively for each enrolled member. The plan or contractor is then "at risk" to deliver the necessary services within that amount. AHCCCS receives federal, state, and county funds to operate, including some money from Arizona's tobacco tax.

Arizona Health Information Security and Privacy Collaboration (AzHISPC)—The Arizona entry for funding from the national Agency for Healthcare Research and Quality (U.S. Department of Health and Human Services) to 1) assess variations in organization-level business policies and state laws that affect health information exchange; 2) identify and propose practical solutions, while preserving the privacy and security requirements in applicable state and federal laws; and 3) develop detailed plans to implement solutions.

Arizona Health IT Accelerator (AHITA)—A nonprofit organization that brings together technologists and physicians dedicated to helping other physicians select, implement, and finance EHRs.

Arizona Health Query (AzHQ)—An integrated database of medical records from public and private data partners in Maricopa County. A joint project of St. Luke's Health Initiatives and Arizona State University, its purpose is to monitor the performance of the local healthcare system in terms of access, quality, and cost, and to conduct research that improves system performance over time.

Arizona Technology Council (ATC)—The largest technology association in Arizona, serving all tech sectors across the state. A member-driven association, ATC represents the interests of technology companies, their support firms, educational institutions, and statewide economic development groups that collectively form Arizona's technology community.

Arizona Telecommunications and Information Council (ATIC)—An economic development foundation under the Governor's Strategic Partnership For Economic Development (GSPED). The ATIC mission is to promote and support the adoption of effective public policies for the state of Arizona and local communities that encourage investment and deployment of information technologies and telecommunication services to enable continued educational advancement, enhanced quality of life, and economic prosperity for the Arizona community.

Broadband—Refers to an increased ability of a user to view content across the Internet that includes large files, such as video, audio, and three-dimensional (3D). A user's broadband capability is typically governed by the last mile issue, the connection between the Internet service provider and the user.

Certification Commission for Healthcare Information Technology (CCHIT)—The mission of CCHIT is to accelerate the adoption of robust, interoperable HIT throughout the U.S. healthcare system by creating an efficient, credible, sustainable mechanism for the certification of HIT products.

Centers for Medicare and Medicaid Services (CMS)—U.S. Department of Health and Human Services agency that seeks to protect and improve beneficiary health and satisfaction; foster appropriate and predictable payments and high-quality care; promote understanding of CMS programs among beneficiaries, the healthcare community, and the public; promote the fiscal integrity of CMS programs and be an accountable steward of public funds; foster excellence in the design and administration of CMS programs; and provide leadership in the broader healthcare marketplace to improve health.

Chronic Care Management—Process used to administer care for high-cost beneficiaries to control costs.

Clinical Document Architecture (CDA)—The CDA, until recently known as the Patient Record Architecture (PRA), provides an exchange model for clinical documents (such as discharge summaries and progress notes) and brings the healthcare industry closer to the realization of an electronic medical record. The CDA Standard is expected to be published as an ANSI-approved standard by the end of 2006. (See Health Level 7.)

Continuity of Care Record (CCR)—A type of patient health summary. CCR is a way to create flexible documents that contain the most relevant and timely core health information about a patient and to send them electronically from one caregiver to another. It contains various sections—such as patient demographics, insurance information, diagnosis and problem lists, medications, allergies, and care plan—that represent a snapshot of a patient's health data that can be useful, even lifesaving, if available when the patient has his or her next clinical encounter.

Disease Management—A system of coordinated healthcare interventions and communications for populations with conditions in which patient self-care efforts are significant. Disease management supports the physician- or practitioner-patient relationship and plan of care, emphasizes prevention of exacerbations and complications using evidence-based practice guidelines and patient empowerment strategies, and evaluates clinical, humanistic, and economic outcomes on an ongoing basis with the goal of improving overall health.

Doctor's Office Quality–Information Technology (DOQ-IT)—Promotes the adoption of electronic health record (EHR) systems and information technology (IT) in small- to medium-sized physician offices with a vision of enhancing access to patient information, decision support, and reference data, as well as improving patient-clinician communications.

Electronic Health Record (EHR)—Generic term for all electronic patient care systems. It is a real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making. The EHR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EHR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting.

Electronic Medical Record (EMR)—Electronic record with full interoperability within an enterprise (hospital, clinic, or practice).

ePrescribing—A type of computer technology in which physicians use handheld or personal computer devices to review drug and formulary coverage and transmit prescriptions to a printer or a local pharmacy. ePrescribing software can be integrated into existing clinical information systems to allow the physician access to patient-specific information to screen for drug interactions and allergies.

Government Information Technology Agency (GITA)—The agency responsible for statewide information technology (IT) planning, coordinating, and consulting. The GITA director serves as the chief information officer for state government. GITA is responsible for administering the state's Executive Branch IT resources.

Governor's Council on Innovation and Technology (GCIT)—Formed by executive order, the council consists of 32 members appointed by the Governor and serves without compensation at the pleasure of the Governor.

Greater Arizona eLearning Association (GAZEL)—GAZEL initiatives help eLearning companies develop new business opportunities and advanced technologies and services. GAZEL helps enhance business practices, develop strategic partnerships, and identify sources of business financing. It also provides opportunities to network with consumers and other eLearning professionals, and to engage in professional development opportunities to export client technologies and services nationally and internationally.

Health Information Exchange (HIE)—The mobilization of healthcare information electronically across organizations within a region or community. HIE provides the capability to electronically move clinical

information between disparate healthcare information systems while maintaining the meaning of the information being exchanged. The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care.

Health Information Technology (HIT)—The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of healthcare information, data, and knowledge for communication and decision-making.

Health Services Advisory Group (HSAG)—Founded by a group of medical professionals in 1979, HSAG is one of most experienced quality improvement organizations in the nation. The mission of the organization is to positively affect the quality of healthcare by providing information and expertise to those who deliver and those who receive health services.

Healthcare Information and Management Systems Society (HIMSS)—The healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of human health.

Health Insurance Portability and Accountability Act (HIPAA)—Enacted by the U.S. Congress in 1996. According to the Centers for Medicare and Medicaid Services, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification provisions, requires the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers.

Health Level Seven (HL7)—One of several American National Standards Institute (ANSI) - accredited standards developing organizations (SDOs) operating in the healthcare arena. Most SDOs produce standards (sometimes called specifications or protocols) for a particular healthcare domain such as pharmacy, medical devices, imaging, or insurance (claims processing) transactions. Health Level Seven's domain is clinical and administrative data.

ICD-9 (International Classification of Disease, 9th Revision)—The 1972 revision of the international disease classification system developed by the World Health Organization (WHO). The International Statistical Classification of Diseases and Related Health Problems (commonly known by the abbreviation ICD) is a detailed description of known diseases and injuries. Published by WHO, it is used worldwide for morbidity and mortality statistics, reimbursement systems, and automated decision support in medicine. The ICD is a core classification of the WHO Family of International Classifications.

Indian Health Service (IHS)—An agency of the U.S. Department of Health and Human Services responsible for providing federal health services to American Indians and Alaska Natives. IHS is the principal federal healthcare provider and health advocate for Indian people, and its goal is to raise their health status to the highest possible level. IHS provides health services to approximately 1.5 million American Indians and Alaska Natives who belong to more than 557 federally recognized tribes in 35 states.

Institute of Medicine (IOM)—A nonprofit organization specifically created for this purpose as well as an honorific membership organization, IOM was chartered in 1970 as a component of the National Academy of Sciences. IOM's mission is to serve as adviser to the nation to improve health. It provides unbiased, evidence-based, and authoritative information and advice on health and science policy to policymakers, professionals, leaders in every sector of society, and the public at large.

Master Patient Index (MPI)—A software database program that collects a patient's various hospital identification numbers, perhaps from the blood lab, radiology, admission and so on, and keeps them under a single, enterprise-wide identification number.

Medical Trading Area (MTA)—An MTAs is usually a geographic area defined by where a population cluster receives its medical services. It is an area in which groups of physicians, hospitals, labs, and other providers work together to serve a population of consumers.

Normalization—The process of redefining clinical data based on some predefined rules. The values are redefined based on a specific formula or technique.

Office of the National Coordinator for Health Information Technology (ONC)—U.S. Department of Health and Human Services office that provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of healthcare and the ability of consumers to manage their care and safety.

Pandemic—An epidemic (outbreak of an infectious disease) that spreads worldwide, or at least across a large region.

Patient Health Summary—Historical, assembled view of a patient's high-value information from across all providers (continuity of care information). High-priority items identified in the *Roadmap* creation process include medications prescribed, medications dispensed, allergies, immunizations, lab results and trends, other providers caring for patient (and contact information), cumulative medical problem list (from billing and/or EMRs), insurance/eligibility and basic demographic information on patient, and hospital and emergency department discharge care summary

Patient Record Locator—An electronic health record locator that would help patients and their clinicians locate test results, medical history, and prescription data from a variety of sources. For example, physicians could use the locator to find out which other physicians have information on patients they are seeing. A record locator would act as a secure health information search tool.

Personal Health Record (PHR)—An electronic application through which individuals can maintain and manage their health information (and that of others for whom they are authorized) in a private, secure, and confidential environment.

Pima Community Access Program (PCAP)—A not-for-profit organization that provides access to professional healthcare at discounted prices that the uninsured adult can afford. PCAP links low-income, uninsured residents of Pima County with an affordable, comprehensive, and coordinated network of healthcare providers.

Practice Management System (PMS)—Part of the medical office record. It carries the financial, demographic, and non-medical information about patients. This information frequently includes patient's name, patient's federal identification number, date of birth, telephone numbers, emergency contact person, alternate names for the patient, insurance company or entities financially responsible for payment, subscriber information for an insurance company, employer information, information to verify insurance eligibility, information to qualify for lower fees based on family size and income, and provider numbers to process medical claims.

Quality Improvement Organization (QIO)—Medicare QIOs work with consumers, physicians, hospitals, and other caregivers to refine care delivery systems to make sure patients get the right care at the right time, particularly among underserved populations. The program also safeguards the integrity of the Medicare trust fund by ensuring payment is made only for medically necessary services, and investigates beneficiary complaints about quality of care. Under the direction of the Centers for Medicare & Medicaid Services (CMS), the program consists of a national network of 53 QIOs responsible for each U.S. state, territory, and the District of Columbia. (See Health Services Advisory Group.)

Results Delivery Service—Service that delivers clinical results from labs to the ordering clinician in the formats they require. Examples of results include blood tests, immunology, pathology reports, X-ray, CAT scan, mammography, and transcribed reports. The service will deliver those results to the ordering physicians and to anyone else requiring a copy.

Request for Proposal (RFP)—An invitation for suppliers, through a tender process, to bid on a specific product or service. An RFP typically involves more than the price. Other requested information may include basic corporate information and history, financial information (whether the company can deliver without risk of bankruptcy), technical capability (used on major procurements of services, where the item has not previously been made or where the requirement could be met by varying technical means), product information such as stock availability and estimated completion period, and customer references that can be checked to determine a company's suitability.

Regional Health Information Organization (RHIO)—Multi-stakeholder organizations expected to be responsible for motivating and causing integration and information exchange in the nation's revamped healthcare system. Generally these stakeholders are developing RHIOs to affect the safety, quality, and efficiency of healthcare as well as access to healthcare as the result of health information technology. (Note: The *Roadmap* uses the term and definition of medical trading area (MTA) instead of RHIO).

Secure Integrated Response Electronic Notification (SIREN)—Arizona Department of Health Services system that supports disease surveillance and public health response efforts statewide, provides a secure gateway to public health systems, has alerting capabilities and online collaboration tools, and is based on national standards for information sharing.

Southern Arizona Tech Council (SATC)—A nonprofit organization formed in August 2000 whose mission is to promote and implement high-tech industry economic development and competitiveness in Tucson and Southern Arizona.

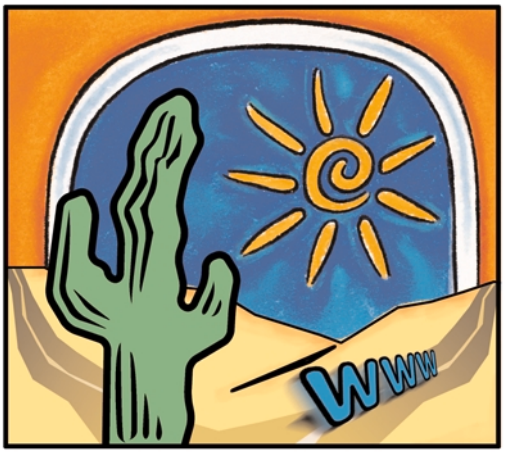
SureScripts—Founded in 2001 by the National Association of Chain Drug Stores (NACDS) and the National Community Pharmacists Association (NCPA) to improve the quality, safety, and efficiency of the overall prescribing process. The SureScripts Electronic Prescribing Network is the largest network to link electronic communications between pharmacies and physicians, allowing the electronic exchange of prescription information.

Veterans Affairs, U.S. Department of (VA)—established on March 15, 1989, succeeding the Veterans Administration. It is responsible for providing federal benefits to veterans and their families. Headed by the secretary of Veterans Affairs, VA is the second largest of the 15 Cabinet departments and operates nationwide programs for healthcare, financial assistance, and burial benefits.

XV. Contact Information

For more information on the report contact:

Chris Muir
Strategic Projects Manager
Government Information Technology Agency
602-364-4779
cmuir@azgita.gov



Produced by Health2 Resources
www.health2resources.com

Funded by St. Luke's Health Initiatives and BHHS Legacy Foundation

St. Luke's Health Initiatives
A Catalyst for Community Health

BHHS LEGACY FOUNDATION

With support and assistance by eHealth Initiative

eHEALTH INITIATIVE
Real Solutions, Better Health

Governor's Office of Health Information Exchange

Arizona Health Information Exchange (HIE)

Appendix B

Arizona Health Security Project

Recommended Minimum Policy Requirements for Privacy and Security

Generated by the stakeholders supporting Arizona's participation in Phase III of the Health Information Security & Privacy Collaboration. The Collaboration is supported and funded by the U.S. Department of Health and Human Services.

In cooperation with the Arizona Government Information Technology Agency and Arizona Health-e Connection

6-15-2009

Table of Contents

Contents

Introduction

Purpose	The purpose of the following policy requirements is to foster Data exchange for Health Information Organizations. This policy is intended to be agnostic to the state-specific health information exchange model(s) and is recommended by the Arizona Health-e Connection Clinical/Technical Committee. Health Information Organizations (HIO) participating in Health Information Exchange (HIE) may have different policies, but should incorporate these basic policy requirements. For provider authentication the HIO must (1) register, (2) execute an agreement with, (3) verify the identity of, (4) provide digital identification for, and (5) maintain an account for all Users. Each of these processes has a set of minimal requirements that must be defined in order for the participants of the HIO to trust their trading partners and Users. The HIO must implement procedures for auditing access in HIE to confirm appropriate use. Pursuant to the American Reinvestment and Recovery Act of 2009, Title XIII, Subtitle D, the HIO and any business associates of Covered Entities must comply with the Privacy and Security Law (and associated provisions) of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
Disclaimer	This policy has not been fully tested and is not intended to represent a complete security policy for health information exchange. This work is intended as a general resource (or reference) and is not meant to provide legal advice to any person or entity that receives a copy of the work. Readers should consult with competent counsel to determine applicable legal requirements, as well as privacy and security experts.

Publication Version Control

Version	Date	Name	Purpose of Revision
Original	11-7-07	CSB	Initial Draft
Version 1.0	6-2-09	Kim Snyder	Add ASPC Policy / reformat document
Version 2.0	6-15-09	Kim Snyder	AzHeC review
Version 3.0	6-30-09	Kim Snyder	AzHeC review

Policy Definitions

- Authorized User (User) means a Participant and its employees and agents authorized by Participant to use the Health Information Organization (HIO) to access Data for the purposes of medical treatment and health care services to Participant's Patients.

- Data means Patient health information provided to an HIO by a Participating Entity and accessible to Authorized Users. For the purposes of this Agreement, Data means Protected Health Information (PHI) as defined by Standards for Privacy of Individually Identifiable Health Information, and the Security Standards, 45 C.F.R. Part 160 et seq. as amended from time to time.

- Data Provider means Participant who provides Data to the HIO.

- Electronic Credential means the credential used by the system to authenticate a User (i.e. digital signature).

- Health Care Provider means a clinician, hospital, pharmacy, laboratory, etc. that provides medical treatment or health care services to Patients and who has entered into an HIO Participation Agreement.

- Health Information Exchange (HIE) means the electronic movement of health-related information among organizations according to nationally recognized standards.

- Health Information Organization (HIO) means the organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.

- Non-repudiation means a party in a dispute cannot repudiate, or refute the validity of a statement or contract.

- Participant, Participating Health Care Provider or Participating Entity means a Health Care Provider who has entered into an HIO Participation Agreement, either as a Data Provider or a Data User. This can also be referred to as the "organization".

- HIO Participation Agreement means an agreement between a Participant and the HIO.

- Identity Service Provider means a service provider that stores identity profiles and offers services for managing those profiles.

- Patient means an individual receiving medical treatment or health care services from a Participant.

- Policies mean these HIO policies.

- Protected Health Information (PHI) means confidential, personal, identifiable health information about individuals that is created or received by a health plan, provider, or health care clearinghouse and is transmitted or maintained in any form.

- Registration Authority means an entity that is responsible for identification and authentication of Users.

- Regulated Healthcare Organization means an officially registered organization that has a main activity related to health care services or health promotion.

- Regulated Health Professional means a User who is authorized by a nationally recognized body and qualified to perform certain health services.

- Use Agreement means the Data sharing agreement between a Data Provider and the HIO.

- Permitted Use means the permitted use of health information by a covered entity under HIPAA as follows:[1]
    - §164.502. A covered entity is permitted to use or disclose protected health information as follows;
    - To the individual who is the subject of the information;
    - For treatment, payment, or health care operations, as permitted by and in compliance with §164.506;
    - Incident to a use or disclosure otherwise permitted or required by subsection (a)(1) of §164.502 provided that the covered entity has complied with the applicable requirements of subsection (b) of §164.502, subsection (d) of §164.514, and subsection (c) of §164.530;
    - Pursuant to and in compliance with an authorization that complies with §164.508;
    - Pursuant to an agreement under, or as otherwise permitted by, §164.510; and
    - As permitted by and in compliance with subsection (a)(1) of §164.502, §164.512, or subsections (e),(f), or (g) of §164.514.

[1] HIMSS Privacy and Security Toolkit Managing Information Privacy & Security in Healthcare, Protected Health Information: General Rules on Use and Disclosure, By Sandra J. Sinay, JD, LLM and Barbara Demster, MS, RHIA, CHCQM © January 2007 Healthcare Information and Management Systems Society. http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D19_Protected_Health_Information_General_Rules_on_Use_and_Disclosure.pdf.

Note: The following section on patient consent contains what the policy should cover, however it does not define what the policy is. This section of the policy will be updated when a consent policy is determined in Arizona.

Consent Policy

Section 1

1.1 Patient Consent for Submission of PHI to an HIO

Three types of consent can be considered when asking Patients to allow their PHI to be part of the HIO:

- Opt-in;
- Opt-out; or
- No consent required.

The Policy should cover:

- What Participant/Participating Entity administers opt-in or opt-out process and secures relevant document (broadly called the "consent document" in this policy)
- Timing and duration of opt-in or opt-out
- Form of consent document
- Maintenance of consent document
- Access to consent document
- Data covered by the consent document
- Restrictions on Data subject to consent document
- Revocation/amendment of consent document

1.2 Notice of HIO Practices

The HIO will create a document ("Notice") containing the following information:

- Description of the HIO.
- A statement that the patient Data is included in the HIO.
- A statement that Authorized Users may access the Data for Patient's care and treatment.
- If opt-in or opt-out approach is adopted, how the Patient can have his or her Data added to or removed from the HIO, respectively. Note: Process will have to be identified for removing Data or limiting access even if Data not removed.
- If technology permits, whether/how the Patient can have access to the Data submitted to HIO.

1.3 Provision to Patients

The HIO will maintain the Notice and make it available to the public through the common portal. [In addition, a Participant will provide the Notice to a Patient at the date of first service

delivery after the Participant's agreement to participate in the HIO and anytime requested by a Patient.]

Authentication Policy

Section 1 - Use Agreement

1.1 Requirement - Use Agreement

Health Information Organizations (HIOs) should have a Data sharing agreement with participating Providers that defines the privacy and security obligations of the Participants in the HIO. These agreements should require the use of appropriate authentication methods for Users of the HIO that depend on the Users' methods of connection and the sensitivity of the Data that will be exchanged. In addition, these agreements should reasonably ensure sufficient auditing requirements to determine access and use of the system, as well as secure transport of health information across the network, as appropriate.

Where there is cross-HIO exchange of Data, authentication and audit requirements should be defined through a Data Use and Reciprocal Support Agreement (DURSA). The DURSA should define their relationship between the HIOs and ensure, among other things, appropriate authentication and audit of Users and queries across HIOs.[2]

Each Participant is responsible for determining which of its employees and agents will be Authorized Users. A Participant may allow access to the HIO only to those employees and agents who need to use the HIO to access Data related to the Participant's care and treatment of Patients on behalf of the Participant.

Each Participant will develop and implement a training program for its Authorized Users. The training will include a detailed review of these Policies. In addition, each Authorized User must sign a certification that the Authorized User received, read, and understands these Policies and completed the training.

The HIO may also have a training requirement that must be taken into consideration during the User's training.

Section 2 - Identity Registration

2.1 Required Data Set for Authentication

A directory of Data sources within the HIO will include primary contact information of registered Users and identity attributes of Users, Participants and systems.

[2] Markle Foundation – Connecting for Health - http://www.connectingforhealth.org/ Reference: M2: A Model Contract for Health Information Exchange and P2: Model Privacy Policies and Procedures for HIE.

2.1.1 Data Source

A directory of Data sources within the target HIO is required, and must include name of the HIO and any Data sources within that HIO. The primary contact information for the Data in the directories should include primary contact name and any contact phone numbers.

2.1.2 User Identity Attributes

The HIO will collect the attributes as needed for unique identification of the User accessing the information in the HIO.[3] Required elements are profession, role, name, the practice address (not home address), identity service provider and Participant affiliation, business/legal address and License/ID. Other attributes that are required, if they exist for this User, includes:

- Specialization / specialty,
- Email address,
- National Provider Identifier (NPI), if applicable,
- Digital identity, and
- DEA Number, if one exists.

Every User of the HIO must be identified and affiliated with at least one Participation Agreement and the HIO system should allow for multiple affiliations. The HIO must have a method for identifying administrative Users who are working at the HIO with access to PHI.

2.1.3 Participant Identity Attributes

Identifying the Participant requires collecting the following attributes: organization name and email address. Other attributes are required if they exist, including:

- Digital identity,
- Electronic Data Interchange (EDI administrative contact,
- Clinical information contact,
- Service location, and
- Predecessor name and date of change.

If the HIO is a Regulated Healthcare Organization, all supporting Participant attributes above are required, as well as:

- License/ID,
- License status,
- Registered name, and
- Registered address.

Participants must have unique and persistent organization identifiers, and unambiguously equate to a corresponding Participation Agreement.

[3] 45 C.F.R. § 164.312(a)(2)(i) (requiring assignment of a unique name or number for identifying and tracking User identity).

2.1.4 Identity Attributes of the Data Source System

Identifying the Data source system requires the attributes of:

- System name,
- Digital identity,
- Participant affiliation,
- System IP address, and
- System domain name.

If there is no system domain name, the system IP address may be used. For purposes of identifying the originating electronic Data sources, it is required that a date stamp and at least one of the following is provided: the (1) system name, (2) IP system address, or (3) system domain name. Any identifying system types, such as the laboratory information systems, electronic health record system, emergency medical system, etc. should also be included.

2.2 Role-based Access

Proper registration requires the establishment of a defined role associated with the registered User. If role-based access is established it must be in accordance with the current RBAC (role-based access control) national standards, established by Health Level 7 (HL7).

2.2.1 Role

The individual's Participant role[4] is required for role-based access and should include the context of the Participant. If the healthcare functional role[5] or the structural roles[6] exists, they are also required.

Section 3 - Verifying Identity

3.1 Processes Used to Verify Identity

Identity is verified through authentication of the User, the Participant and the HIO's system.[7]

3.1.1 User Authentication

The methods for User identity vetting include both verifying the identity in person by a trusted authority and verification through the use of a demonstrated government-issued ID.

[4] As defined in the American Health Information Community (AHIC) Use Cases.
[5] The functional role is dynamic and is a function of the role in which you are acting.
[6] A structural role is persistent and can be mapped to professions that are recognized.
[7] 45 C.F.R. § 164.312(d) (requiring "procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed").

At a minimum, an HIO should establish a trusted relationship with a Participant where the authority to identify the Users is delegated to the Participant affiliated with that User (see AzHeC Model Participation Agreement as an example).

A User requesting an identity tied to a regulated health professional must have provider licensure validation. It is acceptable that this occur along with the validation required of any employee of a licensed provider Participant.
Also, the HIO use of a specific naming convention as a primary identifier is required with a minimum assurance level used of Medium (knowledge/strong password/shared secret).

Identifiers can be issued by the HIO or they can be adopted from an external source as long as that source guarantees the uniqueness and persistence of any identifier.

3.1.2 Participating Entity Authentication

Participating Entity identity vetting can be accomplished through personal knowledge of a Registration Authority, affirming that the Participant is who they say they are by a demonstrated documentation of corporate existence.

The HIO is required to use a specific naming convention as a primary identifier, and this would include the use of object identifier (OID) or idiosyncratic naming, if either of these exists.

Participants must sign a Participation Agreement.

The minimum assurance level required for Participant authentication is Medium (knowledge/strong password/shared secret).

3.1.3 System Authentication

System identity vetting, ensuring the Data are coming from the system that they are supposed to be coming from, requires the assertion by an authorized Participant representative and/or the demonstration of association with another licensed Participant.

The system IP address is required.

The minimum assurance level required for system authentication is High (PKI/Digital ID).

3.2 Variations Based On Type and Location of User

3.2.1 User Identity, Role and Affiliation Verification

The User identity, role and affiliation must be checked for both revocation and expiration at the time of logon to the system. If either case pertains, use would be denied.

3.2.2 Signature Verification

The HIO is responsible for digital verification of non-repudiation signer credentials. Verification implies that:

- The credential was issued by a trusted authority,
- The credential is current,
- The credential is not suspended or revoked, and
- The credential type is appropriate (for example, physician or pharmacist), based on the role.

3.2.3 Assurance Level

It is required that the level of assurance be declared and should be communicated in terms of the then current National Institute of Standards and Technology (NIST) requirements. For the HIO to migrate Data to the User, an assurance level of at least Medium (knowledge/strong password/shared secret) is required.

3.2.4 Relationship to Patient

If the HIO is exchanging Data for purposes of treatment, the User seeking access needs to demonstrate or certify that they have a treatment relationship with the Patient.

3.2.5 Persistence

The use of persistence[8] of the source signature is required and is the responsibility of the HIO with its own Participants. The attributes required are persistent User signature, persistent Participant signature and persistent system signature. Non-repudiation of origin is also the responsibility of the HIO with its own Participants, and includes the attributes of User, Participant and system accountability. If source authentication exists it is also required.

3.3 Accommodations for Cross-HIO Verification and Data Integrity

3.3.1 Restricted Data Sharing and Data Integrity

The transmission of caveats regarding Data completeness is required to indicate that an entire record may not have been transmitted. The use of any existing, pertinent state-specific caveats should be included in the transmission.

3.3.2 Authentication of Recipient Identity (Organization / System / User)

The identity of the recipient must be established and the method of identifying recipients of communications can include, but is not restricted to: (1) derived from

[8] Persistence indicates proof that Data has not been altered and is only valid during the communication session.

ordering system communications, (2) selected from a provider directory, or (3) derived from identifiers included in the request for information.

3.3.5 Data Integrity

For the purposes of cross-HIO verification, the ability to use digital signatures is required at the User level, if available, in order to ensure data integrity. If the digital signature is not available, cross state exchange is still permitted.

3.3.6 Persistence

The use of persistence of the source signature is required and is the responsibility of the HIO with its own Participants. The attributes required are:

- Persistent User signature,
- Persistent Participant signature and,
- Persistent system signature.

Non-repudiation of origin is also the responsibility of the HIO with its own Participants, and includes the attributes of:

- User Accountability,
- Participant Accountability, and
- System accountability.

If source authentication exists, it is also required, however if source authentication is not available cross state exchange is still permitted.

3.3.7 Data Authentication

For purposes of Data authentication, the use of a timestamp is required at the point of signature application.

3.3.8 Data Validation

Data validation of signer credentials issued by a trusted authority should be current, and the credential should not be suspended or revoked, and the credential type should be appropriate (for example, physician, pharmacist or hospital). For purposes of Data integrity, the Data validation should indicate that the Data has not been changed since the signature, and should have a timestamp at the point of signature application.

3.3.9 Type of Requestor

For verification purposes the requestor type should identify the HIO, Participant (entity) and the User (individual).

3.3.10 Signature Purpose

The signature purpose should be included as a minimum requirement, and any of the captured signature elements that exist should be included.

Section 4 - Identity Provisioning

4.1 Types and Levels of Factor Provisioning

Refer to Section 3 for the required assurance levels for User, Participant and system authentication

Section 5 – Identity Maintenance

5.1 Registration Data

5.1.1 Type of Data Maintained

The following types of Data should be maintained for each User:

- NPI, if applicable,
- DEA,
- Name,
- Specialty,
- Address,
- Email, and
- License Number.

5.1.2 Responsible for Maintenance

If the Users are registered by a Participating Entity then the maintenance is shared. Once the HIO receives the User profile from the Participant, it should be processed in a reasonable timeframe. For Users who are accessing the HIO through the Registration Authority, procedures will need to be in place at the HIO for maintaining the information.

Participants that provide the User credentials to the HIO should be responsible for validating who the Users are based on the User access at the Participant organization.

5.2 Re-registration

5.2.1 Forced Timeframes

Participant is responsible for informing the HIO of any change in status of any User whose access is regulated / controlled by the HIO and the HIO in turn is required to reset access as needed within a specified timeframe.

All Users must be affiliated with at least one Participation Agreement.

5.2.2 Information Validity at Re-registration

Information received at re-registration should be validated by the HIO using the same process used for a new registration**.** Re-registration must occur on at least a yearly basis.

5.3 Password Maintenance

Password Maintenance applies to the revoking of passwords, forgotten passwords and forced timeframes.

Password policy should apply to all servers, applications, databases, computer workstations, laptops, mobile computing devices and network equipment used to access PHI. Password procedures must cover the following:

- Password expiration timeframe,
- Prohibition against re-use of passwords,
- Minimum age of a password,
- Timeframes for locking passwords due to invalid logon attempts,
- Process for reissuing lost passwords, and
- Password strength defined using the National Institute of Standards and Technology (NIST) guidelines.

Suggestions for password maintenance include:

- Passwords expire every 90 days,
- A password can't be re-used for one year,
- Default passwords are changed on initial logon,
- A password can't be left blank,
- The minimum age for a password is one day,
- An individual account is locked after three consecutive invalid logon attempts,
- A lost password will require the User to logon and answer a security question to get the password reset, and
- A strong password is 8 characters in length using at least one upper case letter, one lower case letter, one number and one symbol.

5.4 Automatic Logoff

Automatic logoff procedures must be defined in the HIO policy.
Recommendation is that a User be automatically logged off the system after 15 minutes of inactivity.

5.5 Simultaneous Logon

Simultaneous logon is allowed as long as there is a process in place to notify the User that they are logged in more than once and giving the User the option of logging out on the idle computer. Also an automatic logoff procedure should be in place to log a User off after a period of inactivity (see Section 6.4).

An audit check for abnormal logon patterns should be in place.

5.6 Delegated Maintenance Functions

Maintenance of the User access to the HIO is delegated to the Participant.

5.7 Termination Policies and Procedures

There must be a minimum timeframe for freezing / suspending an account for inactivity by a User. The recommended timeframe is 90 days.

A participant must terminate an Authorized User's access to HIO if:

- A User is no longer an employee or agent of the Participant,
- The Participant decides to terminate Users access to HIO for any reason,
- A User doesn't comply with terms and conditions of the Participation Agreement or Policies, or
- The HIO requests that a User's access be terminated. The Participant will notify the HIO immediately when the User's access to the HIO ends for any reason and the HIO will remove the User from the HIO.

Data Use Policy

Section 1 – Access

1.1 Patient Access

A Participant must provide a Patient with the Patient's medical record, including Data secured from the HIO upon the Patient's request.

1.2 Authorized User Access

An Authorized User may access Data only for care and treatment of a Participant's Patients.

Section 2 – Non-Compliance

2.1 Non-Compliance

Each Participant must implement procedures to discipline and hold Authorized Users accountable for violating these Policies or using, disclosing, or requesting a Patient's Data for any reason other than Participant's care and treatment of the Patient.

The disciplinary measures must include, but not be limited to, verbal and written warnings, demotion, and termination. The disciplinary measures may provide for retraining where appropriate.

Authorized Users must report to the Participant any noncompliance with these Policies or the Participant's policies on Data access, use or disclosure. Each Participant must have a process for Patients participating in the HIO to report to the Participant and/or HIO any non-compliance with these Policies and any concerns about Data access, use or disclosure. A Participant must immediately report any noncompliance with the HIO's or Participant's policies for Data access, use or disclosure to the HIO.

Data Submission

Section 1 – Data Submission

1.1 Accuracy

Participants may not provide the HIO with Data that they know is not accurate.

1.2 Amending Information

Each Participant must comply with applicable federal, state and local laws and regulations regarding Patient rights to request amendment of Data.

1.3 Limiting Information Provided to HIO

If a Participant agrees to a Patient's request for restrictions, the Participant must comply with the restrictions when providing Data to the HIO. If an agreed-upon restriction could affect another Participant's use of the Data, the Data Provider must notify the HIO of the fact that certain Data has been restricted, without disclosing the content of the restricted Data.

1.4 Special Information

Some Data may be subject to special protection under federal or state laws and regulations (for example, substance abuse treatment information held by federally-assisted substance abuse treatment programs, psychotherapy notes, and genetic testing information). The HIO will determine and identify special protection that may apply to Data under applicable law and notify Participants of these restrictions. Each Participant will be responsible for identifying Data subject to these special protections and following HIO rules regarding provision of this Data to the HIO.

Audit Policy

Section 1 - Logging and Audit Controls

1.1 Logon Monitoring[9]

As a part of logon monitoring, an audit log is required to be created to record when a User logs on to the network or a software application of the HIO. This includes all attempted and failed logons.

The generated audit logs must be reviewed on a regular basis that is based on an audit criteria developed in advance. Anomalies must be documented and appropriate mitigating action documented. The HIO should determine how long its state laws and risk management policies would require retention of this documentation.

The HIO will audit use of the system to assure appropriate use by Participants and authorized Users and system accuracy.

Random audits of Participants and Authorized Users may be conducted.

Random audits will be conducted by the HIO or an HIO-authorized third party.
The HIO will notify the relevant Participant of any inappropriate use, or any privacy and / or security breach identified through the audit.

Unsuccessful logon attempts and access violations within the system must be logged.

1.2 Information Systems Review[10]

All HIE systems must be configured to create audit logs that track activities involving electronic PHI. The review of information systems shall include software applications, network servers, firewalls and other network hardware and software. The generated audit logs shall be reviewed on a regular basis based on audit criteria developed in advance. All anomalies must be documented and appropriate mitigating action taken and documented. All system logs must be reviewed. The review shall include, but not be limited to, the following types of actions: read, write, update, delete or copy. The HIO should determine how long its state laws and risk management policies would require retention of this documentation.

[9] HIPAA Security Rule: 45 C.F.R. § 164.312(b) (requiring "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information"); 45 CFR § 164.308 (a)(5)(ii)(C) (requiring procedures for monitoring logon attempts and reporting discrepancies).
[10] HIPAA Security Rule 45 CFR § 164.308 (a)(1)(ii)(D) (requiring covered entity to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports").

Specifically:

- Network intrusion detection system activity logs must be reviewed.
- System Administrator authorizations and activity must be reviewed.
- Security Administrator functions must be logged and reviewed.
- Audit records must be readily available for 90 days and archived for a minimum of two years, or up to the six years used for the archiving of HIPAA disclosure.
- All destruction of audit logs and materials will cease in the event that there is knowledge of or involvement in a lawsuit.
- The HIO will develop and follow policies and procedures for document retention and destruction policies that will apply to audit logs and other documents produced.

1.3 System Review

Information system reviews should be conducted on a regular and periodic basis, as determined by the HIO.

Required system logging includes:

- System to system
- Source device
- Destination device
- Activities by each gateway
- Emulator and exchange website
- All Databases
- IP monitoring

1.4 Security Audit Practice

The frequency of performing regular security audits shall be determined at a specified frequency for the HIO. Auditing frequency typically varies by state/HIO (for example, Nebraska conducts audits annually, and Washington conducts quarterly audits). Audits shall be conducted at least annually as a minimum requirement, and the comprehensive audit procedures should be developed, documented and available. The HIO should also conduct periodic external audits.

1.5 Audit Trail and Node Authentication (ATNA)

The Audit Trail and Node Authentication Integration Profile[11] requires the use of bi-directional certificate-based node authentication for connections to and from each node. The use of certificates or encryption is required when the Data are signed or when it is specified by the HIO policy.

[11] IHE: Integrating the Healthcare Enterprise

Section 2 - Periodic Internal Compliance Audits

In order to appropriately assure the security of PHI, the HIO shall perform internal audits to evaluate their process and procedures.

Technical, physical and administrative safeguards established by the policies of the Participant are reviewed at least annually or when a major business process or technical change occurs.

2.1 Evaluation[12]

Under HIPAA security standards, administrative safeguards are required in order to exchange electronic PHI. Users of the HIO need to comply with all privacy and security regulations when exchanging electronic PHI.

Additionally, periodic technical and non-technical evaluations are required to reasonably ensure that the covered entity is compliant with the provisions of the HIPAA Security Rule. Audit criteria must be developed and documented in advance for this type of evaluation, known as a "compliance audit." Evaluations shall be performed at least annually and when any major system or business change occurs. The evaluation shall include:

- The generation of a compliance audit findings report,
- The documentation that an identified deficiency has been addressed, will be addressed in order of priority, or represents a risk that the Participant is willing to accept, and
- The retention of evaluation documentation for a minimum of six years.[13] Some states, however, may have longer retention requirements.

Section 3 - Information Access

3.1 Audit Controls[14]

Under HIPAA security standards, technical safeguards are required including policy, Data, and system requirements. All entities and their business associates must implement technical processes that accurately record activity related to access, creation, modification and deletion of electronic PHI.

3.2 Subject of Care Identity

To identify the identity of the Patient, a matching criteria policy is a required (for example, a match on Date of Birth, First Name, Last Name, Address, etc…)

---

[12] HIPAA Security Rule 45 CFR § 164.308 (a)(8) – Evaluation

[13] 45 C.F.R. § 164.316 (requiring retention for six years of policies and any required activity that must be documented under the rule). While 45 C.F.R. § 164.308(a)(8) does not require documentation of the compliance audit, it is a good business practice to do so and to retain that documentation for risk management purposes.

[14] HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls

3.3 Demographics That May Be Logged

An additional audit log should be performed by the HIO for a subset of the subject identity attributes that have been used when a Patient is found.

Section 4 - Need to Know/ Minimum Necessary for Data Management and Release

4.1 Information Disclosure

For purposes of information disclosure, a written policy is required which includes documentation of the following:

- The date and time of the request,
- The reason for the request,
- A description of the information requested, including the Data accessed, the Data transmission, any changes to the Data (adds, changes, deletes), and whether the Data were transmitted to another party,
- The ID of person/system requesting disclosure,
- The ID/verification of the party receiving the information,
- The ID of the party disclosing the information,
- The device used to authenticate the User, if applicable,
- The source Participant of an access request.

4.2 Auditing Access Where Individual Consent or Authorization is required

An authorization policy must be in place for any exchange of PHI, and requires the audit log to identify whether the release requires an authorization and, if so, whether the authorization was obtained.

A consent ID would be required, if it exists, for transactions that require a consent or authorization to be tracked for audit purposes.

Section 5 - Need-to-Know Procedure/ Process for User Access to PHI

5.1 Information Request

For purposes of information requests, a written policy is required that includes the following components:

- The date and time of the request,
- The reason for the request,
- A description of information requested, including the Data accessed, Data transmission, any changes to the Data (adds, changes, deletes), and whether the Data were transmitted to, or printed by another party,
- The ID of User/Participant/system requesting disclosure,
- The ID/verification of the User/Participant receiving the information,
- The ID of the Participant disclosing the information,

- The method used for verification of the requesting Participating Entity's identity.

An authorization policy must be in place for any exchange of PHI and requires the audit log to identify whether the release requires an authorization and if so, whether the authorization was obtained.

A consent ID is required, if it exists, for transactions that requires a consent or authorization to be tracked for audit purposes.

5.2 Audit Log Process

The HIO's audit log procedure shall be developed and documented prior to any HIO exchange of PHI and shall include identifying who is responsible for reconstitution and sharing audit log information. This includes identifying who is authorized to request the audit log. Also, the procedure shall identify whether or not the audit log information is available to individuals and if so, how that request is handled.

5.3 Data Authentication

If a document is shared with a patient, methods for assurance shall be established and shall indicate that Data have not been modified.

5.4 Preparing a Query Message

When an HIO generates a registry stored query, a registry or Record Locator Service (RLS) will be asked if there are records for this Patient [Refer to HITSP IS01].

Section 6 - System Capabilities

6.1 Audit Controls[15]

Audit logs are required to record activity specified by the HIO and the HIO shall periodically review the generated audit logs. This review of the audit logs is based on established audit criteria and shall include documentation of any anomalies. The HIO will document its mitigating action (including sanctions, security incident response team activation, etc., as appropriate). Audit logs must include at least the following:

- Unique User name/ID,
- Date/time stamp, and
- All actions taken (read, write, update, delete or copy).

Audit logs should either be in readable form or translatable by some easy to use tool to be in readable form, and must be examined with some frequency appropriate to the HIO in order to detect improper use.

Additional audit controls include:

[15] HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls

- A User's log recording logon and logoff Data will be maintained,
- Audit logs must be kept of HIO-enabled functionality with respect to accessing confidential and restricted Data initiated by Authorized Users and systems for access directly supported by the HIO,
- The system should have the ability to log queries; or alternatively the tables read must be logged,
- Row-level logging must be available on demand,
- A Participating Entity's identifier must be unique and persistent and unambiguously equate to a corresponding Participation Agreement, Identifiers can be issued by the HIO or they can be adopted from an external source as long as that source guarantees the uniqueness and persistence of any identifier,
- An HIO User's identifier must be unique and persistent,
- Audit records must include the User's identifier,
- Audit records will include the source (the Participating Entity) of the access request, and
- The User must have at least one Participant Agreement on record.

6.2 Audit Log Content

The HIO's audit logs shall include:

- User ID,
- A date/time stamp,
- Identification of all Data transmitted, and
- Any authorizations needed in order to disclose the Data.

The audit log shall include any system activity of use and disclosure of Data, and shall retain a record of information systems activity that occurs at established periodic time frames. The audit log for the use and disclosure of Data is also required to have a set report in place. Actions that have been identified in the event of discovered anomalies/breaches shall be included in the audit log. Also, logon auditing is required as noted under the HIPAA Security Rule auditing standard. If it exists, any state-specific[16] consent policy under which the Data were disclosed shall be tracked. This may be a global consent policy or a specific consent for each access.

If sensitivity restricted information exists, the HIO may choose to implement restrictions as permitted under their state.

6.3 Information Integrity

Information integrity is audited by logging that no change has occurred since the signature was applied and shall include a valid date/time stamp.

6.4 Data Authentication

For purposes of Data authentication, the use of a valid date/time stamp is required.

[16] For example, the consent policy of the State of Massachusetts.

6.5 Data Validation

For the purposes of Data validation, the signer credentials must be from a trusted authority (certificate authority), and the credential must be current and without constraints, and the credential must be of the appropriate type for the requested Data (for example, physician or pharmacist). To ensure Data integrity, credentials shall indicate that no change has occurred since the signature was applied and must have a valid date/time stamp.

6.8 Simultaneous Logons

Multiple concurrent logons must be logged and reviewed.

Governor's Office of Health Information Exchange

Arizona Health Information Exchange (HIE)

Appendix C

Arizona Health Security Project

Overview of Basic Authentication Concepts Useful to Health Information Organizations

Generated by the stakeholders supporting Arizona's participation in Phase III of the Health Information Security & Privacy Collaboration. The Collaboration is supported and funded by the U.S. Department of Health and Human Services.

In cooperation with the Arizona Government Information Technology Agency and Arizona Health-e Connection
3/31/2009

Table of Contents

1. Introduction and Purpose

Managers responsible for the security environment of a health information organization (HIO) focus on services associated with the 4 "A"s – Authorization, Authentication, Access and Audit. One of the 4As - *Authentication* - includes the responsibility for managing the identity credentials of those attempting to access healthcare data. The proper management of identity credentials allows an organization to *authenticate*, or unambiguously verify, who a user is before authorizing that user's right to access specific categories of information.

The purpose of this whitepaper on authentication is to provide an overview of authentication system characteristics, identify ways those systems can be evaluated, and provide a basic subset of common authentication options commonly used in the healthcare environment.

2. Context and Definitions

This paper discusses managing identity credentials in the context of authenticating healthcare providers accessing a health information exchange for treatment purposes. While the authentication of healthcare providers is just one example of the identity management services performed by HIOs, the fundamentals underlying provider authentication can be applied to other users of the system.

The following concepts apply to this authentication discussion below:

Identity – Identity is an individual person or institution needing access to healthcare data. An identity is not merely a role; it is an actual person or institution. It is not enough to know that the user is a doctor, but that the user is Howard M. Williams, MD.

Identifier – An identifier is an attribute that points unambiguously and uniquely to an identity. For instance, an employee ID number identifies only one employee in an organization.

Authentication – Authentication requires a user with an established identity to provide an identifier that will prove identity, establishing that the user is who he/she claims to be.

Health Information Exchange (HIE) – HIE means the electronic movement of health-related information among organizations according to nationally recognized standards.

Health Information Organization (HIO) - HIO means the organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.

3. Authentication System Characteristics

There are different factors and combinations of factors used in an authentication system. These factors are commonly grouped into the following three categories:

- Something you know (a password)
- Something you have (ID badge, cryptographic key, proximity card)
- Something you are (voice print or other biometric)

Section 4 of this report provides details of some commonly used authentication factors in each of the above categories. There is a brief description of how each factor works and a summary of the pros and cons associated with each factor.

Authentication systems can be made stronger by requiring a combination of factors to authenticate users. A system requiring two different categories of factors is stronger than one requiring two types of the same category. For example, a system requiring both a password (something you know) and a fingerprint scan (something you are) is stronger than one requiring a password and a PIN (both something you know). When more than one category of factor is used, the system is referred to as having multi-factor authentication (two-factor or three-factor). Using one or more methods that all belong to the same category is termed single-factor authentication. In all cases, the terms can apply to either people or objects. Thus, a computer can present its identifier to another computer using something like a digital certificate, just as a user can provide an identifier consisting of a password or a token.

The goal of a healthcare authentication system is to protect healthcare data, but the system must always balance the user's need for quick and easy access against the requirement to keep the healthcare data secure by applying stringent requirements for establishing a user's identity. HIOs understand that they can only create and maintain trust in their systems by avoiding authentication errors.

To better understand possible authentication errors, it is helpful to identify, describe and compare the varying levels of authentication. The National Institute of Standards and Technology (NIST) in its Electronic Authentication Guideline identified four levels of assurance. Those levels and their characteristics are summarized in the table below: (William E. Burr, April 2006)

Level #	Type	Level of Assurance	Characteristics
Level 1	Single factor, no identity proofing	Little confidence user is who they claim to be	Simple password challenge-response protocol allowed – secrets may be revealed to verifiers

Level #	Type	Level of Assurance	Characteristics
Level 2	Level 1 + identity proofing	Somewhat confident user is who they claim to be	Passwords, PINs, tokens; requires approved cryptographic techniques
Level 3	Level 2 + multi-factor authentication	Very confident user is who they claim to be	Three types of tokens – soft cryptographic token, hard cryptographic token and one time password tokens can be used
Level 4	Level 3 + hardware cryptographic tokens	High confidence user is who they claim to be	Hard cryptographic tokens are required

In addition to understanding the relative ease of use and characteristics of each authentication level, HIOs must consider the expense and complexity associated with implementing and maintaining each level. Increased levels of assurance can be costly and complex. Complex systems often then suffer from low user acceptance. When determining the level of assurance needed, organizations must carefully balance expense and complexity against the risk associated with an authentication failure.

4. Authentication Options

The following section provides detailed examples of authentication methods by category and provides general information about how specific authentication factors work, along with important pros and cons of using that authentication factor.

Something You Know

The factor category of *Something You Know* authentication includes security factors based on information an individual retains by memory or in a written form that can be replicated and communicated by standard communication means, e.g., mail, fax, over the phone, or e-mail. Security may be associated with distributing the information, but the information itself is not encrypted. Examples of these factors may be passwords or phrases, PINs, or responses to pre-determined questions in a challenge/response scenario. The advantage of these factors is their widespread current use for access to networks and application systems, the user community's familiarity with them, and their universality of use across cultural and political environments. Costs of these factors are primarily limited to the distribution and re-issuance of the information through a help desk or through a web-based application/e-mail redelivery scenario like those used by most web subscription services. Their major drawback is that the information (the password or phrase) can be forgotten or lost, disclosed to inappropriate individuals, or guessed/hacked by software programs. In these cases, re-issuing the factor is the only available

method of recovery. Installation and implementation costs are relatively low, and range from current provider-based systems which might carry no implementation cost, to standalone software products that would require costs of up to $8,000 for software and $3,000 for servers. These higher-end systems would easily sustain thousands of user access records, bringing the per user cost down below the $1 threshold. It is generally accepted that *Something You Know* factors are the least secure factors and are not sufficient as a single factor for authentication. Multiple instances of *Something You Know* can be used to increase the security level, but multiple instances are also likely to increase the error rate as every response must be correct to complete the authentication session.

USER PASSWORD

How the technology works	The user generally provides an *identifier* (User ID) previously obtained by providing appropriate proof of *identity* to the managers of the authentication system. The user then chooses a password to be used with the identifier to gain access to the system. The managers of the authentication system know and manage all the User IDs associated with the system, but only the user knows both the identifier and the chosen password.
Pros	• High user acceptance and widespread use • Most systems have the capability to enforce secure passwords built in, allowing organizations to acquire and configure authentication controls easily and inexpensively • Low per user cost
Cons	• When password formats become complex enough to heighten security, users have increasing difficulty remembering and using them appropriately • Requires creation and continual enforcement of strong associated security policies to provide effective protection • Users can easily share their passwords and may do so inadvertently by retaining written records of them • Become less secure over time because users reselect the same password for multiple applications and because these applications generally do not require PINs to be reset at frequent intervals

Because the requirement to provide a User ID and Password for authentication is ubiquitous in today's security environment, it is worth examining requirements for user passwords in detail. Many systems contain configurable password requirements that allow organizations significant control over the level of security actually in effect. It is essential that organizations review the default password requirements set in their systems and reconfigure those requirements to meet their specific security needs. Some good options that can be chosen to improve security include:

- Allowing or requiring a mix of upper and lower case characters, numbers and special characters, and requiring a minimum password length
- Automatically forcing passwords to expire periodically and restricting reuse of passwords
- Restricting the number of consecutive unsuccessful attempts to log in
- Setting sound security procedures in place for revoking and resetting passwords
- Making system users responsible for securing their passwords and accountable for system activities performed under their logins

- Associating a user ID and password with one specific individual, never with multiple individuals such as those performing the same role.

Training system users about the value of sound security policies can increase their acceptance of stronger password requirements and significantly reduce the risk of an authentication failure.

PERSONAL IDENTIFICATION NUMBER (PIN)

How the technology works	A PIN is a 4 to 7 digit number chosen by a user, usually as one part of a multi-factor authentication system. The user is expected to commit the number to memory and provide it as an electronic signature that allows the system to authenticate the user. PINs are normally entered using a keypad and are usually not sent across the network to avoid interception.
Pros	• Quick and easy to enter • Short enough to be committed to memory • Can easily be used on devices without full keypads
Cons	• Not secure enough to be used as a single factor to authenticate • Often shared with friends or relatives • Become less secure over time because users reselect the same PIN for multiple applications and because these applications generally do not require PINs to be reset at frequent intervals

CHALLENGE/RESPONSE QUESTIONS

How the technology works	A system may ask a user for multiple pieces of information, or for information, such as a previous address, that is historically based and not normally found somewhere like the user's wallet. The system may also vary the information requested with each access to decrease an imposter's likelihood of having the necessary information. The challenge/response scenario can be made even more secure if users are able to configure some of the challenge questions.
Pros	• High user acceptance and widespread use • Allows validation of a broad range of users such as consumers, who do not have consistent unique identifiers such as an employee number or license number associated with the system they are accessing • May be required as needed to protect systems sometimes accessed from public or shared computers
Cons	• Requires additional data to be stored for each user • Challenge/response scenarios are typically implemented by more complex and expensive systems • Time requirements to complete the authentication process can be too lengthy for some business processes

Something You Have

Authentication can be based on something a user has. Various token and card technologies support this type of authentication. Two-factor authentication is an important authentication process that involves two independent means of authenticating the user. Something the user knows, such as a secret password (for example, PIN or password) can be required, as well as the possession of a device. Without two-factor authentication, a stolen device would allow an attacker to impersonate the user of the device, but with two-factor authentication, the attacker would still have another authentication requirement to meet.

Authentication factors based on something a user has include:

MAGNETIC STRIPE CARDS

How the technology works	Magnetic Stripe Card technology has been in use for decades and is found in credit cards and ID cards, and is used for building access, mass transit and many other uses. The stripe uses magnetic material to store data. Data is encoded by setting the polarities of the magnets, and the readers detect changes in polarity signifying a binary value of "0" or "1." Magnetic Stripe Cards are commonly one part of a two-factor authentication process requiring the user to know a 4 to 7 character PIN whenever the card is used.
Pros	• User acceptance is high • Has a history of successful use in everyday applications • Add security because they are not in human readable form • No moving components, physically robust
Cons	• Easy and inexpensive to duplicate • Can easily be lost or stolen • Data can be damaged by stray magnetic fields • Requires close contact with the card reader

DIGITAL CERTIFICATES

How the technology works	Digital Certificates are issued by a server and are unique for each user. Users can be sent an email containing their user ID, a one-time password and a digital certificate enrollment web address. The user installs the digital certificate (software) on the computer that is used to access a secure website. Upon login, the server sends its own digital certificate to the user's computer and requests the user's unique digital certificate. After these certificates are exchanged and verified, the login is completed and the user can access the secure website.

Pros	• Less expensive than implementing a hardware token solution for two-factor authentication • Easy to use because the user ID is filled in by the certificate and the user supplies only a password • Hard to hack because the user would have to modify the certificate without disturbing its validity
Cons	• If the user computer containing the certificate is stolen, only the user password is needed to complete two-factor authentication • Issuing certificates inside the organization requires modification to every user's Internet browser • Outsourcing issuance of certificates to a trusted third party can be expensive

CHALLENGE/RESPONSE CARDS (SMART CARDS) AND CRYPTOGRAPHIC CALCULATORS

How the technology works	Challenge/Response Cards and Cryptographic Calculators are cards sized like credit cards with an embedded Integrated Circuit Chip providing medium to high data storage capabilities. The card has a small gold plate on the front instead of a magnetic stripe on the back. The card can make decisions about the data stored and can perform cryptographic calculations. The Smart Card is inserted into a reader and the user generally establishes identity via a PIN or biometric. Electrical connectors transmit data to and from the microchip.
Pros	• More secure than magnetic stripe cards and supports laws to protect individual data privacy • Optimize portable solutions for information access • Have a large enough capacity to store broad profiles • Can have information easily added or deleted from the memory • Can perform decision making via the chips processing capabilities to enable such things as data encryption • Meet user demands for small and secure ways to carry data
Cons	• Cards are inexpensive, but the readers can be costly • Liability issues if lost or stolen • Difficulty assessing responsibility for lost data and transactions when activity occurs offline • Cards and card accepting devices have to be manufactured to identical specifications

PROXIMITY CARDS OR RADIO FREQUENCY IDENTIFICATION DEVICE (RFID) FOR AUTHENTICATION

The proximity devices described below represent a sub-category of *Something You Have* authentication factors sometimes referred to as *Somewhere You Are* devices.

How the technology works	Proximity Cards are contactless cards that have an embedded antenna and communicate by radio frequency signals without physical contact. The cards are powered by inductive coils and send a signal through capacitive plates. Controllers validate the cards and perform read/write functions. Information is then sent to the host computer which makes appropriate decisions. One prevalent form of these cards is the RSA SecurID. This key fob device continuously displays a numeric code (an encrypted form of the time), and each SecurID encrypts with a different key. An RSA SecurID card user responds to server challenges by typing the numeric code. The server knows what key is associated with each user's card, and can then authenticate a user. Wal-Mart is putting RFID tags on every product they shelve and both the German and U.S. governments are including them in passports. There are two types of RF proximity cards: passive and active. Passive cards are not powered, and use the RF energy from a requesting device to reply with information stored by the card. Active cards are powered and broadcast information, allowing a receiver in range to query the card.
Pros	• More secure than magnetic stripe cards and support laws to protect individual data privacy • Optimize portable solutions for information access • No contacts to deteriorate • No chance of an electric shock passing through the contacts and damaging the integrated circuit • Clear technical specification standards are established
Cons	• Liability issues if lost or stolen • Cannot be updated in real time • Less able to support multiple applications • Some proprietary standards are currently in use

Proximity cards have the following special characteristics:

a. Since these security factors are based on the location from which the individual is attempting to initiate access to health information, being in the location may validate the appropriateness of the context for the requested access to data. Example locations could be within the Emergency Department of a trusted hospital facility or a room housing the computer system used to access the health information database. In these

examples, a passive proximity card could be activated and authenticate a user when the user carrying the device approaches within a designated distance from the secure location.

b. Having the context in which data will be used can be very important in a healthcare application. For example, requests that originate from within an emergency facility may qualify for data overrides allowing otherwise restricted information to be made available. A disadvantage is that a proximity card is not inherently personal to the individual. Anyone in possession of the card would be allowed access to the location, and more than one individual may be present in the location at a time. Secondary checks, such as a user ID/password would need to be employed to link a specific individual to the access scenario.

c. The error rate for such devices is very low. The cards have no moving parts, and they generally do not malfunction. The readers similarly have few moving parts and are often used in less than ideal physical locations. Speed of authentication is measured in seconds with two or three seconds being typical.

d. Hardware for turnkey proximity systems tend to be sized for large enterprises with licensing for software scalable to the size of the individual facility. A hardware “vault” (a secure and redundant server with a paired secondary server) may typically cost around $19,000 and have the capacity to handle 25,000 users. A single card reader may be relatively inexpensive at under $200, while individual cards may be around $6 each. Licensing for the software may start at $20 to $30 per user with discounts starting at blocks of 500 users. It is realistic to consider that implementation of a turnkey system could be done in five days at a cost of $10,000. Support and maintenance of these systems require minimal staff time. Typical installations of 200,000 users can be supported by one half-time employee. A 400-user installation would only require a few hours a week of support time.

e. Use of proximity devices can be adversely affected by the presence of metal on or near the individual and their range of sensitivity is reduced by the presence of water. Since the body is largely water, placement of the card on the individual can reduce its effectiveness.

f. Implementation can be streamlined because self-enrollment can be done by the individual if a user ID/password is assigned with deployment of the card. Recovery from failure can also be managed by the individual when a user ID and password is used as a backup authentication method.

Something You Are

For security factor purposes, the category of *Something You Are* includes technologies that measure and identify biological characteristics (or biometrics) of an individual, such as her fingerprints, hand structure, facial features, iris patterns, etc. Additionally, biometric technologies often also include analyzing human behavioral characteristics, such as voice recognition and signature dynamics. All biometric technologies are very effective for identification, due to the distinct characteristics of each person. Additionally, since this type of technology is integral to something that a person is, the technology is more reliable, cannot be forgotten, and is less likely to be lost, stolen or otherwise compromised. The performance of a biometric device is usually measured in terms of its "false accept rate."

The following table compares characteristics of biometrics.[1]

- Universality indicates how common the biometric is found in each person;
- Uniqueness indicates how well the biometric separates one person from the other;
- Permanence indicates how well the biometric resists the effect of aging;
- Collectability measures how easy it is to acquire the biometric for processing;
- Performance indicates the achievable accuracy, speed and robustness of the biometrics;
- Acceptability indicates the degree of acceptance of the technology by the public in their daily life; and
- Circumvention indicates the level of difficulty to circumvent or fool the system into accepting an imposter.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L

[1] Yun, Y. W. (2003). *The '123' of Biometric Technology*. http://www.cp.su.ac.th/~rawitat/teaching/forensicit06/coursefiles/files/biometric.pdf.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

Ranking: H=High, M=Medium, L=Low

While details in the security technology table include hand geometry, retina/iris patterns, facial recognition, voice recognition, signature dynamics, palm scan, keystroke dynamics and fingerprint scan, most of these technologies would not be acceptable for regular use in the healthcare environment. The types of biometric technologies that are most likely to be used in healthcare include fingerprint scan, palm scan, signature dynamics or keystroke dynamics. Therefore, we will explore these biometric technologies in greater detail.

The information in the security technology tables below, unless otherwise noted, came from the Biometric Technology Application Manual.[2]

FINGERPRINT SCAN

How the technology works	Fingerprint verification systems identify locations of small lines or ridges found in the fingerprint. The system stores features from impressions created by the distinct ridges.
Pros	• Robust • Accuracy and reliability is good for most systems • Fingerprints are stable throughout an individual's lifetime • Systems are easy to use, typically requiring the user to touch a plate with his/her forefinger • Most systems are relatively inexpensive and easy to integrate
Cons	• Systems are not highly mobile. They generally need to reside in the location of a computer within the healthcare entity. Remote implementation requires installation of fingerprint plates on laptops, keyboards or mice and an Internet connection for verification. • User error can be high if individuals are not accurately trained in system usage or are not motivated to cooperate when placing their finger on the reader. • Condition variation, such as wet or moist fingers, cuts, dirt or grease on fingers may alter the authentication process. • Occupational impact (such as hands in constant contact with abrasive or chemicals) may interfere. This may be especially applicable to healthcare, depending on the environment.

[2] *Biometric Technology Application Manual Volume One: Biometric Basics.* (Summer 2008). www.nationalbiometric.org: National Biometric Security Project.

SIGNATURE DYNAMICS

How the technology works	Relies upon the manner in which a signature is written, using a stylus on a pressure sensitive tablet to track hand movements (specifically, the changes in pressure, position and velocity of the pen during the course of signing). A pressure-sensitive tablet or a PDA can be used.
Pros	• Very difficult to duplicate behavioral characteristics of signing a signature • Reasonably accurate in operation • High level of resistance to impostors • Considered non-invasive because people are very accustomed to signing their signature for transaction authorization
Cons	• Some systems have problems with individuals whose signature is different each time it is signed and with left-handed individuals. • Data acquisition difficulties exist: • Signatures can't be too long or short. • User must complete enrollment and verification in same conditions (i.e., sitting, standing, etc.) • Prone to an increase in the error rate over time. • Has not become a market leader like other biometric technologies. Most likely biggest market application will be in document verification and authorization.

PALM SCAN

How the technology works	Made up of principal lines, wrinkles and ridges, categorized into "geometry" features (width, length, area), line features (principal lines, course wrinkles, fine wrinkles) and point features (minutiae and delta points). Similar to fingerprints.
Pros	• Stable throughout one's lifetime, are unique and cannot be forged or transferred • Less likely to be worn away (unlike fingerprints) due to excessive wear or occupational abuse (note: there is no data to support this claim) • Could be combined with fingerprint technology or hand geometry systems as an additional layer of security or a back-up in case one of the other technologies doesn't read correctly
Cons	• Similar limitations to fingerprint technology • Excessive dirt, grime or oils on the skin can dirty the platen, causing possible false reads or non-reads of users. • Some users hesitant to touch something that many people have touched before them. • Failure to touch all or enough of their palm onto the imaging platen can cause false or inadequate reading.

KEYSTROKE DYNAMICS

How the technology works	Also referred to as typing rhythms. An automated method of analyzing the way a user types at a terminal or keyboard, examining dynamics such as speed, pressure, total time taken to type particular words, and the time elapsed between hitting certain keys. Two distinct variables: "dwell time"- amount of time a person holds down a particular key, and "flight time"- which is the amount of time it takes between keys.
Pros	• One of the easiest biometric technologies to implement and administer. Completely software-based, no new hardware needed. Utilizes the existing computer and keyboard. • Easily integrated with other, existing authentication processes. • Minimal training required, since most people are already used to typing in a user ID and password. • Static vs. continuous approaches. Static approaches provide more robust user verification than simple passwords, but do not provide continuous security. Continuous verification monitors the user's typing behavior throughout the course of the interaction. • The extent of statistical correlation needed to declare a match between the enrollment template and verification measures can be modified to accommodate the required security level. • Allows for a more robust authentication system than traditional password-based alternatives alone.
Cons	• Does not ease the burden of having to remember multiple passwords, nor does it decrease the administrative costs of having to reset passwords or enhance convenience to the individual using the system. • Cannot be used in one-to-many verification applications due to the limitations in the matching accuracy. • Has not been fully tested in wide-scale deployments.

DIGITAL SIGNATURES

While this document's primary purpose is to provide information on managing the identity credentials of those attempting to access health records for treatment purposes, it would be remiss if the concepts of digital signature for the authentication and non-repudiation of a signer were not included. Electronic documents containing digital signatures are becoming more prevalent in the healthcare industry, and requirements for using them continue to be proposed as part of many health privacy and security efforts.

When a medical record is digitally signed, a unique electronic "fingerprint" is added to the record. The "fingerprint" is unique to the combination of signer and document and binds them

together. When the same individual digitally signs a second record, the combination of the signer and the new document generate a different "fingerprint." Thus the primary use of digital signatures is to guarantee the integrity of a signed document and to link the signer to the document. It ensures the intent and accountability of the user with respect to the document and makes certain that it has not been changed since it was signed.

While the terms *"electronic signature"* and *"digital signature"* are sometimes used interchangeably, they serve different purposes. Electronic signature usually refers to a graphical or digitized image of a person's handwritten signature, a symbol, or even a voiceprint. Signature pads used to capture electronic signatures are low in cost and readily available. Electronic signatures are physically or logically incorporated in a document, and may even be added without the signer's knowledge as a standard for the organization. They are generally considered to be forgeable.

Digital signatures, conversely, are based on Public Key Infrastructure (PKI), an industry standard. They cannot be copied or altered, and are preferred for sealing and authenticating documents.

How the technology works	A user presents credentials to a Certificate Authority or a trusted third party and, if the credentials are certified, receives a pair of keys, one public and one private. The keys are used together to encrypt data using a process called hashing that converts the document into a unique "digest" representing the original document. The private key is kept solely by the user, and is used to validate incoming messages and sign outgoing messages. The public key is used to validate the private key owner's signature and the integrity of the signed document.
Pros	• Supports all signature properties - uniqueness, persistence, transportability, independent verifiability, integrity and non-repudiation • Becoming the preferred method for sealing and authenticating electronic documents • Standards for healthcare applications are already being published • The federal government has standardized its use of digital signatures
Cons	• Can be expensive and costly to administer • Not yet integrated into many vendor applications • Has many other implications for the organization with respect to interoperability, policies and procedures, complexity of upgrading applications and capabilities for handling digital documents

5. Evaluating Authentication Methods

In order to develop an appropriate authentication system, HIOs should evaluate a variety of authentication methods and choose a method or combination of methods that will make electronic health information both secure and usable. Comparison tools used include the following:

- Error Rate
- Cost
- Ease of Use
- Ease of Implementation
- Ease of Maintenance

Error Rate

Two types of error rates are associated with authentication methods. The first type is a False Acceptance Rate (FAR) specifying the likelihood that an imposter will access the system. FAR is related to the speed of the system, with systems that quickly verify identities generally having higher error rates. The second type of error rate is a False Reject Rate (FRR). FRR specifies the likelihood that a genuine user will be rejected by the system. FRR errors generate a very high level of frustration on the part of system users and can have serious consequences in the healthcare environment. The FRR and FAR are commonly plotted on graphs. The False Acceptance Rate (FAR) goes down as the sensitivity of the system increases, while the False Rejection Rate (FRR) increases as the system becomes more sensitive. The point at which the FRR and FAR are equal is call the Crossover Error Rate (CER). The CER is a standard assessment point used to compare the accuracy of different authentication methods. Figure 1 below illustrates the statistical concept of these error measurements.

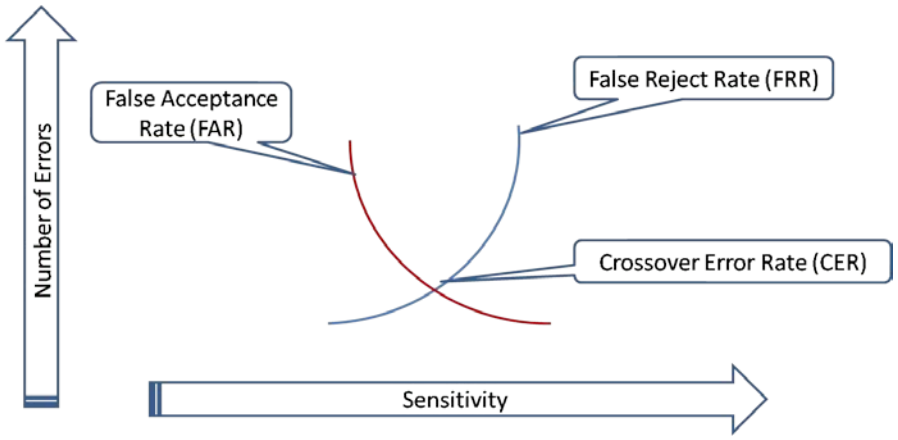


Figure 1

Cost

There are several costs associated with an authentication method, only one of which is the *initial purchase cost* of the hardware and software used for authentication. The *implementation cost* includes the work done to plan, test and integrate the authentication method into the health information exchange system. This cost can be particularly significant if legacy systems remain operational. All system users and support personal require training and there are *training costs* both initially as the system goes into operation and ongoing as personnel change and the system requires updating to maintain or increase its effectiveness. The *maintenance and replacement costs* associated with some authentication devices can be a significant part of the overall system cost, and there are ongoing costs associated with maintaining and upgrading authentication software. *Labor costs* vary widely. For example, the cost per user can rise quickly when users are widely dispersed and there are "hands on" support requirements.

An effective strategy for providing the labor required to support user access and maintain systems availability must be designed around the specific authentication method(s) to be used. In assessing the cost of an authentication method, it is important to use the most current information available, as the cost of more commonly used systems often decreases as their associated technologies mature and more tools to manage them become available.

Ease of Use

Three important characteristics relate to ease of use. They are the user's view of the system, the technical view of the system and the context in which the system is being used.

For health information applications, the primary system user considered is generally the healthcare provider. The provider needs to be authenticated quickly and easily. Since systems having quick and easy access also have higher error rates, the challenge is to find an authentication method that reduces errors but is still acceptable to the provider. Other system users may be able to tolerate a work flow that requires a more complex authentication system. For example, administrative users continually working with healthcare demographics would generally be more accepting of a multi-factor or multi-step authentication process. It is possible that having more than one authentication method in place would be desirable.

From a technical perspective, an organization must have the appropriate resources to support its authentication system. One of the most common and straightforward authentication processes requires users to provide a user ID and password to gain access to the system. Up to half of help desk calls, however, are related to password problems. An organization unable to provide immediate support for password-related problems will not pass an ease of use test. If the authentication system is device-dependent, evaluating both the user's acceptance of the device, and the technician's ability to keep it operational, are necessary.

Considering the context in which authentication takes place is critical. Systems requiring complex passwords are highly recommended. But entering a complex password on a mobile

device without a standard keyboard can be challenging for users, especially in time-critical situations. Allowing users to be logged on to more than one system device may make sense in an emergency department. But if the same user is permitted to log on at two separate remote locations simultaneously, there may be an authentication system failure, depending on the authentication policy. The authentication system and its context of use must be complementary.

Ease of Implementation

Technical, training and time requirements all contribute to the ranking of ease of implementation. Multi-factor authentication systems raise all three requirements significantly.

Technical and training efforts to implement authentication systems are interrelated. If technical support for implementation will be provided from within the organization, the technicians should be fully trained and involved at the outset of the project. If technical support for implementing the authentication system will come from outside the organization, then the training needs to focus on transferring the more limited skills necessary to internally support the system when it becomes operational. Availability of users for training is a challenge in the healthcare environment, and small, intensive training sessions may be required along with larger forums to prepare all users for the system

All authentication systems require both system administrators and users to follow well-defined security policies and procedures. New authentication systems invariably require new or upgraded security policies and procedures to be in place within the organization. These policies and procedures must be developed, and sufficient related training provided, in addition to any required hardware and/or software training.

Ease of Maintenance

Evaluating statistics around help desk requests can be very helpful when comparing systems with respect to ease of maintenance. Organizations using authentication systems similar to those being evaluated will often have service level agreements (SLAs) in place and manage service calls through an automated incident management system (e.g., issuance and tracking of trouble tickets). They can easily provide data indicating what kind of maintenance effort may be required.

Many authentication systems provide management tools that can effectively reduce the overall cost of maintenance. These tools can be expensive, but also often offer high returns on investment. When the management tool cost is compared to the related system administration labor savings, over the expected life of the authentication system, management tools are often easier to justify.

6. Organizational Factors

Organizational factors play a big role in selection of an authentication system. Authentication requirements must be viewed in the context of an organization’s unique business operations

and address the specific level of risk identified in those operations. The organization must then manage those risks with an effective audit program.

Risk

Risk analysis considers the probability of a negative event occurring and its impact on the organization. Risk management involves identifying risks, assessing them and taking steps to reduce them to an acceptable level. Organizations need to identify what areas of risk pose the greatest danger to their business. For any healthcare organization, failure to properly authenticate users accessing a system to obtain protected health information poses a significant risk. The degree of risk is related to such elements as the organization's size and general security environment, as well as the type of data available to system users. New healthcare regulations increasingly expect organizations to be fully accountable for securing their information and outline significant penalties for noncompliance. Enforcement of these penalties sharply increases the risks of tolerating lower standards for security-related actions, like authentication. In the healthcare field, a loss of trust can have even more important consequences and a serious security breach can jeopardize the business viability of the organization itself. Having a secure and appropriate user authentication process in place for all system users is one essential way to help build and maintain trust in the organization.

Audit

An effective audit process evaluates an organization's ability to manage risk, documents adherence to security policies and procedures, assesses the security environment and confirms adherence to regulatory requirements. With respect to an authentication system, an audit process is required to determine who accessed the system after the fact, and it must be sufficient to assure accountability. It requires that all users be authenticated before they are given any data, and that a record of the user's access is created for subsequent audit. The concept of non-repudiation is critical. Non-repudiation refers to the ability to provide proof of the integrity and origin of data that can be verified by any party. A secure authentication system allows an organization to prove who accessed the system (during the provision/creation of data), thus supplying one very critical piece of the information needed to establish non-repudiation.

7. Conclusion

The components of an organization's security policy are commonly referred to as the 4As – Authorization, Authentication, Access and Audit. This Overview of Basic Authentication Concepts Useful to Health Information Organizations introduces some basic concepts essential to authentication. Having a proper authentication system in place for a system user means that an organization can unambiguously verify who a user is before permitting access to protected health information. This capability is essential to building the trust needed to allow organizations to exchange health information, and furthers the goal of having complete and correct health information available when and where it is needed.

The information provided in this paper is a starting point for organizations forming or reviewing the systems they will use to authenticate their users. It should be considered along with the most current technical and standards information available, and the recommendations from a thorough risk assessment, to select a secure and appropriate authentication system for the organization.

Bibliography

Biometric Technology Application Manual Volume One: Biometric Basics. (Summer 2008). www.nationalbiometric.org: National Biometric Security Project.

William E. Burr, D. F. (April 2006). *NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline.* Gaithersburg, MD 20899-8930: National Institute of Standards and Technology.

Yun, Y. W. (2003). *The '123' of Biometric Technology.* http://www.cp.su.ac.th/~rawitat/teaching/forensicit06/coursefiles/files/biometric.pdf.

Contributors

Robert Grenart
Security Analyst
Arizona Health Care Cost Containment System

Michael McKay
Information System Coordinator
Wickenburg Community Hospital

Melissa Rutala
Associate Director
Arizona Health-e Connection

Kim Snyder
Project Director – Health Information Privacy and Security Collaboration (HISPC)
Government Information Technology Agency, State of Arizona
Principal, Illumine IT Solutions

Emilie Sundie, MSCIS
Project Manager – Health Information Privacy and Security Collaboration (HISPC)
Government Information Technology Agency, State of Arizona
Principal, The Sundie Group

Arizona Health Information Exchange (HIE)

Appendix D

Health Information Security and Privacy Collaboration (HISPC)

Guide to Adoption of Uniform Security Policy

March 2009

Table of Contents

Introduction

This Guide to Adoption of Uniform Security Policy ("Adoption Guide") was developed by the Adoption of Standard Policies Collaborative (ASPC), part of the Health Information Security and Privacy Collaboration (HISPC) initiative. Sponsored by the Office of the National Coordinator (ONC) for Health Information Technology, HISPC was formed to address privacy and security issues that may be barriers in sharing electronic health records.

One of the major challenges identified during the HISPC project was that organizations were hesitant to electronically exchange health information with each other because of mistrust due to the variation in their privacy and security policies. The Adoption of Standard Policies Collaborative was formed to develop an approach and process to identify and reconcile the variation in how organizational security policies are implemented across different electronic health information exchange models. [1]

This Adoption Guide outlines a process to define and harmonize minimum policy requirements specifically for authentication and audit and provides a framework to assist health information organizations (HIOs) as they seek consensus on privacy and security to support the exchange of electronic health information. The context for application of these policies is providers accessing patient health information for treatment purposes across HIOs.

Throughout this document the terms "minimum policy requirements" and a "Uniform Security Policy" have specific meanings, as follows:

- **Minimum policy requirements** are an agreed upon consensus set. They refer specifically to the policy requirements that the ASPC developed through extensive individual state review of current policy and the subsequent comparison and negotiation of these requirements across the 10 states in the collaborative. These minimum policy requirements become the framework across which the Uniform Security Policy was built. They are reflected in the Individual Requirements Review document, which can be found within the Final Report of the Adoption of Standards Policies Collaborative, located on the following website: www.okhca.org/aspc
- The **Uniform Security Policy** is an aggregated set of policies that the ASPC recommends organizations adopt as a minimum policy to allow for interoperability with other organizations for health information exchange.

This document is the culmination of a 12 month effort to develop consistent common and minimum policies for authentication and audit. The states that participated in the ASPC were Arizona, Colorado, Connecticut, Maryland, Nebraska, Ohio, Oklahoma, Utah, Virginia, and Washington. Each state, through their governor's office, had the approval of the state government to participate in the Collaborative. Additionally, many other policies and business practices that support exchange among organizations must be examined and because only 10 states and respective organizations within them were involved in this effort, further work remains to make the Uniform Security Policy applicable nationwide.

[1] Please refer to www.okhca.org/aspc for detailed information about the process and work products of the Adoption of Standards Policies Collaborative.

To define minimum policies for authentication and audit, the Adoption of Standard Policies Collaborative (ASPC) developed an approach and process to identity and reconcile variations in differing security policies among the collaborating states. At a high level, this approach included:

An environmental scan of existing best practice for authentication and audit policies and procedures, that included a:

- Review of literature and standards for authentication and audit concepts
- Design of a standard set of questions to determine existing policy within each collaborative state for authentication and audit
- Development of security policy templates for authentication and audit, use case documentation and analysis

A negotiation of requirements for authentication and audit and policy development that included:

- Comparison of each state's use case mapping, articulating similarities and arbitrating differences
- Development of the Uniform Security Policy
- Legal review of the Uniform Security Policy
- Stakeholder outreach
- Development of the Guide to Adoption of Uniform Security Policy

The Adoption of Standard Policies Collaborative (ASPC) planned to replicate this approach when they evaluated policy needs for authorization and access to protected health information.

The products the Adoption of Standard Policies Collaborative (ASPC) authored include the following publications: [2]

- *Uniform Security Policy* (USP) and
- *The Guide to Adoption of Uniform Security Policy*.

Lessons Learned

To responsibly articulate a model security policy for trusted multi-state health information exchange is a significant undertaking. The variability in architectures, methods of exchange, organizations, processes and other elements served to complicate the environmental scan. The elements of a security policy, authorization, authentication, access, and audit are not truly discreet in practice and have many interdependencies.

To facilitate the success of future efforts the scope of the project needs to be very clearly defined initially and methodology specified with concrete delineation of the work to be completed. Scope creep occurs without intention. For example, when the collaborative addressed system and data

[2] The *Uniform Security Policy* is included as Appendix B and contains the actual policies developed and vetted by the ASPC. The *Guide to Adoption of Uniform Security Policy* is available as a separate publication.

authentication, there were new requirements in the audit parameters. The minimum necessary to assure audit component compliance meant that timestamp needed to be communicated and stored in order to run a valid audit report. Another example was that consumer matching is critical to authentication and audit and was outside of the project scope.

Consensus-based decision making was limited by attempts to negotiate model neutral policy requirements. This was evident with the health record bank patient/consumer controlled model. Specifically, the Washington Health Record Bank (HRB) model for interoperability gives patients web based electronic access to their medical data from multiple sources and the patient controls access. The patient also supplies information to validate medications and advance directives. The patient-controlled HRB fosters patient activation and is designed to be shared electronically by the patient action. To design universal authentication and audit requirements that would fit this model and a provider to provider exchange lead to fewer agreed to elements in the Uniform Security Policy. Developing a typology of architectures and functionalities to overlay onto the security requirements would expedite future analysis.

Policies cannot be static if they are to address the changing landscape of health information exchange. Formulation of policies that conform to current standards also must address the need to evolve with changes across the industry. For audit, there were too many variations in the methods for identifying entities responsible. The specificity needed to identify what has been transmitted (data), to which entities (system) and what record (audit) is to be held in which location are all subject to industry practice and standards that are still evolving. The responsibility for tracking audit information is architecture dependent and rules about data transmission are subject to interpretation.

The following elements were critical to the collaborative's success and were essential to developing the policy requirements:

- A common glossary of terms and definitions
- A baseline of existing policies within each collaborative state that accurately represented the practices and procedures of the negotiating parties
- Identification of relevant standards and detailed documentation of their relationship to the HIO policies being developed

Concepts that were helpful in reaching consensus were:

- An understanding that current common practices and the current level of technological development may fall short of the ideal for effective, reasonably-priced and secure exchange of health information. Policies must be established to support the present reality and must be improved cyclically as health information exchange processes evolve.
- Acknowledgement of the necessity for a minimum policy that is acceptable to organizations whose size, available resources, and complexity vary widely. Organizations will vary in their determination of what policies they will adopt, and what minimum policies they require their exchange partners to have in place. The USP is offered as a best practice solution.
- Outreach throughout the process to stakeholders responsible for policy implementation

While the goal of the ASPC was to define standard policies to achieve interoperability in health information exchange (HIE) on multiple organizational levels including state-wide health information

organizations (HIOs), state and regional HIOs and HIOs in another state, this document will be pertinent to any exchange between any two entities. This adoption guide describes the process for working through and coordinating the efforts of several organizations as minimum requirements for authentication and audit are explored.

The Uniform Security Policy was developed to apply to any type of health information exchange architecture. Therefore, your organization's own experiences will be instrumental in building upon the ASPC's initial experience and shaping the process for adoption into one that meets the unique needs of your state or organization. This adoption guide, along with tools in the appendices, should serve as a helpful starting point as security policies are developed.

Overview

The Adoption Guide includes the following sections:

Introduction

The Adoption Process
This section details a 7-step process for Adopting the Uniform Security Policy. It includes information on gaining consensus from stakeholders and adapting the Uniform Security Policy to meet the unique needs of your specific organization as well as your state.

The following 7 steps are described in detail:

1. Goal and Scope
2. Resources
3. Desktop Review and Risk Analysis
4. Consensus Building
5. Legal Assessment
6. Documentation of Policy
7. Implementation: Testing, Training, Deployment and Production (including Evaluation and Maintenance)

Anticipated Challenges and Recommended Mitigation Strategies
This section provides an illustration of how health information organizations (HIOs) who participate in health information exchange will benefit from adopting the Uniform Security Policy. It also provides a chart of potential challenges that can be expected during the adoption process, along with recommended mitigation strategies.

Summary and Next Steps
Recommendations made by the ASP collaborative are summarized and next steps are indicated.

Appendices

- **Appendix A: Feasibility – Preparing for Change and Process Checklist**
  An organization interested in assessing the feasibility of adopting the Uniform Security Policy must first be prepared for the significant changes that will be required to adopt and implement these standards. This appendix includes both a framework for preparing for change and a checklist to assist organizations in tracking progress of their implementation of the Uniform Security Policy.
- **Appendix B: Uniform Security Policy**
- **Appendix C: Other Useful Resources**
- **Appendix D: Glossary**
- **Appendix E: References**
- **Appendix F: Contributors**

Audience

The Guide is appropriate for both of the following audiences: 1) organizations just beginning their HIE efforts and therefore are adopting new policies, and 2) organizations that have HIE policies in place who need to verify that their current policies, procedures, and practices meet the minimum requirements and possibly make some minor changes of what they already have in place.

This includes individual organizations (hospitals, health systems, healthcare providers,[3] and managed care organizations), HIOs, RHIOs, and state agencies (Medicaid, Health Departments).

Purpose

The purpose of the Guide to Adoption of Uniform Security Policy is to provide support and guidance to entities as they review and adopt the Uniform Security Policy. The guide can be used to:

- Provide a framework for establishing inter and intra-state authentication and audit policies through the use of minimum (core) policies that have been vetted by an inter-state collaborative effort.

- Demonstrate how alignment of local policies with broadly-accepted policies can facilitate health information exchange agreements.

[3]The Adoption of Standard Policies Collaborative (ASPC) chose and used the definition of "provider" as given in the HIPAA Regulation, 45 CFR 160.103 and the privacy rule, 45 CFR 164.501.

Figure 1: **Problem**: With one-to-one policy agreements, each of the entities must negotiate with each of the other parties. Here the ten states of the ASPC are illustrated. As the number of entities grows, the number of bilateral agreements grows almost exponentially; thus, for ten states, there would need to be 36 bilateral agreements. Were one to consider all of the U.S. states and territories, the number of bilateral agreements needed would exceed 1000, a daunting number of negotiations.

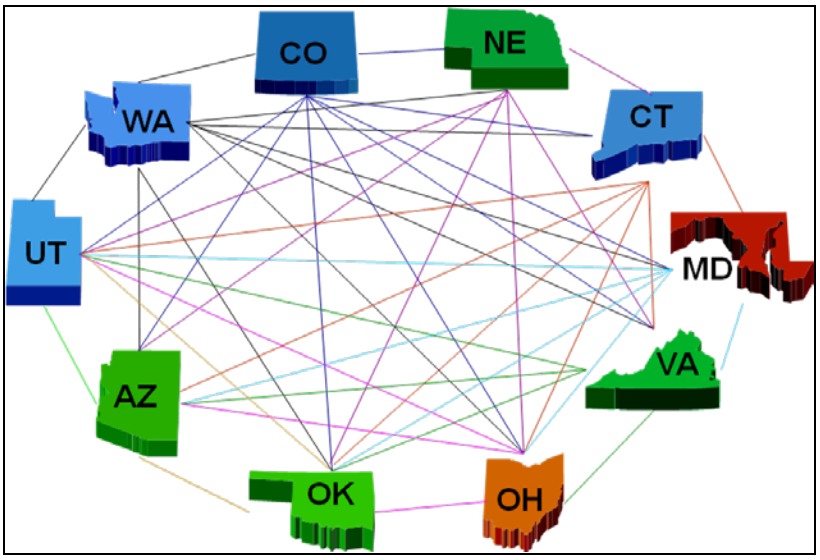
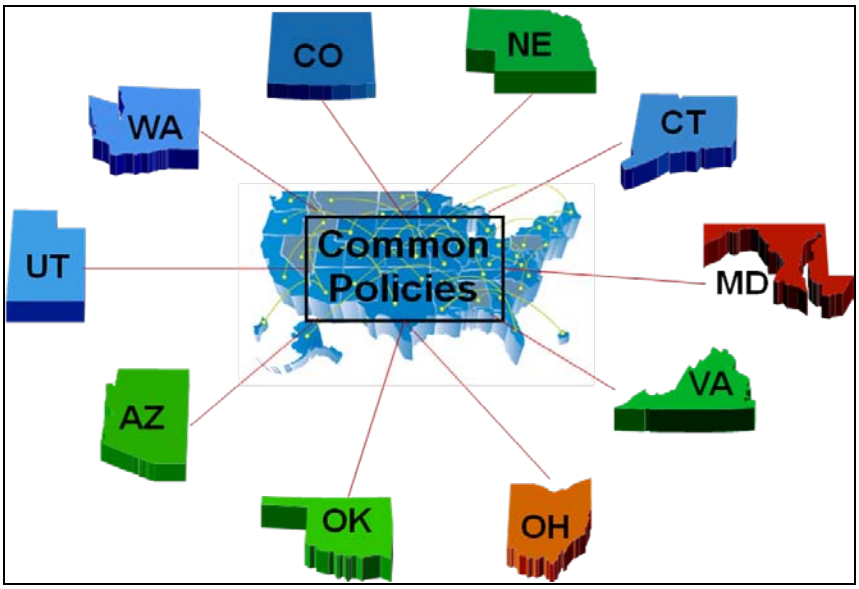


Figure 2: **Solution**: Adoption of the Uniform Security Policy offered in this Guide to Adoption of Uniform Security Policy will create common policies for HIE by all the participants. To illustrate this benefit, consider that for the ten states in the ASPC, the hard work of achieving consensus has provided the common policies.



Highlights of the Uniform Security Policy

In this Adoption Guide, a common policy, titled the "Uniform Security Policy" is recommended by the HISPC Adoption of Standard Policies Collaborative (ASPC). This policy, which currently includes requirements for Authentication and Audit, has been publicly vetted and accepted and can be used to establish baseline privacy and security protections for organizations engaged in exchanging electronic health information for treatment purposes.

Health information organizations (HIOs) participating in health information exchange (HIE) may have variations in security policies. Adoption of the Uniform Security Policy will help establish common business practices for registering and authenticating users, to benefit the individual users and the participating organizations. The guide will also help establish minimum audit requirements, consistent with the HIPAA Security Guidelines.

In order to successfully exchange health information electronically, HIOs must at least register; execute an agreement with; verify the identity of; provide digital identification for; and maintain an account for all users.

Each of these five processes has a set of minimal requirements that must be defined in order for HIOs to reliably trust their HIE trading partners and users and to be able to exchange health information with appropriate security rules in place.

The HIO must also consider the audit requirements for the HIE following the HIPAA Security Guidelines; The Uniform Security Policy provides minimum requirements for audit which include:

1. logging and audit controls
2. periodic internal compliance audit
3. information access
4. need to know / establish minimum necessary for data management and release
5. need to know procedure / establish process for personnel access to personal health information, and
6. system capabilities

NOTE:

- While the ultimate scope of a comprehensive security policy should include services that support operations and payment as well as treatment, the scope of the current Uniform Security Policy is specific to electronic authentication and audit policies and process when a healthcare provider requests patient health information through an HIO **for the purpose of treatment**.

- The ASPC did not address the policies needed to govern provider authorization or access to specific types of health information permitted after the authentication process is complete. The project did develop the corresponding policies required to audit provider authentication as defined in the project. Since the audit policies considered both the authentication action and subsequent access to the records requested, the scope of the audit policies became broader.

- These policies do not necessarily pertain to the secondary use of data such as the exchange of data for the purposes of public health improvement or the detection and control of outbreaks; however, the process that the ASPC used to work toward common policies across the ten states of the collaborative is likely to be generic enough to use as these other areas of data exchange are explored.

- The policy is determined as a minimum to be built upon. It can be more stringent depending on an organization's individual need and state-specific requirements.

- Also, throughout this document the term "state" is generic and includes any of the states, the District of Columbia, and/or territories of the United States.

The following table lists some key authentication and audit features of the Uniform Security Policy regarding use agreement, identity management, audit log data elements, audit reports and enforcement.

Table 1: **Key Authentication and Audit Features of the Uniform Security Policy**

<table>
<tr><th colspan="3">Authentication</th></tr>
<tr><td colspan="2">Use Agreement
• Information is true, complete & accurate
• Agree to comply with Federal and State laws
• Act in good faith & be truthful at all times
• Access and use information only as permitted
• Confidentiality, integrity and accessibility will be reasonably ensured</td><td>Identity Management
• Unique identifier
• Affiliation
• Role</td></tr>
<tr><th colspan="3">Audit</th></tr>
<tr><td>Audit log data elements
• Unique Universal ID of viewer
• Role
• Data elements viewed, created, modified, deleted or transmitted
• Date and time/duration of access</td><td>Audit reports
• Routine scheduled reports
• Routine surveillance
• Ad hoc reporting by request or on suspicion of inappropriate access</td><td>Enforcement
• Common policy on enforcement necessary for public trust of HIE, regulatory compliance and limiting legal risk.</td></tr>
</table>

Benefits of the Uniform Security Policy include:

- **Commonality *Across* States** (because the Policy defines what is required in terms of the data set)
    - From a regulatory standpoint, it is important to adopt a policy set that supports systematic processes needed for ever-expanding HIE.
- **Commonality *Within* States**
    - Inter-state exchanges can model their policies based on nationwide adopted standards.
- **Starting Point for New HIOs**

- A starting framework for policy development would help any HIO as a floor for standardizing and develop consistent expectations prior to exchanging protected health information among organizations.

An outline of the Policy, including the focus of each section and sub-category covered, is listed in the tables that follow. The full Uniform Security Policy can be found in the appendix.

Table 2: **Minimum Policy Requirement categories for Uniform Security Policy: Authentication**

Authentication
Section 1: Use Agreement
1.1 Requirement – Use Agreement
Section 2: Identity Registration
2.1 Required Data Set for Authentication
2.1.1 Data Source
2.1.2 Provider Identity Attributes
2.1.3 Organization Identity Attributes
2.1.4 Identity Attributes of the Data Source System
2.2 Role-based Access
2.2.1 Role
Section 3: Verifying Identity
3.1 Processes Used to Verify Identity
3.1.1 User Authentication
3.1.2 Organization Authentication
3.1.3 System Authentication
3.2 Variations Based on Type and Location of User
3.2.1 User Identity, Role, and Affiliation Verification
3.2.2 Signature Verification
3.2.3 Assurance Level
3.2.4 Relationship to Patient
3.2.5 Threshold Calculation
3.2.6 Digital Signature
3.2.7 Persistence
3.3 Accommodations for Cross-HIE Verification and Data Integrity
3.3.1 Restricted Data Sharing and Data Integrity
3.3.2 Authenticate Recipient Identity (Organization / System / User)
3.3.3 Required Elements for Matching
3.3.4 Matching Criteria
3.3.5 Digital Signature
3.3.6 Persistence
3.3.7 Data Authentication
3.3.8 Data Validation
3.3.9 Type of Requestor
3.3.10 Signature Purpose
Section 4: Identity Provisioning
4.1 Types and Levels of Provisioning
Section 5: Identity Maintenance
5.1 Registration Data

Table 3: **Minimum Policy Requirement categories for Uniform Security Policy: Audit**

Audit

Section 1 – Logging and Audit Controls

- **1.1 Log-in Monitoring**
- **1.2 Information Systems Review**
- **1.3 System Review**
- **1.4 Security Audit Practices**
- **1.5 Audit Trail and Node Authentication (ATNA)**

Section 2 – Periodic Internal Compliance Audits

- **2.1 Evaluation**

Section 3 – Information Access

- **3.1 Audit Controls**
- **3.2 Subject of Care Identity**
- **3.3 Demographics that May Be Logged**

Section 4 – Need to Know/ Minimum Necessary for Data Management and Release

- **4.1 Information Disclosure**
- **4.2 Auditing Access Where Individual Consent or Authorization is Required**

Section 5 – Need to know Procedure/ Process for Personnel Access to Personal Health Information (PHI)

- **5.1 Information Request**
- **5.2 Audit Log Process**
- **5.3 Data Authentication**
- **5.4 Preparing a Query Message**

Section 6 – System Capabilities

- **6.1 Audit Controls**
- **6.2 Audit Log Content**
- **6.3 Information Integrity**
- **6.4 Data Authentication**
- **6.5 Data Validation**

The Adoption Process

To facilitate the adoption of minimum policy requirements for authentication and audit the following major steps and questions described in Table 4 should be addressed. The remainder of the Adoption Process section of the Guide will walk through each of these seven steps in detail.

Table 4: **Checklist – 7 Critical Steps to Adoption**

Step		☑	Questions Guiding the Interstate Process
It is recommended you consult this checklist as needed throughout the adoption process.			
1	**Goal and Scope**		• What are the goals for this process? • What is the scope of the project; which use case will be used; what is the business model?
2	**Resources**		• What team resources are required for this project? • Who are the stakeholders and what impact will adopting these policies have on them?
3	**Desktop Review and Risk Analysis**		• Do you already have authentication and audit policies in place? • What business process are you trying to resolve? • How will you measure the risk associated with the business process?
4	**Consensus Building**		• How will you build consensus among the team and stakeholders? • What specific methods will you use to achieve consensus? • How will barriers to consensus be addressed as you proceed?
5	**Legal Assessment**		• How will you assure legal requirements, including HIPAA guidelines are incorporated into your policy? • Does your state have any laws that would dictate or affect the proposed policy requirements? • Do you need to work toward changing existing laws or introducing new legislation?
6	**Documentation of Policy**		• How will you document the policy for end users? • How will you ensure that all policies are semantically accurate for digital translation prior to technical team implementation?
7	**Implementation** **a. Testing** **b. Training** **c. Deployment** **d. Production**		• How will you test that the software performs as expected, and only as expected? • How will you test the minimum policy requirements? • How will you resolve issues that result from testing? • How will users of the policy be trained? • How will you deploy the agreed-on minimum policy requirements? • How will the implementation efforts be evaluated? • What are the outcomes to be measured? • How will you maintain the policy and assure that it is not only adopted but also adhered to?

NOTE: Although these steps appear chronologically and as stand-alone, some steps may be performed simultaneously. For instance, while defining your goals and scope, you may find that your team needs to have the appropriate resources in place to help with the goal definition process.

1. Goal and Scope Definition

The first step in the adoption of Uniform Security Policy is to establish a clear and realistic set of goals and to define the scope of the initiative.

Goals

Goals describe the end product that the HIO is trying to achieve. For purposes of adopting the Uniform Security Policy the goal would be to implement the minimum policy requirements needed to support HIE between two or more states. If the organization is also going to adopt the Uniform Security Policy for use within the state, the goal should encompass that as well. The goal should be agreed-on by all participating parties and should be distributed as a written document to which the team may refer at each meeting throughout the process. A clearly stated, common goal helps define the project scope (described below). As an organization develops the goal statement, consider the different models and sizes of participating HIOs, as this will impact the means by which organizations can adopt these policy requirements. For instance, it may be unreasonable to expect a very small rural HIO to implement 2-factor or biometric authentication measures that a larger, urban and more-sustainable hospital has already implemented.

Scope

The project scope defines a common understanding of what is included in the project and what is outside the project. For instance, the idea of defining requirements for authentication and audit can encompass many different areas ranging from consumer authentication to auditing of system behavior. It is important to define the scope for adopting the minimum policy requirements for authentication and audit (and by extension, the Uniform Security Policy). Further, it is recommended that the scope include the context. For example, if a HIO decides the project will address provider access to the HIO for treatment purposes only, public health improvement or detection would be outside the project scope. The scope should clearly document the intent of the project as well as how the project will impact the key stakeholders. A well-defined scope increases the likelihood of attaining the goal and will help drive the business process analysis.

In identifying the scope of the project, there may be areas (such as authorization, access, and patient consent issues) which need to be included at a high level in order to complete some of the audit policy requirements. For example, when addressing the audit requirement of knowing which provider accessed which patient's record, it would be necessary to understand how the patient was identified.

A strong scope statement for adoption of the Uniform Security Policy could be: "Analyze and define the authentication and audit requirements for a hybrid model HIO to use when allowing providers to access the HIE for treatment purposes, based on a medication management use case. " A very specific scope will help keep the project focused.

Role of Use Cases[4]

It is sometimes difficult to conceptualize what is involved in a process; therefore, it is recommended that "use cases" are included as the project scope is defined. These use cases are workflows that a

[4] The ASPC found the AHIC use cases a starting point for our discussion, Although the AHIC were found to contain far too much detail for our purposes, the ASPC used the AHIC use cases to develop templates to capture the actors, actions, events and policy requirements pertinent to authentication and audit for each use case; and extracted the corresponding policy information from the AHIC use cases into the template. See the ASPC Final Summary Report at www.okhca.org/aspc.

specific system user would perform in order to obtain information. For instance, a HIO may exchange laboratory data. The use case would document a description of an event and the actor who might need to be a part of the event. See, for example: ***Sample 1: "Use Case / Business Requirements Analysis for HIOs Without a Current Security Policy,"*** which outlines the method for defining a use case as well as how to proceed in mapping the use case to the minimum policy. Selection of use cases helps center discussion around which components of authentication and audit are essential to include as policy. The use case should apply to the planned organizational goal and should be pertinent to all the business models present in the HIOs involved. Spending an appropriate amount of time on each use case and organizational goals will be critical to facilitating the conversation between the business and technical teams within the organization.

Role of the Architecture of Business Models

The HIE business model includes the enterprise architecture in use, or planned for use in HIE, and is pivotal in determining the project scope. It is necessary to have a documented, detailed HIO enterprise architecture in order to determine the points in the system where authentication and audit are required. In the case of individual organizations, the same is true – it is necessary to document the detailed HIE structure that exists within an organization and between organizations. The architecture model may be one or a combination of several types of models, including but not limited to: (1) centralized, (2) federated, (3) health record banking, and (4) hybrid models.

The model is used in conjunction with a use case to determine what policies should be required for authentication and audit. In order to reach consensus on minimum policy requirements, a state or organization with several HIE business models, must be certain that all models are accommodated. Many states will want to work with other states to define minimum policy requirements and in that case, each state should be prepared to document its business model or models in order to perform use case mapping that then becomes the basic policy requirements.

2. Resource Planning

Team Resources

In addition to time and material resources, human energy and activity are required to perform the business process/use case mapping and analysis to determine the recommendations for adopting the Uniform Security Policy. Recommended resources for adoption include a project manager, business analyst, security analyst, technical support, legal counsel and episodic availability of stakeholders. This team would be responsible for bringing the project to a successful conclusion, as well as ensuring consensus among stakeholders. It is important to invest in having the correct resources and to continually evaluate these resources as the project matures, to ensure that they are available and devoted to support the adoption of the Uniform Security Policy.

Stakeholders

How to Involve Stakeholders

Stakeholders might be asked to participate in a working group and meet on a monthly basis to help review and evaluate the Uniform Security Policy. Assignments for this group would include use case mapping, documentation of standards, and detailed review of the minimum policy requirements for authentication and audit. The recommended approach is to provide the stakeholders with the goals and scope as well as the detailed scheduled, outlining when input will be expected and what type of input will be needed from them. Since the stakeholders will have a vested interest in how these policies work, it is important to include them in major decisions around the adoption of the minimum policy requirements. A Steering Committee or other review body will take the work completed by the working group and approve the policy implementation. A steering committee would be comprised of high level stakeholders, such as those from leadership and managerial ranks from the medical community mentioned above. This group could meet monthly or quarterly to review the progress and results from the efforts in adopting minimum policy requirements for authentication and audit. Having "buy-in" from this group is important to success overall, as they, too, can become advocates for the results.

Organizations from which community stakeholders may be drawn include:

- Hospitals and hospital associations
- Medical groups
- Schools of Medicine/Osteopathy/Nursing/Pharmacy
- Medical association chapters (for example, of the American Medical Association)
- Behavioral health organizations
- State and/or local healthcare and public health departments and agencies
- Community health center representatives
- Quality improvement organizations
- Health/managed care plans
- Forming or existing HIOs
- Local sections of the Healthcare Information and Management Information System Society (HIMSS)
- Advocacy groups (for example, the American Association of Retired Persons)
- Law offices specializing in health law
- Consumers
- Employers

Participation of various stakeholders in analyzing and reviewing the authentication and audit minimum policy requirements is critical to the success of the adoption process. Not only should stakeholders be involved in setting new policy but they should be involved in adopting an existing policy. This will ensure broad consensus as you move forward. Representation from the community and a diversity of disciplines is recommended to achieve consensus.

3. Desktop Review of Business Processes and Risk Assessment

Desktop review of business processes

In order to determine if the Uniform Security Policy is going to be adopted by your organization, it is first necessary to perform a desktop review of the business process the authentication and audit will apply to. Each component of the Uniform Security Policy needs to be reviewed against each actor and event applicable to the business process.

Step one in the business analysis process is to use the selected use case to define the actors, the information they would need to access, and the authentication and audit requirements. If specific policy requirements are not in place, the use case can help define what policies would be needed for a specific use case and business model. If there are existing policy requirements in place, these can be used as a comparison tool to determine if the Uniform Security Policy can be adopted. If policies for authentication and audit do not exist, it is necessary to analyze the business requirements for providers accessing the HIO for treatment purposes. The first step in this analysis is to determine who the actor is that will be processing transactions through the HIO for the use case selected. It may be necessary to reiterate that the basic minimum policy requirements are only for providers accessing the HIO for treatment purposes. This method of analysis can be used to determine the business process requirement for each person accessing the HIO and the patient information that person would need to access. The business requirement is compared to the authentication and audit requirement to validate that this is a point at which the actor would need to be authentication and subsequently, audited.

The sample below illustrates how this process would work, citing a portion of the applicable security policy element. Some Uniform Security Policy statements may require more than one test scenario. For example, in Appendix B, Section 3, element 3.1.1 addresses the registration of the provider and the authentication method. It is necessary to test each of these elements individually.

Sample 1: **Use Case / Business Requirements Analysis for HIOs without a Current Security Policy** [5]

Actor	Event	Authentication / Audit Requirement	ASPC Recommended Basic Policy Requirement	Issues	Resolution
Clinician	Laboratory results for a patient	Clinician is identified by the trusted authority Clinician logs into system using password and login name	**Authentication Section 3 – Verifying Identity** 3.1.1 User Authentication HIO use of a specific naming convention as a primary identifier is required with a minimum assurance level used of Medium (knowledge/strong password/shared secret).	Current system only allows for password	Upgrade system security to allow for shared secret
HIO	List and review of people accessing the HIO	HIO must be able to audit access to the HIO by providers	**Audit Section 1 – Logging and audit controls** 1.1 Log-in Monitoring Audit log is required and must be reviewed on a regular basis.	No issue	NA

Once the business process analysis is completed, issues should be discussed with the team and the stakeholders. For instance, if a "shared secret" is the business requirement, any HIO participant system that does not provide for a "shared secret" as part of the authentication process will need to determine how to provide this functionality, for those who want to exchange with other HIO participants.

The next step in the business process analysis is to map the future requirements for authentication and audit to the business model defined in the project scope, using the selected use case(s). This can be accomplished by constructing a flow chart of the relevant HIO architecture and identifying points at which authenticating a user or system, or auditing access to the HIO should be conducted, based on the use case. The mapping of the use case to the system architecture will confirm that all the authentication and audit requirements for secure transmission of medical data have been identified.

If there is already a security policy in place, a desktop review of business requirements analyses can be performed by comparing policy requirements within the Uniform Security Policy to the organizations existing security policies. Existing security policies might be entity-specific, i.e. your hospital's policies, HIO policies, policies associated with a particular business model or state agency, policies that pertain to a particular application like an immunization registry. The purpose of the desktop review when existing policy is in place is to check for gaps and propose recommendations in order to adopt the Uniform Security Policy. The desktop review can be completed by using the following format to track and compare your local policy requirements to the minimum policy requirements in the Uniform Security Policy.

[5] The authentication / audit requirement in the sample contains one element of that requirement. Refer to the full Uniform Security Policy in Appendix B for all elements.

Sample 2: **Format for Business Process Analysis for Organizations having a Security Policy[6]**

Uniform Security Policy Requirements	Local Policy	Gaps	Recommendation	Solutions
Authentication Section 1- Use Agreement 1.1 Use Agreement Health Information Organizations should have a data sharing agreement with participating providers that defines the privacy and security obligations of the parties participating in the HIO. These agreements should require the use of appropriate authentication methods for users of the HIO that depend on the users' method of connection and the sensitivity of the data that will be exchanged.	Local one-to-one contracts	Stricter than minimum	Accept a less strict policy for cross-state sharing only	Allow for cross-state sharing of HIE
Authentication Section 2- Identity Registration 2.1 Required Data set for Authentication A directory of data sources within the target HIO is required, and includes primary contact information of registered members, identity attributes of providers, organization and systems.	Same	None	Accept minimum policy requirements	
Authentication Section 2- Identity Registration 2.1.1. Data Source A directory of data sources within the target HIO is required and includes name of the HIO and any data sources within that HIO.	None	Currently no such data source	Need new system capability	Install and deploy X
Authentication Section 2- Identity Registration 2.1.2 Provider Identity Attributes The HIO will collect the attributes as needed for unique identification of the individual accessing the information in the HIO. Required elements are profession, role, name, practice address, business/ legal address and License/ID.	Required but no field in the system for role	Roles not codified and assigned	Add field for role	Update application

[6] The authentication / audit requirement in the sample contains one element of that requirement. Refer to the full Uniform Security Policy in Appendix B for all elements.

Once the desktop review is completed and gaps and/or issues have been identified in the authentication and audit process, a risk analysis should be completed. It is also possible to begin the risk analysis during the desktop review process.

Risk Analysis

A risk analysis should be preformed when adopting the Uniform Security Policy. This assessment will be critical in determining what threats and vulnerabilities may impact the users and systems and what security controls have been implemented to protect against identified threats and vulnerabilities. The risk analysis can be performed at the inception of this process as the desktop review is being completed. A risk analysis should also be completed whenever a significant business or technical change occurs following implementation. This assessment involves reviewing the data, hardware, people and networks, prioritizing those items and determining what threats and vulnerabilities exist, what security controls are already established and where action may be necessary to prevent regulatory, liability, financial and reputation issues. Further the risk assessment will help define the type of audit reports you need to have as well as the type of monitoring requirements you need in place. The risk assessment should be done in relationship to the Uniform Security Policy.

The following steps should be followed when conducting a risk assessment of an HIO:

- Definition of System Boundaries
- System inventory (hardware, software, facilities and data)
- Identification of information owners (electronic and non-electronic data)
- Identification of workforce members with access to stored data by hardware/software
- Mapping data flow and identifying data exchange points (for example, where data is transmitted from one system to another, from the system to an individual or entity, etc.)
- Conducting an inventory of data storage (including non-electronic data)
- Assessment of criticality (for example, mission critical, important, ancillary, etc.)
- Vulnerability identification
- Threat identification
- Security control analysis using the Uniform Security Policy
- Likelihood determination (for example, how likely will an identified threat or vulnerability impact the organization given existing security controls)
- Impact analysis (for example, what is the cost if an identified threat or vulnerability impacts the organization given existing security controls)
- Risk determination (based on likelihood and impact)
- Security control changes/mitigation recommendations
- Results Documentation (includes mitigation plan and documentation of risks that will be accepted by the organization such as threats or vulnerabilities that will likely impact the organization and with a low impact cost)

Please refer to the **National Institute of Standards Technology (NIST) 800 series** of publications on this topic in order to complete a risk assessment (http://www.nist.gov/index.html).

4. Consensus Building

After each HIO within a state or across state lines has mapped the recommended basic policy requirements to the individual models, negotiations with the project team and stakeholders may be necessary to reach consensus about the adoption process. Conflicts may be inevitable but can also be productive in the negotiation process. In a negotiation process, it is important to have a neutral facilitator who will manage all meetings during the negotiation process (e.g., setting meeting schedules, keeping minutes and tracking both policies agreed upon and areas that require further negotiation). The facilitator should have the knowledge and skills to articulate differences in the types of authentication and audit, be an experienced facilitator and bring the group to consensus about which will work as a basic minimum policy requirement. It will be important to emphasize the positive elements of adopting this policy, for example, the value of having a Uniform Security Policy in place will enhance an organization's ability to exchange electronic health records. The legal considerations should be highlighted and discussed as well so there is an understanding of legal compliance. It will also be important for each stakeholder to understand the impact of the policy on other stakeholders. For instance, a provider will have a different view of what should be audited than a consumer.

The following should be taken into consideration at the consensus building phase:

- Documented desktop review of business processes for each HIO represented should be available
- Appropriate personnel including the business analyst, security analyst and technical support
- A decision maker who has the authority to make decisions about the policy in case of negotiation should be included in any negotiations
- Issues will need to be tracked as "parking lot issues" and resolved before the policy analysis is complete
- It may be necessary to involve the legal counsel as negotiations progress in order to be sure any state or federal legal requirements are taken into consideration

The following are some techniques commonly employed by organizations to achieve consensus and improve group decision-making. A brief definition is included below to describe each technique and each will involve several steps that reference how to successfully execute the method.

- **Delphi technique:** This technique collects and uses opinions of individuals with certain expertise by mail. Responses are ranked, compiled, and computed. The consensus is used to make a decision. This would involve listing the items from the policy that you are unable to reach consensus on, providing the detail around those items and collecting responses for ranking.
- **Nominal group process:** This technique involves small groups of individuals who systematically present and discuss their ideas before privately voting on their preferred solution. The most preferred solution is accepted as the group's decision.
- **Stepladder technique**: This technique may be used to minimize the tendency for group members unwilling to present their ideas by adding new members to a group one at a time and requiring each to present ideas independently to a group that already has discussed the problem at hand.[7]

[7]Greenberg, J. and Baron, R. 2007. **Behavior in organizations**. Upper Saddle River, NJ: Prentice Hall.

5. Assessment of Legal Requirements

Integral to the adoption of standard policies is a complete legal review of HIPAA, other federal laws (such as CLIA regulations and federal substance abuse treatment regulations) and of relevant state statutes and regulations. Given the complexity of legal requirements that affect security policies for HIE, it is important to include legal expertise during the process of adopting these minimum policy requirements for authentication and audit. Although HIPAA and other federal regulations were taken into consideration in drafting the Uniform Security Policy, adopting states should review their own states laws that may impact the adoption process (and should keep abreast of federal laws issued after the date the policy was issued, as well).

The legal review should be completed once the use case has been mapped to the model architecture, because legal requirements for authentication and audit may change with different HIE architecture and use cases (who will have access to the information and for what purpose). In addition to considering federal and state laws that apply in the adopting state, the legal review should also encompass ways to minimize legal risk in the policy. Many states tie these requirements to HIE participation agreements as well, in order to require HIE participants to comply with the applicable policies.

Once the legal review is completed, the team should give serious consideration to any legal issues that may hinder the adoption of the minimum policy requirements. At this point, it may be necessary to return to the desktop review phase and reconsider some of your recommendations. Or, you may need to go back to the consensus building process and get buy-in on the changes required as a result of the legal review. Alternatively, it is possible to go back to the State Legislature and get statutes changed or work with the appropriate state agency for rule/regulation amendment.

If your state is considering interstate exchange with other states, consider conducting the legal review with representatives from the other states to facilitate identification of different state laws (or different interpretations of federal laws) that may pose barriers to exchange.

6. Documentation of Policy

After the legal review and final negotiation of policy is complete, the policy should be documented not only for the end users but for the technical team. The Uniform Security Policy should be documented as it applies to the organization. Please refer to Appendix ___ for a standard format for documentation of the policy. It is important to ensure that the written policies agreed upon can be understood by the users and the technical team.

At this point it will also be necessary to document the configuration of existing applications. This will ensure that the written policies can be executed with your applications. This means that special care must be expended in drafting the specifications that are passed to the technical team that will be configuring appropriate applications, customizing those applications, or developing the needed applications. Because of the sensitivity to unauthorized disclosure of protected health information (PHI) and the compliance rules with which the HIO must be cognizant, this is an important step in the process. The technical team will need specific instructions in order to implement solutions that do not permit illicit activity. By careful drafting of the application specifications, this type of activity can be avoided. The implemented applications will do what is expected, but no more. An example of this type of specification follows:

Sample 3: **Technical Specification of a Policy Statement**[8]

Policy Statement	**Technical Specification**	**Date Completed**	**Issues Reported**
Authentication Section 2 -Identity Registration 2.1.2 Provider Identity The HIO will collect the attributes as needed for unique identification of the individual accessing the information in the HIO. Required elements are profession, role, name, practice address, business/ legal address and License/ID.	Coding must include a role.	Ex. 2-27-10	Custom code required to add field for role.
Audit Section 6 – System Capabilities **6.4 Data Authentication** For purposes of data authentication the use of a valid date/time stamp is required.	Coding of the system and the audit reports must include the valid data / time stamp required. Data stamp needs to print on the audit report.	Ex. 3-5-09	Audit report doesn't include time of access.

[8] The authentication / audit requirement in the sample contains one element of that requirement. Refer to the full Uniform Security Policy in Appendix B for all elements.

7. Implementation

The implementation phase of the adoption process includes:

- **Testing** – functional, regression, system, integration and load testing
- **Training** – training the end users and the support team
- **Deployment** – deploying the new policy to the end users and the systems
- **Production** – post implementation review, modification and support

Testing

The testing phase is critical to the successful adoption of the Uniform Security Policy. Testing of the new policy against the applications is completed so that the users can determine if the new policy is going to satisfy requirements for using the system from a security viewpoint. It is important that testing validate that the system is responding as expected to the new policy; however, it is more important the users can abide by the new policy and that the user's work load is not increased.

Preparing to Test
The purpose of testing is to determine if the Uniform Security Policy and technical requirements of the policy will operate as planned within a given organization's technical environment. It is critical that test scripts are developed to reflect the use case and workflow as well as the authentication and audit points that are required based on the basic minimum policy requirements and the work completed in the desktop review of business processes. Having formal test scripts will help track areas where gaps may be present or identify any type of system malfunction that occurs while testing the policy.

As you are preparing for the testing phase, it is important to develop test scripts that reflect the workflow expected with the Uniform Security Policy. They can be used for each testing phase and should reflect the actual workflow that the HIO performs. The test scripts can be developed by determining the action a user or (actor) would perform based on the policy element from the Uniform Security Policy. Each element in the policy needs to be tested. Below is an example of how a test script should be designed. This example reflects adding a provider to the system and authenticating the provider.

Sample 4: **Test Script Sample – HIO entering Provider Data** [9]

Script Number	Test Script Name / Policy Reference	Action	Actor	Expected Results	Issues
1	Identity Registration: ref. 2.1.2 Provider Identity Attributes	Add a new provider to the system, using the required attributes: profession, role, name, practice address, business/ legal address and License/ID	HIO	Successful addition of provider to the system, issuance of login and password	None
2	Verifying Identity: 3.1.1 User Authentication	Provider is accessing lab results using login and password	HIO	Provider uses assigned login and password to access the system	Provider Unable to login in. Fix and retest

It is critical to also have a list of standard data that the testers will use in their testing. (This list will likely grow over time as more use cases are added). A sheet of allowable attributes for testing can be developed to be referred to depending on the script. It is required to have data for each test script. Using predetermined data for entry gives the users and the technical team the ability to track that data through the system, validating that the data went into the right fields and shows up on the audit reports. It can also help when debugging the system. The figure below is an example of predetermined data.

Sample 5: **List of Provider Data for Testing for Script #1 and #2**

Profession	**Name**	**Role**	**Address**	**Business Address**	**License #**	**Test Login**	**Test Password**
MD	Dr. J.	Provider	6 Oak Street	6 Oak Street	123456	Drj	Drjej!23J34*
PA	Tim Jones	Physician Assistant	8 Tree Street	8 Tree Street	123454	Timj	DF$c56J23#

The database and applications must be configured to reflect the Uniform Security Policy prior to testing. The application specifications provided in the Documentation of Policies section provides the basis for the technical work. This can be done using configuration methods but in some cases may require custom coding. The process involves converting the policies into digital rules on a test database that should be a replicate of existing HIE database and applications.

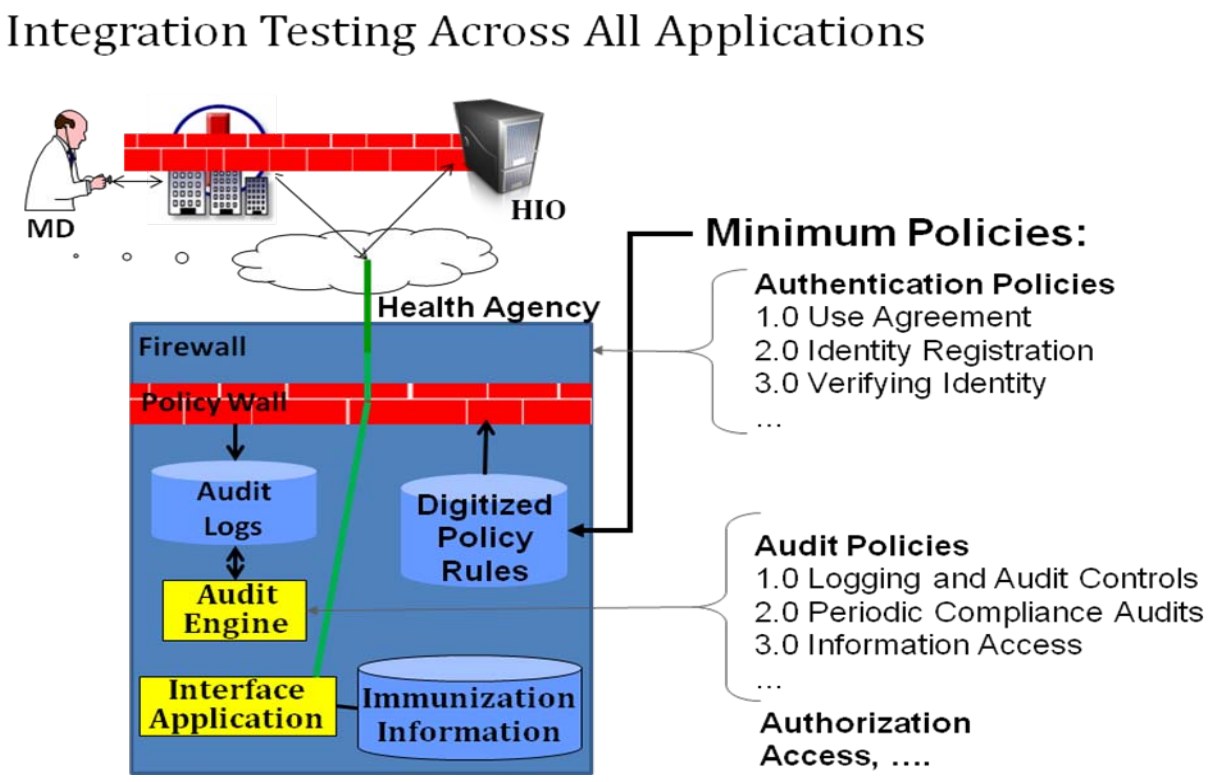
[9] Each element of the Uniform Security Policy components must be tested. There may be more than one action in (for example) authentication policy 2.1.2

IMPORTANT NOTE:

Because testing involves many different types of users, it is critical to de-identify the data used for the test in order to protect patient identity. Testing should also be limited to a test environment using valid logins and passwords that apply only to that environment.

Figure 3: **Testing of Applications and Infrastructure**

This figure is a graphical representation of policy integration. As a transaction enters an organization's system, it typically passes thru a "firewall" that provides an initial security screening. Policies need to be digitally implemented in the next layer of security, a policy rules engine or "Policy Wall." Basic policies (written in English) are converted to Digitized Policy Rules which are parsed according to the type of transaction and implemented with a minimum amount of human intervention. The authentication policy invoked by a particular type of transaction should determine the success or failure of passing thru the Policy Wall. Both incoming and outgoing transactions should pass thru the Policy Walls rules checking. Because the audit policies are meant to record activity "after the fact," they are not intended to be an upfront screen function. However, it is necessary to ensure that the correct information is being recorded.



Next are the five levels of testing that should be completed while evaluating adoption of the Uniform Security Policy. A description of each level of testing follows:

1. Functional Testing
2. Regression Testing
3. System Testing
4. Integration Testing
5. Load Testing

Functional Testing
The first phase of testing the Uniform Security Policy is the functional testing. This should be completed to prove that the system configuration for the security policies is working on each individual software application. For example, if there is a Master Provider Index, a test would be completed on that application to ensure that the test script for entering provider data is validated and in the system. Information entered into the fields in the Master Provider Index should be checked to confirm it is the expected result. The process should be completed for each application in the architecture.

Regression Testing
Within the testing phase regression testing proves that the system does not work when it should not work. An example of this would be to prepare test scripts knowing that the data for adding a provider to the system is missing an attribute. For instance, the Uniform Security Policy requires that the provider license be entered into system when you register the provider. This testing phase would purposely leave out the license number for a provider during the data entry. The result should be that the system doesn't accept that provider. The tester will enter the data they do have for the provider and the expected result is an error message "all fields are required, provider entry cannot be completed". To validate this error, check the Master Provider Index to make sure the provider did not get entered into the system. Regression testing should be completed at each phase of the testing.

System Testing
System testing is the testing of the database and applications within the HIE of the Uniform Security Policy. This phase of testing is still at the organization level and tests the workflow for a provider accessing a patient record for treatment purposes all the way through the system, touching each application as required in order to prove that the Uniform Security Policy will work throughout the applications. The same test scripts from the functional test can be used, however, each application must be checked to validate that the provider data is where it is supposed to be and that the authentication of that provider works as the Uniform Policy states. The auditing process should be checked thoroughly during this phase as well. Once all the test scripts have been completed, audit reports should be generated and checked against the test scripts to be sure all applicable information is on the audit log. Again, the audit reports should reflect the components of the Uniform Security Policy. Any and all issues should be resolved before moving into integration testing.

Integration Testing
Integration testing occurs after the system testing. This is the testing where the HIO is validating that all interfaces to external or internal systems are working properly based on the Uniform Security Policy. Integration testing involves the test of sending transactions that relate directly to the Uniform Security Policy, between multiple applications and/or organizations to determine if interfaces work, the data transmitted is what is expected and the established policies are supported as data moves between organizations. As these policies are meant to apply to sharing of electronic health information across

state lines, it is necessary to have any partner HIOs involved in the testing process. The check points tested include adding a provider, authenticating that provider and an audit record of what the provider accessed and when. Again, all of this is based on the Uniform Security Policy and a test script should be developed for each policy element.

The methods for testing in the system test also apply to the integration testing. Both methods of testing need to ensure that each use case transaction invokes the proper policy rules at the appropriate level of testing. Any issues that are found should be classified by type of issue and resolved by reviewing and modifying the workflow, the software and hardware functionality or the policy.

Once the issues have been resolved it is necessary to completely test the system and the integration until you can get through all your test scripts with all issues resolved. At that point it is appropriate to move to the next phase of testing.

Load Testing

Load testing is the testing of the system to examine scalability issues. This type of testing is done in order to ensure that the software applications will be able to handle the normal workload, with the Uniform Security Policy in place. Load testing is completed by using the test scripts already developed and having several people perform each transaction at the same time. If the system becomes slow, it may be necessary to tune the database and/ or have a hardware review. At this point the technical team may also need to review the policy configuration or the custom coding, if applicable.

As a final step, the testing team needs to document that all testing was successful. This documentation will be important for Certification and Authorization to operate using the Uniform Security Policy. The documentation should ultimately be approved by the project team and stakeholders.

Training

Creation of a training plan is an essential step in assuring properly implemented Uniform Security Policies for authentication and audit. The plan should reflect system roles and access requirements, define users, document functionalities of the system and how they integrate with subsystems, as this relates to the Uniform Security Policy. The plan needs to identify who will be trained in what role level, what methodology and curriculum will be used, who will conduct the training, how frequently the training will be repeated and how the training will be evaluated. Ongoing training beyond "go live" should be offered whenever the authentication and audit policy changes, a new application and/or HIO is added or new system users are brought on board.

Initial feedback from the stakeholder group should be included in the design of curriculum and care should be taken to have the curriculum reviewed by the privacy, security and legal professionals assigned to the team.

The training plan should include the groups targeted as well as standard messaging about the organizational minimum policy requirements. It is critical that all training materials be consistent across all HIOs with emphasis on the group you are targeting. HIPAA and other applicable federal and state laws should be included in the training materials so everyone is aware that by adopting the Uniform Security Policy, regulatory requirements have been addressed and are being adhered to.

To assure transparency and to ensure public "buy-in" for the project, it is recommended that a structured public education/outreach effort be undertaken with the following groups:

- **State Government** – State Government should be informed about the Health Information Security and Privacy Collaboration at a high level with emphasis on the Adoption of Standard Policies Collaborative and the basic minimum policy requirements around authentication and audit.
- **HIOs** – The detailed basic minimum policy requirements as well as the Uniform Security Policy should be shared with all HIOs and adoption should be encouraged so they are able to effectively achieve interoperability with other HIOs.
- **Provider Community** – The provider community will need to be aware of the Uniform Security Policy and how it will impact them. It is recommended that the HISPC Provider Education Toolkit be reviewed as a tool to help make providers aware of these policies.
- **Consumer Community** – The Uniform Security Policy should be shared with consumers so they can be assured that their health information is protected in a consistent, safe manner.

Deployment

Once system testing is complete and the system users have been trained, it is time to deploy the Uniform Security Policy. The following steps should be taken during the deployment phase:

1. Determine a "go live" date for the Uniform Security Policy across HIOs.
2. Complete and document the training phase with all system users.
3. Ensure that all new or modified applications (off the shelf or custom programmed) to accommodate the Uniform Security Policy have been installed and correctly tied to the production database by having the technical team document new or modified applications that need to be moved into the production database and creating a checklist to follow.
4. Have the appropriate support in place to handle questions that may arise with the use of the Uniform Security Policy. For the first week or two it may be necessary to have additional staff on your support team in order to ensure fast response times for systems users. This support team should be a combination of business analysts and technical personnel.
5. Communicate the "go live" to the systems' users, provide copies of the policy and a documented support mechanism (this could be your "help desk" procedure).
6. Post copies of the policies and user guides to each organization's intranet or co-locate them on a common secure web site.
7. As users begin using the system and the new policy requirements, keep track of any issues that may arise.
8. Regularly review issues and make modifications as necessary to training material, FAQs, policy verbiage and other supporting material.
9. Regularly schedule follow up/refresher training for all users required to adhere to the new policies.

Production

The production phase involves the actual "go live" and the ongoing evaluation and maintenance of the Uniform Security Policy. The first item that should be addressed at "go live" is the support requests received from your users. These requests can include many different types of issues. Many times when a user needs support, it can be attributed to user error, system error (bug) and/or a workflow process. The support requests should be continually evaluated and may require decisions around several areas. Some of the questions to ask when reviewing support requests are:

- Is the workflow efficient when using the Uniform Security Policy? For example: is the authentication practice efficient for a provider to use during a patient encounter? Should business process analysis be completed again?
- Are there software bugs in the application when implemented in a production environment and/or integrated with the production database? Remember: A system and/or integration testing must be completed again after the bug fix is applied to the test database. You may find that users have workflow that will need to be added to the test data.
- Was training sufficient for the users? Are there groups or sub-groups of users that need more instruction on the policies, procedures, and or practices? Should the training material and the material posted on an organization's intranet site or common web site be revised?

In addition, the HIO should have answers to the following questions regarding the production phase:

- How will you measure the successful application of policies after they are moved to production?
- How will you evaluate on a regular basis if the policy is current and/or needs to be modified because of regulatory changes, changes in the environment, technical changes, etc.?
- Who is responsible for policy updates, ongoing monitoring for effectiveness and follow up training, especially when policies change?

By keeping track of the support requests, the HIO can begin to measure the effectiveness of the adoption of the Uniform Security Policy. It is possible to create reports that can show the types of issues encountered, who encountered the issue, the response time to resolution and improvements in system use. This will be very valuable as the effectiveness of the adoption process is measured.

It is important to have a process in place to continue evaluating and maintaining the usefulness of the Uniform Security Policy as the policy may be impacted by several issues. It is suggested that the steps in this adoption guide be used to evaluate the Policy if any of the following events occur within your organization:

- Addition of any new business process to your workflow
- A change in workflow
- An upgrade of your software applications
- An upgrade to your hardware infrastructure
- Results from regularly conducted risk analyses and compliance audits
- A change in federal or state law related to privacy and security

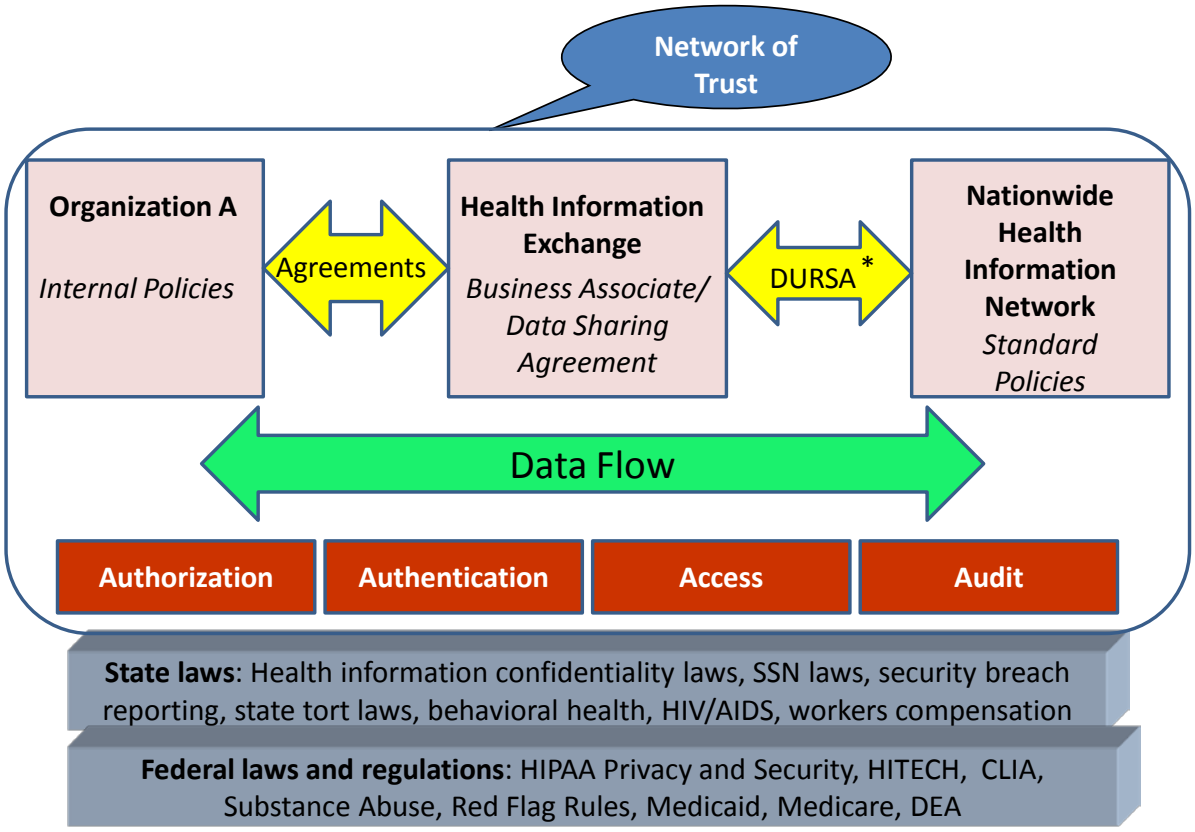
Anticipated Challenges and Recommended Mitigation Strategies

Figure 4: **How Health Information Exchange Fits in the Legal and Security Context**

As depicted in the graphic below, the focus of health information exchange is the secure transmission of meaningful health data across organizational boundaries. The legal and policy context of health information exchange is found in federal rules and laws that are further modified by state laws. The technical foundations for secure and private transport of health information are principles used to control the "**4 As**":

- **Authorization** (who gets to view and edit the data)
- **Authentication** (how we know them to be who they assert)
- **Access** (what data they can access)
- **Audit** (the record of who has seen and changed what data)

The applications of the principles outlined by the 4As are specified in legal agreements among organizations, health information exchanges, and the Nationwide Health Information Network. This network of trust will benefit from the Uniform Security Policy recommended by the Adoption of Standard Policies Collaborative.



*Data Use and Reciprocal Support Agreement

The following table delineates some anticipated challenges that your organization may face during the adoption process and some potential mitigation strategies to effectively address these categories:

Table 5: **Anticipated Challenges and Recommended Mitigation Strategies**

	Anticipated Challenge	Mitigation Strategy
BUSINESS	Local or regional solutions do not conform to national standards	Educate member organizations on standards and the benefits of standards
	Nomenclature varies across organizations	Use the technical work group to map nomenclature to the standard
	Funding is not available	Write the business plan; solicit funding
	National standards have not been adopted	Review draft national standards and coordinate local/regional standards development to match, where feasible, draft new national standards; inform national standards organizations of lack of standards
	Administrative, physical and/or technical safeguards are not adequately addressed	Incorporate regularly scheduled and comprehensive review of policies, procedures and practices into the business plan. Regularly schedule risk analysis and audit (periodic and compliance). Provide regular training to new and existing users and management.
LEGAL	Granularity of audit logs are not adequate for reports	Evaluate system triggers; implement more granular data capture
	Too many or too few audit logs are generated but do not capture either what is needed or more than can be reviewed in a timely manner.	Perform a legal review of audit plans and procedures as well as proposed content of logs to reduce legal risk, meet appropriate security standard requirements and address regulatory requirements.
	Identifying data specified in policy: o Behavioral Health o HIV/AIDS o Sexually transmitted diseases o Alcohol and Chemical Dependency o Worker's Compensation o Medicaid o Medicare o Certain Minor Information o Genetic o Reproductive	Establish a legal work group to review policies, law and practices related to consent, authorization and specific "more stringent than HIPAA" requirements.

	Anticipated Challenge	Mitigation Strategy
POLITICAL	Lack of transparency	Educate the stakeholders; develop a web site for documentation and dissemination.
	Assumptions are not clearly defined	Improve governance processes to include better communication and greater specificity.
	Complaints of lack of inclusiveness from stakeholder groups	Widen reach by adding more stakeholders. Communicate with stakeholders who had been invited to participate and elected not to be involved, re-inviting them to the table.
TECHNICAL	Varying authentication practices	Define the minimum requirements by adopting the standard policies.
	System performance/ scalability	Provide a technical evaluation of changes recommended to effect improvement including resources and timeline.
	Identifying data specified in policy: o Behavioral Health o HIV/AIDS o Sexually transmitted diseases o Alcohol and Drug o Worker's Compensation o Medicaid o Medicare o Certain Minor Information o Genetic o Reproductive	Present a list of all available data elements to have reviewed by legal. When feedback is provided implement the ability to "lock"/ "unlock" data elements by role.
	Legislation or regulations are required to implement the policy.	Identify models and educate the lawmakers and/or regulators.
EDUCATIONAL	Policy implementation requires legislation or regulation	Prepare whitepapers identifying models. Provide proposed statutory or regulatory language to the legislature or regulating body.
	Importance of security parameters is not understood by all	Educate all users and governance groups.
GOVERNANCE	Policy conflict in member organizations	Specify mechanisms to be used in conflict resolution as part of the legal agreements.

Summary and Next Steps

Since health information technology will be a significant component in national plans to improve healthcare, the importance of privacy and security has become preeminent. However, the specifications to ensure standard application of best security practices across organizations have not been addressed. The Adoption of Standard Policies Collaborative (ASPC) has begun this work. This Guide to the Adoption of the Uniform Security Policy provides a framework designed to assist groups as they seek consensus on privacy and security practices to support the electronic exchange of health information and clears the path for addressing more of the critically important concerns that lie ahead.

Specifically, model policies for interstate exchange of health information are offered for authentication and audit. The other two security domains, authorization and access, were outside of the scope of the work of the ASPC during this specific project. However, having prioritized authentication as one cornerstone of privacy and security, and audit as the foundation for accountability and trust, a few aspects of authorization and access bled into the discussion. The more complete standardization of policies for these areas is one that remains open for the work of other groups. The framework used by the Adoption of Standard Policies Collaborative provides a solid basis for developing standard policies for authorization and access.

Next steps in developing standard security policies and practices include evaluating and testing the viability of this framework as it is adopted and implemented for interstate health information exchange. No matter what legal mechanisms are used to establish a network of trust among health information exchange organizations, specificity is required for security policies and practices. The framework offered here is intended as a starting point to be augmented, expanded, and tested as health information exchange becomes the modality to provide accurate clinical information at the point of care to improve healthcare quality.

The Adoption of Standard Policies Collaborative recommends the following:

1. Testing the framework in environments (for example, Virginia/Tennessee and Washington/Oregon) that implement and assess the viability of the standard policies for authentication and audit.
2. Documenting the types of use cases and transactions that will and do occur in health information exchanges, to provide paradigms for policy and practice development for authorization, access, disaster recovery, archiving, and other intersecting domains.
3. Establishing or designating a rigorous and transparent policy review process, using the standards development organizations methodologies and practices.
4. Standardizing the testing of the technology supporting these policies for the vendor market.
5. Evaluating the capacity to adhere to and support these policies as demonstrated in the certification of health information exchanges.
6. Providing funding for prototypes to test policy standards as they are technologically implemented.

In summary, the focus of health information exchange is the secure transmission of meaningful health data across organizational boundaries. The legal and policy context of health information exchange is found in federal rules and law that is further modified by state laws. The technical foundations for secure and private transport of health information are principles used to control:

- **Authorization** (who gets to view and edit the data)
- **Authentication** (how we know them to be who they assert)
- **Access** (what data they can access)
- **Audit** (the record of who has seen and changed what data)

The application of the principles outlined by these "**4As**" is specified in legal agreements among organizations, health information exchanges, and the Nationwide Health Information Network. This network of trust will benefit from specified standard policies like those recommended by the Adoption of Standard Policies Collaborative.

APPENDICES

Appendix A: Feasibility: Preparing for Change and Process Checklist

If your organization is interested in assessing the feasibility of adopting the Uniform Security Policy must first be prepared for the significant changes that will be required to adopt and implement these standards. The steps that follow in the change process are articulated in the Checklist that follows in Section 2.

Section 1: Preparing for Change

To provide background for adopting the Uniform Security Policy, it is critical to understand the nature and context of organizational change, as change is a prerequisite to adoption. The organizational change perspective focuses on contextual features that enable an organization to respond to both internal pressures and external influences. The ASPC adapted its framework from Rogers' work on diffusion of innovative practices.[10] The diffusion model emphasizes characteristics of the policy/practice that may increase the likelihood of adoption by individuals and organizations. These complementary perspectives provide the framework that informed the recommendations for the adoption process proposed by the ASP Collaborative.

It is important to remember that any organizational change needs to involve senior organizational leadership for both public and private sector organizations. There needs to be a demonstrated value that can be bought in before senior leadership will consider adoption of the Uniform Security Policy, especially when that policy stretches beyond the bounds of an individual organization.

[10] Rogers, E. 2003. Diffusion of Innovations. New York: Free Press

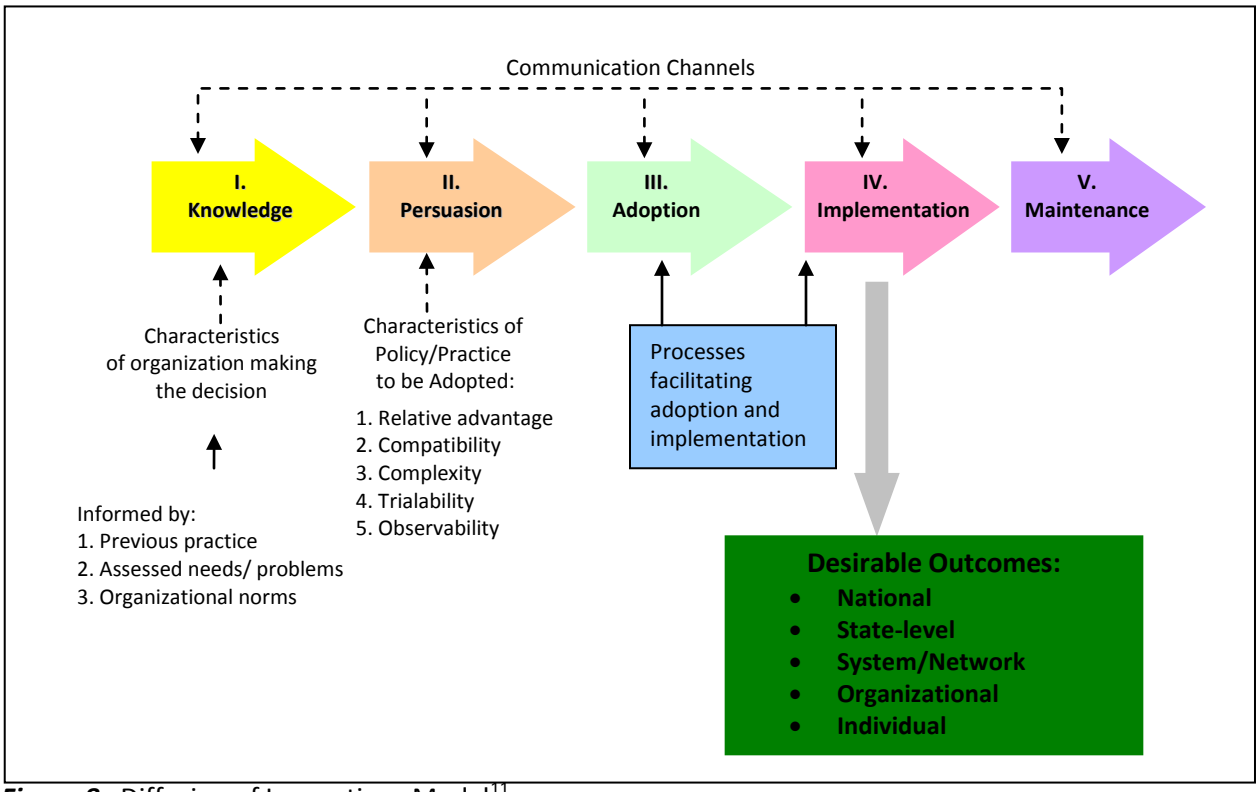


Figure 8: Diffusion of Innovations Model[11]

To use this framework to prepare for change, consider the following:

1. Is your organization prepared to assure ***communication*** among organizational members as the central focus of all steps in the change process?
   - ✓ Transparent
   - ✓ Across many organization levels
   - ✓ Develop respect for the input of all
   - ✓ Organizational structure is important in facilitating the communication

2. Does your organization have the ***knowledge*** that it needs to implement minimum security standards for health information exchange?
   - ✓ Assess current policies, procedures, and practices
     - Internal
     - Industry-specific
   - ✓ Needs assessment or gap analysis
   - ✓ Factors that impact change
     - Organizational culture
     - Professional norms

[11] Rogers, E. 2003. Diffusion of Innovations. New York: Free Press p.170

3. Is your organizational leadership ***persuaded*** to pursue this change to implement minimum security standards for health information exchange?
    - ✓ Relative advantage
        - Cost perception vs. value
    - ✓ Compatibility
        - Ease of transition
    - ✓ Complexity
        - Number of business units affected
    - ✓ Trial-ability
        - Proof of concept: Can we test the proposed innovation?
    - ✓ Observe-ability
        - Does system output reflect all processes
        - Transparent functionality

4. Is your organizational leadership ***adopting*** minimum security standards for health information exchange?
    - ✓ Accept the proposed idea or innovation as a valued institutional goal
    - ✓ Awareness of the changes that will be required to adopt
    - ✓ Determined to proceed
    - ✓ Prepared to develop a change management plan and strategy, including:
        - Solicit feedback
        - Assess adopter involvement or user attitude
        - Commit to the organizational investment (such as training and resources)
        - Commit to the timeliness of delivery, ease of use
        - Evaluate the perceived efficiency and relevance of the policies and practices
        - Channel information to organizational members
        - Convey the salience of the practice
        - Actively enable a change in behavior
        - Documenting the change process

5. Is your organizational leadership prepared to ***implement*** minimum security standards for health information exchange?
    - ✓ Require a focus of both management commitment of resources and research efforts
        - Aware of the types of change taking place within the organization
        - Internal barriers and facilitators
    - ✓ Require system-wide alterations and major changes at all levels of the organization
        - Requirements of resources
        - Centrality of consensus
    - ✓ Been adopted and accepted throughout the organization as standard practice
        - Systematic and continuous evaluation
        - Monitor outcomes
    - ✓ Recording and communicating the progress of the change process

Section 2: Checklist

The following checklist is offered as a summary of steps described in the adoption guide. The purpose is to assist organizations in tracking progress of their adoption of the Uniform Security Policy. It may also be useful in assigning tasks and functions to actors in the HIO.

Goal and Scope		
	☑	**Notes**
Consider Pre-existing Structure		
Determine if this is an existing health information organization (HIO) or if an HIO is being planned		
If the HI0 exists, what level is it organized at: **Local** **Sub state region** **Sub state region that crosses state lines** **State** **Multi-state**		
What are the existing agreements?		
Do these agreements include references to standards for: **Authentication** **System to NHIN** **System to system** **Entity or individual to system** **Individual to participating entity**		
Authorization **License or credential checking** **Use of digital certificates** **System certification** **Automatic checks for changes**		

Goal and Scope (continued)		
	☑	Notes
Access **Role definition:** **What are roles** **What roles see what data** **Web, intranet or closed network** **Data use** **Use for treatment** **Use for medical analysis and consultation on behalf of a patient** **Secondary use of data** **Research** **Public Health** **Other (define)**		
Audit **Log generation (for example, network level, application level, transaction level, etc.)** **Log content specification** **Sharing logs/log reporting** **Failed logins/logins at inappropriate hours** **Audit policies and procedures (periodic and compliance)** **Investigation/mitigation/action for inappropriate use and disclosure** **Capability to change audit criteria and what is tracked**		
Establish a privacy, technical security and administrative/business security work group[12]		

[12]Due to potential breaches, this group needs to include representation from the general technical side, the general business side, the security side (administrative, physical and technical), the compliance side and the privacy side. (Compliance needs to be included due to potential state law issues, differing federal laws such as GLBA for health plans, etc.)

Goal and Scope (continued)		
	☑	Notes
Membership **Chief Information Officer (CIO) from the highest level of organization** **Network Engineer** **Application engineer** **Legal/compliance** **Human resources** **Chief Security Officer (CSO)** **Chief Privacy Officer (CPO)** **Management (business side)** **User** **Administrative policy** **Legislator** **Government (executive branch)** **Public information officer/communications** **Liaisons from other organizations, government, etc.**		
Goal and Scope Milestones ✓ **Document the business model of the Health Information Organization** ✓ **Collect and analyze existing agreements** ✓ **Establish a privacy, technical security and administrative/business security**		

Planning: Resources, Use Case, Risk Analysis and Legal		
	☑	Notes
Existing policy and legal requirements are identified **Legal counsel of the Health Information Organization governing authorities** **HISPC phase 1 and 2 findings[13] (if available for your state)** **CMS, OCR, other federal agencies, state agencies/attorney generals' office(s)** **Consent or authorization requirements**		
Enacting the standards policy **Legislation needed** **Regulation needed** **Contractual terms needed** **Inter-organizational agreement or Memorandum of Understanding (MOU) needed**		
Define the scope **Structure of the HIO: Treatment (individual) health vs. Secondary use of data (such as Public Health business case)** **Use case definition** **Resource availability (fiscal, workforce)** **Realistic time line** **Budget parameters (development and implementation as well as on-going)**		
Planning Milestones: ✓ **Summary report on organizational, state, local, regional legal and institutional (hospital, pharmacy, public health, workers compensation, prisons, behavioral health, etc.) policy environment** ✓ **Written plan to authorize the standards policy** ✓ **Written plan to implement policy for the HIE**		

[13] See the RTI International website (www.rti.org) for information that pertains to the states and territories that you are working with. Another helpful resource would be the ASPC's ***Final Report***.

Implementation: Consensus, Testing and Deployment		
	☑	Notes
Establish the implementation team **Technical personnel** **Business Managers** **Governance group for the organization** **Representatives from the user community**		
Determine type of exchange to be tested **Data elements** **Data formats** **Nomenclature**		
System requirements **Authentication** **Authorization** **Access** **Audit**		

Implementation: Consensus, Testing and Deployment (continued)		
	☑	Notes
Business requirements **Risk Analysis** **Legal Analysis (state and federal, and other regulatory or accreditation requirements appropriate to your situation)** **Policies and procedures** **Training (management and end users)** **Processes** **Participation** **Administrative Safeguards (partial list)** **Authorization, Authentication, Access and Audit** **Disaster Recovery/Emergency Mode Operations Plan (DRP/EMOP)** **Physical Safeguards** **Facility security** **Facility contingency plan (see DRP)** **Data Backup and Recovery** **Media and portable device management and controls** **Remote access management and controls** **Data and media disposal and re-use** **Security and Privacy Enforcement**		
Testing Plan **Minimum requirements specified** **Testing team** **Time line and resources** **Data, applications and processes to be tested**		

Implementation: Consensus, Testing and Deployment (continued)		
	☑	Notes
Testing **Remediation and Documentation of Testing Results** **Approval** **Identification of who has authority to validate test results**		
Re-testing **Acceptable completion** **Identification of who has authority to validate test results**		
Deployment to production **Certification and Accreditation** **Deployment to production** **Production rules and procedures** **Incidence Response**		
Implementation Milestones: ✓ **Documentation of testing and remediation** ✓ **Documentation for C&A** ✓ **Go live**		

Evaluation: Production, Training and Deployment		
	☑	**Notes**
Risk analysis		
Review of audit reports		
Audit of authorized users		
Review of system performance		
Security breaches		
Data quality review		
User access data reviewed		
Evaluation Milestones: ✓ **Report to the Governing group** ✓ **Report to funding source(s)** ✓ **On-going training** ✓ **Feedback to standards setting groups on the viability of minimum requirements** ✓ **Required mitigation and mitigation plan development Required policy, training, audit criteria, etc. review and revision** ✓ **Documentation, document retention and document destruction**		

Uniform Security Policy

March 31, 2009

Table of Contents

Introduction

Purpose	The purpose of the following authentication and audit minimum policy requirements is to foster cross state and cross model data exchange. This policy is intended to be agnostic to the state-specific health information exchange model(s) and is recommended by the HISPC Adoption of Standards Policy Collaborative (ASPC) as a set of basic, minimum policy requirements that have been publicly vetted and accepted. Through consensus negotiations between 6 states[14] and facilitation/support with the other ASPC states[15], the ASPC has established baseline privacy and security protections for organizations engaged in exchanging electronic health information. Health Information Organizations (HIO) participating in Health Information Exchange (HIE) may have different policies, but should incorporate these basic policy requirements for registering and authenticating users, both individual users and organizations, wishing to participate. The HIO must (1) register, (2) execute an agreement with, (3) verify the identity of, (4) provide digital identification for, and (5) maintain an account for all users. Each of these processes has a set of minimal requirements that must be defined in order for the participants of the HIO to trust their trading partners and users. The HIO must implement procedures for auditing access in HIE to confirm appropriate use. Pursuant to the American Reinvestment and Recovery Act, 2009 Title 13 Subpart D, the HIO and its business associates must submit to the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
Scope	The scope of this policy is limited and specific only to electronic authentication and audit policies and process when a health care provider requests patient health information through an HIO for the purpose of treatment. The component parts included in this policy represent the requirements agreed to by participating states. The full scope of the requirements considered for negotiation is available in the ASPC full report at: www.okhca.org/aspc
Draft	March 27, 2009
How To Use	This policy does not serve as a standalone document. For more information on the HISPC Project, go to:

[14] Arizona, Connecticut, Colorado, Nebraska, Oklahoma, and Washington.
[15] Maryland, Ohio, Utah, and Virginia.

	http://www.hhs.gov/healthit/privacy/execsum.htm
Disclaimer	This policy has not been fully tested and is not intended to represent a complete security policy for health information exchange. This work is intended as a general resource (or reference) and is not meant to provide legal advice to any person or entity that receives a copy of the work. Readers should consult with competent counsel to determine applicable legal requirements, as well as privacy and security experts. Upon publication/public release of this document, please contact the Office of the National Coordinator (ONC) for Health Information Technology, Health and Human Services (HHS) for additional information. Email: onc.request@hhs.gov

Publication Version Control

Version	Date	Name	Purpose of Revision
Original	Jan 26, 2009	Chris Doucette Francesca Lanier	Initial Draft
Version 1.0	Feb 5, 2009	Chris Doucette	Add ASPC states / Legal / TAP comments
Version 2.0	Feb 25, 2009	Chris Doucette Francesca Lanier	Add Stakeholder Review Comments
Version 3.0	March 10, 2009	Chris Doucette Francesca Lanier	Add final Legal comments / Final Draft submittal to ONC.
Version 4.0	March 27, 2009	Chris Doucette Francesca Lanier	Final ASPC project deliverable

Authentication Policy

Section 1 - Use Agreement

1.1 Requirement - Use Agreement

Health Information Organizations should have a data sharing agreement with participating providers that defines the privacy and security obligations of the parties participating in the HIO. These agreements should require the use of appropriate authentication methods for users of the HIO that depend on the users' method of connection and the sensitivity of the data that will be exchanged. In addition, these agreements should reasonably ensure sufficient auditing requirements to determine access and use of the system, as well as secure transport of health information across the network, are appropriate.

Where there is cross-HIO exchange of data, authentication and audit requirements should be defined through a Data Use and Reciprocal Support Agreement (DURSA). The DURSA should define their relationship between the HIOs and ensure, among other things, appropriate authentication and audit of users and queries across HIOs.[16] Reference: M2: A Model Contract for Health Information Exchange and P2: Model Privacy Policies and Procedures for HIE.

Section 2 - Identity Registration

2.1 Required Data Set for Authentication

A directory of data sources within the HIO will include primary contact information of registered members, identity attributes of providers, organization and systems.

2.1.1 Data Source

[16] Markle Foundation – Connecting for Health - http://www.connectingforhealth.org/

A directory of data sources within the target HIO is required, and includes name of the HIO and any data sources within that HIO. The primary contact information for the data in the directories should include primary contact name and any contact phone numbers. *DAT 2*[17]

DAT 2 Attribute also considered:
Service location

2.1.2 Provider Identity Attributes

The HIO will collect the attributes as needed for unique identification of the individual accessing the information in the HIO[18]. Required elements are profession, role, name, the practice address (not home address), identity service provider and organization affiliation, business/legal address and License/ID. Other attributes that are required, if they exist for this individual, includes:

- Specialization / specialty,
- Email address,
- National Provider Identifier (NPI), and
- Digital identity. *DAT 10*

DAT 10 Requirements also considered:

Directory of all HIO's
Included in the directory: Contact fax numbers
Master provider index to query by provider for a specific patient

2.1.3 Organization Identity Attributes

Identifying the organization requires collecting the following attributes: organization name and email address. Other attributes are required if they exist, including:

- Digital identity,
- EDI administrative contact,
- Clinical information contact,
- Service Location, and
- Predecessor name and date of change.

If the HIO is a regulated healthcare organization, all supporting organization attributes above are required, as well as:

- License/ID,
- License status,
- Registered name, and
- Registered address. *DAT 11*

[17] AUT *, AUD *, DAT *, SYS *, POL * - refers to a negotiated minimum policy requirement and can be referenced the Cross State technical source document.

[18] 45 C.F.R. § 164.312(a)(2)(i) (requiring assignment of a unique name or number for identifying and tracking user identity).

DAT 11 Attributes also considered:
Identifying an organization requires -License status

If the HIO is a regulated healthcare organization-
Address
NPI
Organization address, National Provider Identifier (NPI), organization affiliation, closure date, and successor name

2.1.4 Identity Attributes of the Data Source System

Identifying the system requires the attributes of:

- System name,
- Digital identity,
- Organization affiliation,
- System IP address, and
- System domain name.

If there is no system domain name, the system IP address may be used. For purposes of identifying the originating electronic data sources, would require a date stamp and at least one of the following is required: the system (1) name, (2) IP address, or (3) domain name. Any identifying system types, such as the laboratory information systems, electronic health record system, emergency medical system, etc should also be included. *DAT 12*

2.2 Role-based Access

Proper registration requires the establishment of a defined role associated with the registered user.

2.2.1 Role

The individual's organization role[19] is required for role based access and should include the context of the organization. If the healthcare functional role[20] or the structural roles[21] exists, they are also required. *DAT 1*

Section 3 - Verifying Identity

3.1 Processes Used to Verify Identity

Identity is verified through authentication of the user, the organization and the HIO's system.[22]

3.1.1 User Authentication

The methods for user identity vetting include both verifying the identity in person by a trusted authority and verification through the use of a demonstrated government-issued ID. The trusted authority is recognized by the state or federal government.

[19] As defined in the American Health Information Community (AHIC) Use Cases.
[20] The functional role is dynamic and is a function of the role in which you are acting.
[21] A structural role is persistent and can be mapped to professions that are recognized.
[22] 45 C.F.R. § 164.312(d) (requiring "procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed").

An applicant requesting an identity tied to a regulated provider type must have provider licensure validation. It is acceptable that this occur along with the validation required of any employee of a licensed provider organization.
Also, the HIO use of a specific naming convention as a primary identifier is required with a minimum assurance level used of Medium (knowledge/strong password/shared secret). *AUT 1*

AUT 1 Requirements also considered:

The use of a Notary for user identity vetting;
HIO using of an Object Identifier (OID) as a specific naming convention for the primary identifier;
The User handling sensitive information, given the state's legal/regulatory restrictions on records including HIV, mental health, substance abuse, sexual health, prison health and/or genetic information

3.1.2 Organization Authentication

Organization identity vetting can be accomplished through personal knowledge of a registration authority, that the organization is who they say they are by a demonstrated documentation of corporate existence.
The HIO is required to use a specific naming convention as a primary identifier, and this would include the use of object identifier (OID) or idiosyncratic naming, if either of these exists. This is a requirement at the state level and the ASP Collaborative recommends development of a naming convention that can be registered and identified nationally.
The minimum assurance level required for organization authentication is High (PKI/Digital ID). *AUT 5*

AUT 5 Requirements also considered:

Organization identity vetting using a certification such as Joint Commission, SAS-70 Compliance, or ENHAC Compliance
The Organization handling sensitive information, given the state's legal/regulatory restrictions information including HIV, mental health, substance abuse, sexual health, prison health and/or genetic information.

3.1.3 System Authentication

System identity vetting, ensuring the data are coming from the system that they are supposed to be coming from, requires the assertion by an authorized organization representative and/or the demonstration of association with another licensed organization.
The minimum assurance level required for system authentication is High (PKI/Digital ID). *AUT 3*

AUT 3 Requirements also considered:

System identity vetting through in-person site visits, certification such as FDA or CCHIT, or verifying the system IP address and system domain name The System handling sensitive information, given the state's legal/regulatory restrictions information including HIV, mental health, substance abuse, sexual health, prison health and/or genetic information.

3.2 Variations Based On Type and Location of User

3.2.1 User Identity, Role and Affiliation Verification

The user identity, role and affiliation must be checked for both revocation and expiration at the time of logon to the system. If either case pertains, use would be denied. *SYS 13*

SYS 13 Requirements considered as optional:

Authentication method checking and challenge/response checking

3.2.2 Signature Verification

The HIO is responsible for digital verification of non-repudiation signer credentials. Verification implies that:

- The credential issued by a trusted authority,
- The credential is current,
- The credential is not suspended or revoked, and
- The credential type is appropriate (for example, physician or pharmacist).

If the signed-by-person claimed (non-repudiation) exists, it should also be verified. *SYS 11*

3.2.3 Assurance Level

It is required that the level of assurance be declared and should be communicated in terms of the then current National Institute of Testing and Standards (NIST) requirements. For the HIO to migrate data an assurance level of at least Medium (knowledge/strong password/shared secret) is required. *DAT 3*

3.2.4 Relationship To Patient

If the HIO is exchanging for purposes of treatment, the provider seeking access needs to demonstrate or certify that they have a treatment relationship with the patient. *POL 12*

POL 12 Requirement also considered:
A system ability to calculate some value that represents the quality of a match based on an algorithm, for purposes of tracking measurements

3.2.5 Threshold Calculation

Patient matching content out of scope[23]. *SYS 5*

3.2.6 Digital Signature

The HIO is required to have the ability to use digital signatures, if they exist, at least at the provider level. *SYS 9*

SYS 9 Requirement also considered:

A policy allowing the organization to accept or express data without signature or would it express with a caveat or some marker that no signature was received

3.2.7 Persistence

The use of persistence[24] of the source signature is required and is the responsibility of the HIO with its own participants. The attributes required are persistent user signature, persistent organization signature and persistent system signature. Non-repudiation of origin is also the responsibility of the HIO with its own participants, and includes the attributes of user, organization and system accountability. If source authentication exists it is also required. *DAT 8*

3.3 Accommodations for Cross-HIE Verification and Data Integrity

3.3.1 Restricted Data Sharing and Data Integrity

The transmission of caveats regarding data completeness is required to indicate that an entire record may not have been transmitted. The use of pertinent state-specific caveats should be included in the transmission. *POL 2*

3.3.2 Authenticate Recipient Identity (Organization / System / User)

[23] This requirement is outside the limited scope of the ASPC effort, however the states elected to collect this information due to the subject matter and relevancy as it related to the selected use cases. For more information see the ASPC Individual Requirements Review (IRR) document.
[24] Persistence indicates proof that data has not been altered and is only valid during the communication session.

The identity of the recipient must be established and the method of identifying recipients of communications can include, but is not restricted to: (1) derived from ordering system communications, (2) selected from a provider directory, or (3) derived from identifiers included in the request for information. *AUT 6*

3.3.3. Required Elements for Matching

Elements for patient matching are considered out of scope[25], including if patient matching is necessary for the authentication or audit functionality. *DAT 6*

DAT 6 Elements considered for patient matching include:
Identifiers (Patient Account Number, SSN, Driver License, Mother's ID, MRN, Alt Patient ID);
Patient Name (First, Middle, Last, Family Name, Suffix, Prefix/Title, Type); Mother's Maiden Name (Family Name, Surname); Patient DOB; Gender, Patient Previous Name; Race;
Patient Home Address (Home Street, Street or mailing Address, Street Name, Dwelling Number, Other Designation (second line of street address), City, State/Province, Zip, Country, Address type, County Code); Patient Daytime Phone (country code, Area/City Code, Local Number, Extension, any other text); Work Telephone; Primary Language; Marital Status; Religion; Patient Ethnicity; Birth Place; Multiple Birth Indicator; Birth Order; Citizenship; Veteran's Military Status; Nationality; Deceased (Date/Time, Deceased Indicator)

3.3.4 Matching Criteria

Patient matching criteria is considered out of scope[26], including if patient matching is necessary for the authentication or audit functionality. *DAT 7*

DAT 7 Requirement also considered:

Defining a minimum number of three (3) data elements to query another system

[25] This requirement is outside the limited scope of the ASPC effort, however the states elected to collect this information due to the subject matter and relevancy as it related to the selected use cases. For more information see the ASPC Individual Requirements Review (IRR) document.
[26] This requirement is outside the limited scope of the ASPC effort, however the states elected to collect this information due to the subject matter and relevancy as it related to the selected use cases. For more information see the ASPC Individual Requirements Review (IRR) document.

3.3.5 Digital Signature

For the purposes of cross-HIE verification, the ability to use digital signatures is required at the provider level. *SYS 9*

3.3.6 Persistence

The use of persistence of the source signature is required and is the responsibility of the HIO with its own participants. The attributes required are:

- Persistent user signature,
- Persistent organization signature and,
- Persistent system signature.

Non-repudiation of origin is also the responsibility of the HIO with its own participants, and includes the attributes of:

- User Accountability,
- Organization Accountability, and
- System accountability.

If source authentication exists, it is also required. *DAT 8*

3.3.7 Data Authentication

For purposes of data authentication, the use of a timestamp is required at point of signature application. *AUT 4*

> *AUT 4 Requirement also considered, but is difficult to implement:*
>
> *Signature Purpose (ASTM E1762)*

3.3.8 Data Validation

Data validation of signer credentials should be issued by a trusted authority, should be current, and the credential should not be suspended or revoked, and the credential type should be appropriate (for example, physician, pharmacist or hospital). For purposes of data integrity, the data validation should indicate that the data has not been changed since the signature, and should have a timestamp at point of signature application. *AUT 7*

3.3.9 Type of Requestor

For verification purposes the requestor type should identify the exchange, organization (institution) and the user (individual). *DAT 4*

3.3.10 Signature Purpose

The signature purpose should be included as a minimum requirement, and any of the captured signature elements that exist should be included. *DAT 13*

The DAT 13 elements that were considered include:

Author's signature, Coauthor's signature ,Co-participant's signature, Transcriptionist/Recorder, Verification signature, Validation signature, Consent signature, Witness signature, Event witness signature, Identity witness signature such as a Notary, Consent witness signature, Interpreter, Review signature, Source signature, Addendum signature, Administrative, Timestamp, Modification, Authorization, Transformation and Recipient

Section 4 - Identity Provisioning

4.1 Types and Levels of Factor Provisioning

Refer to Section 3 for the required assurance levels for user, organization and system authentication [HISPC ASP reference AUT 1, 5 & 3 respectively]

Section 5 - Identity Maintenance

5.1 Registration Data

No current minimum policy requirements exist.

Audit Policy

Section 1 - Logging and Audit Controls

1.1 Log-In Monitoring[27]

As a part of log-in monitoring, an audit log is required to be created to record when a person logs on to the network or a software application of the HIO. This includes all attempted and failed logons.

The generated audit logs must be reviewed on a regular basis that is based on an audit criteria developed in advance. Anomalies must be documented and appropriate mitigating action and documented. The HIO should determine how long its state laws and risk management policies would require retention of this documentation. *POL 16*

1.2 Information Systems Review[28]

All HIE systems must be configured to create audit logs that track activities involving electronic Protected Health Information (PHI). The review of information systems shall include software applications, network servers, firewalls and other network hardware and software. The generated audit logs shall be reviewed on a regular basis based on audit criteria developed in advance. All anomalies must be documented and appropriate mitigating action taken and documented. All system logs must be reviewed. The review shall include, but not limited to, the following types of information: data modification, creation, and deletion. The HIO should determine how long its state laws and risk management policies would require retention of this documentation *POL 15*

1.3 System Review

Information system reviews should be conducted on a regular and periodic basis, as determined by the HIO. *SYS 4*

SYS 4 Requirement also considered:

Automatic trigger exists for any out of state access; Automated Audit review to permit ready review of any interstate access exists

1.4 Security Audit Practice

The frequency of performing regular security audits shall be determined at a specified frequency for the HIO. Auditing frequency typically varies by state/HIO for example Nebraska conducts audits yearly, and Washington conducts quarterly audits. Audits shall be conducted at least annually as a minimum requirement, and the comprehensive audit

[27] HIPAA Security Rule: 45 C.F.R. § 164.312(b) (requiring "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information"); 45 CFR § 164.308 (a)(5)(ii)(C) (requiring procedures for monitoring log-in attempts and reporting discrepancies **).**

[28] HIPAA Security Rule 45 CFR § 164.308 (a)(1)(ii)(D) (requiring covered entity to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports").

procedures should be developed, documented and available. The HIO should also conduct periodic external audits. *SYS 8*

SYS 8 Requirement also considered:

The sharing of risk scores with other RHIOs

1.5 Audit Trail and Node Authentication (ATNA)

The Audit Trail and Node Authentication Integration Profile[29] requires the use of bi-directional certificate-based node authentication for connections to and from each node. The use of certificates or encryption is required when the data are signed or when it is specified by the HIO policy. *SYS 6*

Section 2 - Periodic Internal Compliance Audits

In order to appropriately assure the security of Protected Health Information HIO's shall perform internal audits to evaluate their process and procedures.

2.1 Evaluation[30]

Under HIPAA security standards, administrative safeguards are required in order to exchange electronic PHI. Users of HIO exchanges needs to comply with all privacy and security regulations when exchanging electronic health information.

Additionally, periodic technical and non-technical evaluations are required to reasonably ensure that the covered entity is compliant with the provisions of the HIPAA Security Rule. Audit criteria must be developed and documented in advance for this type of evaluation, known as a "compliance audit". Evaluations shall be performed at least annually and when any major system or business changes occur. The evaluation shall include:

- The generation of a compliance audit findings report,
- Documentation that an identified deficiency has been addressed, will be addressed in order of priority, or represents a risk the organization is willing to accept,
- The documentation on the evaluation shall be retained for minimum of six years[31] however some states may have longer retention requirements. *POL 17*

Section 3 - Information Access

[29] IHE: Integrating the Healthcare Enterprise

[30] **HIPAA Security Rule 45 CFR § 164.308 (a)(8) – Evaluation**

[31] 45 C.F.R. § 164.316 (requiring retention for six years of policies and any required activity that must be documented under the rule). While 45 C.F.R. § 164.308(a)(8) does not require documentation of the compliance audit, it is a good business practice to do so and to retain that documentation for risk management purposes.

3.1 Audit Controls[32]

Under HIPAA security standards, technical safeguards are required including policy, data, and system requirements. All entities and their business associates must implement technical processes that accurately record activity related to access, creation, modification and deletion of electronic PHI. *POL 18*

3.2 Subject of Care Identity

To identify the identity of the subject of care, a matching criteria policy is a required (for example, a match on DOB, First Name, Last Name, Address, etc…) *AUT 2*

> *AUT 2 Requirements also considered:*
>
> *The collection and processing of patient demographics includes the collection of SSN and driver's license;*
> *The provider needs to demonstrate proof of the identity of the subject of care*

3.3 Demographics That May Be Logged

An additional audit log should be performed by the HIO for a subset of the subject identity attributes that have been used when a person is found. *DAT 9*

Section 4 - Need to Know/ Minimum Necessary for Data Management and Release

4.1 Information Disclosure

For purposes of information disclosure, a written policy is required which includes documentation of the following:

- The date and time of the request,
- The reason for the request,
- A description of the information requested, including the data accessed, the data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to another party,
- The ID of person/system requesting disclosure,
- The ID/verification of the party receiving the information,
- The ID of the party disclosing the information. *AUD 2*

> *AUD 2 Requirement also considered:*
>
> *The description of the information requested also includes whether data was printed from another party*

[32] HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls

4.2 Auditing Access Where Individual Consent or Authorization is Required

An authorization policy must be in place for any exchange of PHI, and requires the audit log to identify whether the release requires an authorization and, if so, whether the authorization was obtained.

A consent ID would be required, if it exists, for transactions that require a consent or authorization to be tracked for audit purposes. *AUD 2*

Section 5 - Need-to-Know Procedure/ Process for Personnel Access to PHI

5.1 Information Request

For purposes of information requests, a written policy is required that includes the following components:

- The date and time of the request,
- The reason for the request,
- A description of information requested, including the data accessed, data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to, or printed by another party,
- The ID of person/system requesting disclosure,
- The ID/verification of the party receiving the information,
- The ID of the party disclosing the information,
- The method used for verification of the requesting entity's identity.

An authorization policy must be in place for any exchange of PHI and requires the audit log to identify whether the release requires an authorization and if so, whether the authorization was obtained.

A consent ID is required, if it exists, for transactions that requires a consent or authorization to be tracked for audit purposes. *AUD 1*

5.2 Audit Log Process

The HIO's audit log procedure shall be developed and documented prior to any HIE exchange and shall include identifying who is responsible for reconstitution and sharing audit log information. This includes identifying who is authorized to request the audit log. Also, the procedure shall identify is the audit log information is available to individuals and how that request is handled. *POL 9*

5.3 Data Authentication

If a document is shared with a patient, methods for assurance shall be established and shall indicate that data have-not been modified. *POL 10*

5.4 Preparing a Query Message

When an HIO generates a registry stored query, registry or Record Locator Service (RLS) will be asked if there are records for this patient [Refer to HITSP IS01]. *SYS 1*

SYS 1 Requirement also considered:

The ability of the HIO to generate an HL7 message

Section 6 - System Capabilities

6.1 Audit Controls[33]

Audit logs are required to record activity specified by the HIO and the HIO shall periodically review the generated audit logs. This review of the audit logs is based on established audit criteria and shall include documentation of any anomalies. The HIO will document its mitigating action (including sanctions, security incident response team activation, etc. as appropriate). Audit logs must include at least the following: unique user name/ID, date/time stamp, and all actions taken (add, change, delete). Audit logs should either be in readable form or translatable by some easy to use tool to be in readable form, and they need to be examined with some frequency appropriate to the HIE in order to detect improper use. *POL 18*

6.2 Audit Log Content

The HIO's audit logs shall include:

- User ID,
- A date/time stamp,
- Identification of all data transmitted, and
- Any authorizations needed in order to disclose the data. *SYS 3*

The audit log shall include any system activity of use and disclosure of data, and shall retain a record of information systems activity that occurs at established periodic time frames. The audit log for the use and disclosure of data is also required to have a set report in place. Actions that have been identified in the event of discovered anomalies/breaches shall be included in the audit log. Also, login auditing is required as noted under the HIPAA security rule auditing standard. If it exists, any state-specific[34] consent policy under which the data were disclosed shall be tracked. This may be a global consent policy or a specific consent for each access. If sensitivity restricted information exists, the HIO may choose to implement restrictions as permitted under their state. *SYS 2*

SYS 3 Requirements also considered:

Ability to share responsibilities for identifying what has been transmitted, which entities are responsible for tracking on specifics, and whether data can be transmitted to another party

6.3 Information Integrity

Information integrity is audited by logging that no change has occurred since the signature was applied and shall include a valid date/time stamp. *SYS 12*

6.4 Data Authentication

For purposes of data authentication the use of a valid date/time stamp is required. *AUT 4*

[33] **HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls**

[34] For example, the consent policy of the State of Massachusetts.

AUT 4 Requirement also considered, but is difficult to implement:

Signature Purpose (ASTM E1762)

6.5 Data Validation

For the purposes of data validation, the signer credentials must be from a trusted authority, and the credential must be current and without constraints, and the credential must be of the appropriate type for the requested data (for example physician or pharmacist). To ensure data integrity, credentials shall indicate that no change has occurred since the signature was applied and must have a valid date/time stamp. *AUT 7*

Requirements Out of Scope

1.0 Electronic Signature *SYS 10*

SYS 10 Requirement also considered:

Ability for electronic signature (distinct from a digital signature)

2.0 Interim Reports *POL 1*

POL 1 Requirement also considered:

Interim reports made available for sharing once the ordering physician has signed off on the results, and has been discussed with patient where this is required by policy. There was a difference in state perspective (ie border states) about withholding information from a patient

3.0 Returning More Demographics *POL 8*

POL 8 Requirement Also Considered:

The identification of risk issues– e.g. Data authentication not a high risk in this scenario

4.0 Risk Assessment *POL 13*

POL 13 Requirement also considered:

The returning of more demographic information to the end user than was entered

5.0 Signature / Data Validation Checking *POL 14*

POL 14 Requirements also considered:

Signature and Data Integrity conducted prior to allowing the following procedures:
Using data communicated through secured methods (e.g. VPN);
Using data communicated through insecure methods (e.g. patient USB);
Storing data;
Submitting data to shared resource

References

Connecting for Health Common Framework (from the Markle Foundation) - See http://www.connectingforhealth.org/

M2 – A Model Contract for Health Information Exchange
P2 – Model Privacy Policies and Procedures for Health Information Exchange
P5 – Authentication of System Users
P7 – Auditing Access to and use of a Health Information Exchange

Appendix C: Other Useful Resources

- **American Health Information Community (AHIC)**
- **American Health Information Management Association (AHIMA)**
- **Connecting for Health**
- **eHealth Initiative (eHI)**
- **Healthcare Information Management Systems Society (HIMSS)**
- **Healthcare Information Technology Standards Panel (HITSP)**
- **Integrating the Healthcare Enterprise (IHE)**
- **North Carolina Healthcare Information and Communications Alliance, Inc (NCHICA)**

American Health Information Community (AHIC)
www.hhs.gov/healthit/ahic

The American Health Information Community (AHIC) was formed to help advance efforts to reach President Bush's call for most Americans to have electronic health records within ten years. The Community is a federally-chartered advisory committee and provides input and recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way.

AHIC has developed a set of use cases outlining events and actions for different types of access to the health information exchange. The use case documents are available for download at the AHIC website.

The following use cases were utilized in developing the ASC standard policies:

- Laboratory Reporting
- Medication Management

American Health Information Management Association (AHIMA)
www.ahima.org

The American Health Information Management Association (AHIMA) is the premier association of health information management (HIM) professionals. AHIMA is committed to advancing the Health Information Management profession in an increasingly electronic and global environment through leadership in advocacy, education, certification and lifelong learning.

The Foundation of Research and Education (FORE) of AHIMA under contract to ONC has developed many practice and policy guidance documents for state-level HIE initiatives in the areas of governance, structure, operations, financing and HIE polices. The documents, as well as a tool kit, are available on the AHIMA website.

Connecting for Health
www.connectingforheatlh.org

Connecting for Health **is** a public-private collaborative with representatives from more than 100 organizations across the spectrum of healthcare stakeholders. Its purpose is to catalyze the widespread changes necessary to realize the full benefits of health information technology (HIT), while protecting patient privacy and the security of personal health information. **Connecting for Health** is continuing to tackle the key challenges to creating a networked health information environment that enables secure and private information sharing when and where it's needed to improve health and healthcare.

The Common Framework helps health information networks to share information among their members and nationwide while protecting privacy and allowing for autonomy and innovation. It consists of 17 mutually-reinforcing technical documents and specifications, testing interfaces, code, privacy and security policies and model contract language. The documents are available for download at the Connecting for Health website.

The following framework documents were used in the development of the ASC standard policies:

- M1 – Key Topics in a Model Contract for Health Information Exchange
- M2 – A Model Contract for Health Information Review
- P5 – Authentication of System Users
- P7 – Auditing Access To and Use of a Health Information Exchange

Healthcare Information Management Systems Society (HIMSS)
www.himss.org

The Healthcare Information and Management Systems Society (HIMSS) is the healthcare industry's membership organization exclusively focused on providing global leadership for the optimal use of healthcare information technology and management systems for the betterment of healthcare.

HIMSS provides resources, relevant news and a toolkit to keep its membership and the community informed about the every-changing areas of RHIOs and HIEs. The resources are available on their website.

Health Information Technology Standards Panel (HITSP)
www.hitsp.org

The Healthcare Information Technology Standards Panel (HITSP) was founded in October 6, 2005 when awarded a contract award from the Office of the National Coordinator for Health and Information Technology (ONC) offered to advance President Bush's vision for widespread adoption of interoperable health records (EHR) within ten (10) years. The contracted targeted the creation of process to harmonize standards, certify EHR applications, develop nationwide health information network prototypes and recommend necessary changes to standardized diverse security and privacy policies.

The American National Standards Institute (ANSI), in cooperation with strategic partners HIMSS, Booz Allen Hamilton and Advanced Technology Institute, was selected to administer the standards harmonization initiative. The resulting collaboration became HITSP.

The Panel's work is driven by a series of priorities (Use Cases) issued by the American Health Information Community (AHIC). HITSP produces recommendations and reports in Interoperability Specifications and related Constructs that guide the standard implementation of each use case. The constructs consist of Interoperability Specifications, Transaction Packages, Transactions and Components. The recommendations, constructs and reports as well as a more in depth explanation of the harmonization process are available on the HITSP website.

The HITSP Specifications and documents applicable to the use cases of Lab Reporting and Medication Management were utilized by the ASPC to harmonize policies with the use cases.

Integrating the Healthcare Enterprise (IHE)
www.ihe.net

IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinates use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. The IHE Technical Framework documents are available on the IHE website.

North Carolina Healthcare Information and Communications Alliance, Inc (NCHICA)
www.nchica.org

The North Carolina Healthcare Information and Communication Alliance (NCHICA) is a nationally recognized nonprofit consortium that serves as an open, effective and neutral forum for health information technology initiatives that improve health and healthcare in North Carolina.

NCHICA's leadership in conducting demonstration projects, hosting educational sessions, and fostering collective efforts within North Carolina helps position the state as a vanguard of national HIT acceleration efforts. NCHICA has developed a *Toolkit for State-Level HIE* to assist other communities, regions and states develop a nonprofit similar to theirs. The Toolkit is located on the NCHICA website, under the "Health IT" tab.

eHealth Initiative (eHI)
www.ehealthinitiative.org

The eHealth Initiative and the Foundation for eHealth Initiative are independent, non-profit affiliated organizations whose missions are the same: to drive improvement in the quality, safety, and efficiency of healthcare though information technology. eHI focuses on the following topics to support its mission:

- Monitoring, assessing and reporting out changes in the policy environment
- Developing multi-stakeholder consensus
- Developing and disseminating tools and resources
- Providing “hands-on help”
- Launching learning laboratories
- Expanding its coalition

Information about the eHI Blueprint and the eHealth Initiative Toolkit are available on their website.

National Institute of Standards Technology (NIST) 800 series of publications
http://www.nist.gov/index.html

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Special Publications in the **800 series** present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. http://csrc.nist.gov/publications/PubsSPs.html

Appendix D: Glossary and Abbreviations

The following glossary includes the definition of key terms found in this Adoption Guide. A common understanding and use of these terms is critical in the consensus and adoption process.

This glossary represents an excerpt of terms included in a broader Glossary developed by the HISPC Adoption of Standard Policies Collaborative (ASPC) for the purposes of developing the Uniform Standard Policy. The full ASPC glossary can be found in the ASPC Final Report.

Term	Definition	Source of definition
4 As	Authorization, Authentication, Access and Audit	HIPAA
Access Control	Prevention of unauthorized use of information assets **(ISO 7498-2).** It is the policy rules and deployment mechanisms, which control access to information systems, and physical access to premises (OASIS XACML).	HITSP Glossary
Accountability	Property ensures that the actions of an entity may be traced to that entity.	[ISO 7498-2:1989]
AHIC	American Health Information Community.	Emergency Responder Use Case
AHIMA	The American Health Information Management Association	N/A
AHRQ	The Agency for Healthcare Research and Quality	N/A
Alliance	The State Alliance for E-Health	N/A
Assurance	In the context of NIST SP 800-63, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.	NIST 800-63-1
Audit Trail and Node Authentication (ATNA)	Establishes the characteristics of a Basic Secure Node: 1. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. 2. It defines basic auditing requirements for the node	[Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 16)]

Term	Definition	Source of definition
	3. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. 4. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. 5. This profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor specific requirements. The Radiology Audit Trail option in the IHE Radiology Technical Framework is an example of such an extension.	
Authentication	The process of establishing confidence in the identity of users or information systems.	NIST 800-63-1
Authorization	The granting of rights, which includes the granting of access based on access rights.	[ISO 7498-2:1989]
Availability	The property of being accessible and useable upon demand by an authorized entity.	[ISO 7498-2:1989]
Care	Relieving the suffering of individuals, families, communities, and populations by providing, protecting, promoting, and advocating the optimization of health and abilities.	Emergency Responder, Medication Management Use Case
CCHIT	Certification Commission for Healthcare Information Technology.	Medication Management
Claimant	A party whose identity is to be verified using an authentication protocol.	NIST 800-63-1
Clinicians	Healthcare providers with patient care responsibilities, including physicians, advanced practice nurses, physician assistants, nurses, and other credentialed personnel involved in treating patients.	Medication Management Use Case

Term	Definition	Source of definition
CMS	Centers for Medicare & Medicaid Services, a federal agency within the Department of Health and Human Services.	Medication Management Use Case
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	[ISO 7498-2:1989] 45 CFR § 164.304 Definitions
Consumers	Members of the public who may receive healthcare services. These individuals may include: caregivers, patient advocates, surrogates, family members, and other parties who may be acting for, or in support of, a patient in the activities of receiving healthcare.	Medication Management Use Case
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.	NIST 800-63-1
Credentialed Personnel	A degree, certificate or award which recognizes a course of study taken in a certain area, and acknowledges the skills, knowledge and competencies acquired. In the health field, personnel are usually required to register with the credentialing body or institution not only in their discipline, but also in the state, locality, and institution where they practice.	Emergency Responder Use Case
Demographics	Basic patient identifying information such as name, age, gender, and primary language spoken.	Emergency Responder Use Case
Department of Health and Human Services (HHS)	This is the federal agency responsible for human health, and has oversight over many other federal agencies such as FDA, the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), CMS, the Agency for Health Research and Quality (AHRQ), the Substance Abuse and Mental Health Services Administration (SAMHSA), and others.	Medication Management Use Case
Digital Identity	A digital representation of a set of claims by one party about itself or another digital subject	ASPC Negotiated Definition
Digital Signature	Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against	[ISO 7498-2:1989]

Term	Definition	Source of definition
	forgery, e.g. by the recipient.	
DRP/EMOP	Disaster Recovery Plan/Emergency Mode Operation Plan	N/A
eHI	The eHealth Initiative	N/A
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.	NIST 800-63-1
Electronic Health Record	An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization.	National Alliance For Health Information Technology
FDA	Food and Drug Administration; a federal agency within the Department of Health and Human Services responsible for the safety regulation of foods, dietary supplements, vaccines, drugs, medical devices, veterinary products, biological medical products, blood products, and cosmetics.	Immunization, Medication Management Use Case
Functional Roles	Functional roles reflect the essential business functions that need to be performed. Functional roles are defined by a set of standard healthcare tasks (e.g., Neurologist).	Neuman/ Strembeck
Health Information Exchange	The electronic movement of health-related information among organizations according to nationally recognized standards.	National Alliance For Health Information Technology
Health Information Organization	An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.	National Alliance For Health Information Technology
Health Record Banking	Entities/mechanisms for holding an individual's lifetime health records. This information may be personally controlled and may reside in various settings such as hospitals, doctor's offices, clinics, etc.	Immunization Use Case
Health Registry	A health registry is an organized system for the collection, storage, retrieval, analysis, and dissemination of information on individual persons who have either a	Emergency Responder Use

Term	Definition	Source of definition
	particular disease, a condition (e.g., a risk factor) that predisposes to the occurrence of a health-related event, or prior exposure to substances (or circumstances) known or suspected to cause adverse health effects.	Case
Healthcare Organization	Officially registered organization that has a main activity related to health care services or health promotion. *EXAMPLES:* Hospitals, Internet health care web site providers and health care research institutions. *NOTE 1:* The organization is recognized to be legally liable for its activities, but need not be registered for its specific role in health. *NOTE 2:* An internal part of an organization is called an organizational unit, as in X.501.	[ISO IS 17090]
HIMSS	The Healthcare Information and Management Systems Society is the healthcare industry's membership organization exclusively focused on providing global leadership for the optimal use of healthcare information technology and management systems for the betterment of healthcare.	The Healthcare Information and Management System Society
HISPC	Health Information Security and Privacy Collaboration	N/A
HITSP	The American National Standards Institute (ANSI) Healthcare Information Technology Standards Panel; a body created in 2005 in an effort to promote interoperability and harmonization of healthcare information technology through standards that would serve as a cooperative partnership between the public and private sectors.	Immunization, Medication Management Use Case
Identification	Performance of tests to enable a data processing system to recognize entities.	[ISO/IEC 2382-8:1998]
Identifier	Piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator.	[ENV 13608-1]
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.	NIST 800-63-1

Term	Definition	Source of definition
IHE	Integrating the Healthcare Enterprise is an initiative by healthcare professionals and industry to improve the way the computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care.	Integrating the Healthcare Enterprise
Integrity	Proof that the message content has not been altered, deliberately or accidentally, in any way during transmission.	Adapted from ISO 7498-2:1989
Medication	Medication includes any prescription medications, sample medications, herbal remedies, over-the-counter drugs, vaccines, and diagnostic and contrast agents used on or administered to persons to diagnose, treat, or prevent disease or other abnormal conditions. This also includes any product designated by the FDA as a drug with the exception of eternal nutrient solutions, oxygen, and other medical gases.	Medication Management Use Case
Medication Management	The system for how healthcare organizations handle medications. The medication management process includes ordering and prescribing, preparing and dispensing, administration, monitoring, medication selection and procurement (i.e., formulary considerations), and medication storage.	Medication Management Use Case
Minimum Policy Requirements	An agreed upon consensus set. They refer specifically to the policy requirements that the ASPC developed through extensive individual state review of current policy and the subsequent comparison and negotiation of these requirements across the 10 states in the collaborative. These minimum policies requirements become the framework across which the Uniform Security Policy was built.	Adoption of Standard Policies Collaborative
NCHICA	The North Carolina Health Information and Communications Alliance	N/A
Network	An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties	NIST 800-63-1

Term	Definition	Source of definition
	(Claimant, Verifier, CSP or Relying Party).	
NHIN	The Nationwide Health Information Network is being developed to provide a secure, nationwide interoperable health information infrastructure that will connect providers, consumers and others involved in supporting health and healthcare.	The U.S. Department of Health and Human Services
NIST	The National Institute of Standards and Technology is a non-regulatory agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.	The National Institute of Standards and Technology
Node Authentication	Node Authentication - Describes authenticating each computer system in a network that can host one or more databases. [Each node in a distributed database system can act as a client, a server, or both, depending on the situation.]	Oracle
ONC	Office of the National Coordinator for Health Information Technology; serves as the Secretary's principal advisor on the development, application, and use of health information technology in an effort to improve the quality, safety, and efficiency of the nation's health through the development of an interoperable harmonized health information infrastructure.	Emergency Responder, Medication Management, Immunization Use Case
Organization Roles	Organizational roles correspond to the hierarchical organization in a company in terms of internal structures.	Neumann/ Strembeck
Password	A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.	NIST 800-63-1
Patient/Consumer	Person who is the receiver of health related services and who is an actor in a health information system.	ASPC Negotiated Definition
Patients	Members of the public who receive healthcare services.	Immunization, Medication Management Use Case
Privacy	Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.	[ISO/IEC 2382-8:1998]

Term	Definition	Source of definition
Providers	The healthcare clinicians within healthcare delivery organizations with direct patient interaction in the delivery of care, including physicians, nurses, psychologists, and other clinicians. This can also refer to healthcare delivery organizations.	Immunization Use Case
Regional Health Information Organization	A health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community.	National Alliance For Health Information Technology
Registration	The process through which a party applies to become a Subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.	NIST 800-63-1
Role	A set of competences and/or performances that are associated with a task	[ISO TS21298]
RTI	RTI International	N/A
Security	Combination of availability, confidentiality, integrity, and accountability.	[ENV 13608-1]
SLHIE	The State Level Health Information Exchange	N/A
Shared Secret	A secret used in authentication that is known to the Claimant and the Verifier.	NIST 800-63-1
Structural Role	A structural role is a type of healthcare personnel warranting differing levels of access control. Also known as “basic role,” “organizational role,” or “role group.” For a listing of healthcare structural roles see ASTM E 1986-98 (e.g., Attending Physician)	ASTM E 1986-98
Subscriber	A party who receives a credential or token from a CSP.	NIST 800-63-1
Token	Something that the Claimant possesses and controls (typically a key or password) used to authenticate the Claimant’s identity.	NIST 800-63-1

Term	*Definition*	*Source of definition*
Trading Partners	Entities that exchange (submit or receive) data electronically with each other. Examples include any pairing of physicians, providers, billing services, clearinghouses, health plans or third-party administrators.	45 CFR 160.103 Trading Partner Agreements
Uniform Security Policy	Aggregated set of policies that the ASPC recommends organizations adopt as minimum policy to allow for interoperability with other organizations for health information exchange.	Adoption of Standard Policies Collaborative
Verifier	An entity that verifies the Claimant's identity by verifying the Claimant's possession of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.	NIST 800-63-1

Appendix E: References

AHIMA Home - American Health Information Management Association. (n.d.). Retrieved February 2009, from http://www.ahima.org

Connecting for Health. (n.d.). Retrieved February 26, 2009, from http://www.connectingforhealth.org

eHealth Initiative. (n.d.). Retrieved February 2009, from http://www.ehealthinitiative.org

HIMSS - RHIO. (n.d.). Retrieved February 2009, from http://www.himss.org/asp/topics_rhio.asp

HIMSS - RHIO. (n.d.). Retrieved February 2009, from http://www.himss.org/asp/topics_rhio.asp

Health Information Technology. (n.d.). Retrieved February 2009, from http://hhs.gov/healthit/ahic

Health Information Technology. (n.d.). Retrieved February 2009, from http://www.hhs.gov/healthit/privacy/statelevel.html

Healthcare Information Technology Standards - HITSP. (n.d.). Retrieved February 2009, from http://www.hitsp.org

IHE.net Home. (n.d.). Retrieved February 2009, from http://www.ihe.net

NCHICA Homepage. (n.d.). Retrieved February 2009, from http://www.nchica.org

National Institute of Standards and Technology. (n.d.). Retrieved February 2009, from http://www.nist.gov

National eHealth Collaborative (NeHC). (n.d.). Retrieved February 2009, from http://www.nationalehealth.org/

Rogers, E., & Rogers, E. M. (2003). *Diffusion of Innovations, 5th Edition*. New York City: Free Press.

The Privacy Rule. (n.d.). Retrieved February 2009, from http://hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

Welcome to NAHIT. (n.d.). Retrieved February 2009, from http://www.nahit.org

Appendix F: Contributors

Arizona

Kim Snyder
Project Director
Government Information Technology Agency, State of Arizona
Principal, Illumine IT Solutions

Emilie Sundie, MSCIS
Project Manager
Government Information Technology Agency, State of Arizona
Principal, The Sundie Group

Kristen B. Rosati, JD
Coppersmith Gordon Schermer & Brockelman PLC

Colorado

Arthur Davidson, MD, MSPH
Director, Public Health Informatics and Preparedness
Denver Public Health Department
Associate Professor,
Department of Family Medicine, School of Medicine
Department of Community Medicine, Colorado School of Public Health
University of Colorado at Denver

Connecticut

John T. Lynch, MPH
Executive Director
Connecticut Center for Primary Care

Lori Reed-Fourquet, MSCS
Consultant, e-HealthSign LLC
Vice Convenor, TC215 Health informatics WG4 Security and Privacy
Co-Chair, ASTM E31.25 Healthcare Data Management, Security, Confidentiality, and Privacy

Michael J. Purcaro, MS, PT
Executive Director
The Public Health Foundation of Connecticut, Inc.

Maryland

David Sharp, MLA, PhD
Director, Center for Health Information Technology
Maryland Health Care Commission

Nebraska

David P. Lawton RN, PhD
Public Health Informatics Manager
Nebraska Department of Health and Human Services

Ann Fetrick, RN, PhD
University of Nebraska Medical Center
College of Public Health, Center for Biosecurity, Biopreparedness & Emerging Infectious Diseases

Anne Byers, EdM
Community Information Technology Manager
Nebraska Information Technology Commission

Ohio

Mary M. Crimmins, MA, CPEHR, CPHIT
Research Associate, Center for Healthy Communities
HISPC Liaison, HealthLink RHIO
Wright State University
Boonshoft School of Medicine

Philip Powers
Director of Technology
Health Policy Institute of Ohio

Oklahoma

Lynn Puckett
Contract Services Director
Oklahoma Health Care Authority

Ann F. Chou, PhD, MPH
Assistant Professor
College of Public Health & College of Medicine
University of Oklahoma

Utah

Francesca Lanier, MA
Project Director
Office of Public Health Informatics
Utah Department of Health

Virginia

Chris Doucette
Privacy Officer
Virginia Department of Medical Assistance

Kim Barnes
Policy Analyst/Medical Information
Virginia Department of Health

Reneé Kelley
Compliance & Security Analyst
Virginia Department of Medical Assistance

Washington

Jeffrey Hummel, MD, MPH
Medical Director for Clinical Informatics
Qualis Health
Associate Clinical Professor
Internal Medicine, University of Washington
Founder and Chief Medical Officer
Deep Domain, Inc.

Jordana Huchital, MS
Principal and Consultant
Interactive Outcomes

Technical Advisory Panel

Gary G. Christoph, Ph.D., CIPP, CHS, CISM
HHS Client Executive
Northrop Grumman Corporation

Chris Apgar, CISSP
President
Apgar & Associates, LLC

RTI International

David Harris, MPH
RTI International

Governor's Office of Health Information Exchange

Arizona Health Information Exchange (HIE)

Appendix E

Consumer Consent for Health Information Exchange: An Exploration of Options for Arizona's HIEs

Kristen Rosati
Coppersmith Gordon Schermer & Brockelman PLC

Introduction

The rise of Health Information Exchanges (HIEs)[1] across the country is an exciting development that promises to improve the quality of care, increase the efficiency of health care services by making health information available at the point of care for every patient, and empower consumers by making information about their care more available to them. Of course, the development of HIEs also poses real challenges in how to structure HIEs to ensure that consumer information is available to providers and consumers for those purposes, yet ensure rigorous health information confidentiality protections are in place.

This White Paper discusses one other fundamental policy challenge that every HIE must make in establishing its operations: whether and how to seek consumer consent to exchange a consumer's health information through the HIE. As this White Paper explores in detail, this is a difficult issue to resolve because different stakeholders in the health care community—consumers, health care providers, HIE administrators and others—often have different and sometimes strongly held beliefs about this issue. In addition, decisions about consumer consent will have an impact on the way an HIE's technology is structured, and some of those decisions may be too difficult or expensive to implement.

The consumer consent issue is a complicated policy decision that should be made only after a thorough consideration of all the issues involved, and by balancing the needs of the participants in the system. This White Paper presents a discussion on the options available to HIEs.

What issues will affect the decision on consumer consent to exchange health information through an HIE?

The policy decision of whether and when to seek consumers' consent to exchange health information through the HIE is a nuanced decision that depends on many interrelated factors:

- Do state laws or regulations require consumer consent to exchange health information? If so, in what circumstances?
- What type of information will be submitted through the HIE? Does any of the health information exchanged require additional protection, such as substance abuse treatment information?
- Who will access the exchange? For example, is access limited to health care providers or will health plans and others also have access?
- For what purposes is the HIE used? Will it be limited to treatment purposes, or are other uses of the health information contemplated?
- Can consumers trust that the HIE is secure?
- Is there accountability in the event someone inappropriately uses the exchange?

If the answer to any one of these questions changes, it may alter the policy decision about whether and how consumer consent would be sought. For example, if an HIE is used only by health care providers for treatment purposes, the decision on consumer consent may be different than if the HIE is used by health plans for payment purposes. It's three dimensional policy chess!

What do different stakeholders think about the consent issue?

It is important to keep in mind that a person's membership in a certain category of stakeholder does not dictate that person's ideas about consumer consent. So, this discussion will obviously contain generalizations that may not ring true to specific individuals.

Consumers: Not surprisingly, consumers appear to hold varied attitudes about whether they should have the ability to consent before their health information is exchanged via an HIE. Consumers who have chronic care needs, or who have children who have serious illnesses or

disabilities, often express tremendous support for HIE in order to facilitate communication between different parts of the care team and to avoid the need to be the coordinator for the information. These consumers are primarily concerned with the immediate availability of their health information to health care providers and may not support the need to get up-front consent if it will interfere with or slow down the transmission of their health information.

Other consumers are primarily concerned about their privacy, particularly if they have received care for conditions they feel would be stigmatizing or could lead to the denial of insurance coverage. For example, the organization Patient Privacy Rights is a strong advocate of the right to consent in advance of transmission of health information, even to providers for treatment purposes.

Both perspectives are completely legitimate, of course, and there are many individuals and organizations that fall somewhere between these perspectives. Ultimately, an individual's approach to consent depends on an individual's particular life circumstances and experiences.

Health care providers: Health care providers also have varied opinions on this subject. Many are, not surprisingly, primarily concerned with ensuring that they have complete information available about a patient at the time they provide care. In New Hampshire, for example, the legislature is considering a bill (HB 1587) that would allow patients to block provider access to information in electronic health records and in HIEs; hospitals, physicians, nursing homes and other providers have opposed the legislation because they believe it would compromise their ability to get complete information.

Other health care providers, particularly physicians who are involved in providing mental health care or treatment for other sensitive conditions, are extremely concerned that the lack of consumer consent to exchange health information will discourage some individuals from obtaining care at all.

HIE administrators: Individuals involved in creating and running HIEs are concerned with ensuring that the HIE is valuable to their communities. They want to provide a robust service to participating health care providers, and so must respond to the needs of those providers. They also are concerned about the cost of building and maintaining the HIE so that the HIE can be an ongoing service to the community.

Of course, health care providers and HIE administrators are also consumers of health care. Anyone involved in making a policy decision on the consent issue should keep that health care consumer "hat" firmly in place.

What does Arizona law require?

Arizona law does not require consumer consent to exchange health information for treatment purposes. Arizona law also generally does not require consumer consent for providers to exchange health information for a variety of other purposes, such as getting paid for the treatment they provide, for various business functions called "health care operations" (such as quality assurance activities), for public health purposes, and for research where an Institutional Review Board has reviewed the research and approved doing the research without consent (if there is sufficient privacy protection in place).

This analysis starts with the general medical records law for providers in Arizona,[2] which states that providers may follow the Health Insurance Portability and Accountability Act (HIPAA) regulations[3] in their disclosures of health information. HIPAA permits disclosures for treatment, payment, "health care operations" (general business activities, such as quality assurance), public health purposes, and research, without consumer consent or authorization.

We then look to determine whether any of the health information being exchanged is "special" health information that is subject to any greater restrictions. Arizona law has special statutes for genetic testing information,[4] mental health information held by licensed behavioral health providers,[5] and HIV and communicable disease information.[6] All of this information may be disclosed for treatment purposes without consumer consent. This information may also be disclosed for some public health purposes and research where an Institutional Review Board has reviewed the research and approved a waiver of consent. And except for genetic testing information, health care providers may also exchange this health information for payment and "health care operations" without advance consent.

For health care providers that are federally-assisted substance abuse treatment programs, however, the federal regulations on substance abuse treatment information set additional restrictions on the exchange of health information without consumer consent, even for treatment purposes. These restrictions are substantial, so any HIE should exclude information that comes from these providers.

In summary, Arizona law does not require advance consumer consent to exchange information through an HIE for most purposes. It is therefore a *policy* decision on whether consumer consent will be required to exchange health information through an HIE, and for what purpose. A complete explanation of these Arizona and federal laws is included in the Arizona Health-e Connection Briefing Paper at pages 25-29 and 44-53, which can be found on the Arizona Health-e Connection website (www.azhec.org) in the "About AzHeC" section.

What are the options for Arizona HIEs?
Generally, there are four options for HIEs to consider in making the decision about whether and how consumers consent to the electronic exchange of health information:

- **Option 1- Opt In**
  Seek advance consent from consumers to include their health information in an HIE;
- **Option 2- Opt Out**
  Provide consumers the right to "opt out" of having their health information in an HIE;
- **Option 3- Notice Only**
  Include all consumers' health information in an HIE, with notice to or education of consumers about the process; or
- **Option 4- Combination**
  Take a blended approach, employing Options 1-3 as appropriate, depending on the particular uses of information and who has access to the HIE.

HIEs are coming to very different decisions on this issue and are fairly evenly split across the country. Whichever approach is chosen, it should be transparent to consumers through extensive public education!

Option 1: Opt In
Seek advance consent from consumers to include their health information in an HIE. What are the advantages and disadvantages, and how would it work?

Advantages:
Consumer control: Consumers have a very legitimate interest in controlling their health information. Ideally, each consumer would have the right to determine who could see his or her health information and determine the purpose for which that health information is used.

Risk management for the HIE: From the HIE perspective, seeking advance consent could serve a risk management function. The consent form would educate individuals about how health information is exchanged, who will have access to it, and what consumer rights are vis-à-vis the HIE and the participants in the HIE. This proactive education through the consent process could

reduce liability to an HIE in the event a participant misuses the exchange.

Enabling better patient record matching: If the process of seeking advance consent is done through an in-person process, that consent process could eventually support the collection of biometric identifiers, such as fingerprints. These biometric identifiers would permit accurate patient record matching by the HIE—two individuals may have the same names (and sometimes even same birthdates), but they don't have the same fingerprints. At this time, biometric identifiers are not commonly used. Patient access to their own information in an HIE could also assist in increasing the accuracy of records in the system.

Disadvantages:

Delay in getting information to providers for treatment: The primary disadvantage of the opt-in process is that the need to obtain advance consent from a consumer to exchange health information could delay the transmission of that information to providers. Consumers may not have the opportunity to consent before their information is needed, particularly in an emergency.

Less support from physicians: Another substantial disadvantage of the opt-in process is that seeking advance consent to include health information in the exchange may not garner support by physicians and other health care providers for two reasons. First, physicians consistently report that if an exchange does not have complete information on their patients, physicians will not view the exchange as reliable. For liability purposes, physicians want as complete information as possible and may not rely on a source of information from which their patients could withhold information. Second, physicians may not be willing to work an HIE into their office workflow if the information is not complete. In Massachusetts, for example, the Massachusetts Health Data Consortium reportedly discontinued its MedsInfo-ED project because the project could not collect certain medication information without advance patient consent. When physicians consistently found the project did not contain medication information about the patient presenting for care, the physicians stopped using the MedsInfo-ED database.

Granularity of consent: Next, the "granularity" of consent is problematic. Will the HIE seek all-or-nothing consent? In other words, will consumers be forced to make a decision between including all of their information in the exchange or none of it? Or will they be able to consent to the sharing of specific pieces of information? How will this process work?

Expense and administrative burden. The final disadvantage is that an opt-in process would be expensive to support, and may create unwelcome bureaucracy for consumers. In administering a consent process, the following operational issues may be challenging to implement:

- Who will seek the consent? Health care providers may be tasked with seeking consent from their patients, as providers' face-to-face interactions with patients will facilitate the consent process and give them the chance to explain how the HIE works. However, some providers may object to the time that would be required to explain HIE participation to their patients, to fill out the necessary paperwork, and to transmit that paperwork to the appropriate entities.

- Will one consent be sufficient for a consumer to participate in the system as a whole, or will it be necessary for each provider to seek consent from that provider's patients? If the latter, how will this work?

- How will a consumer's consent to participate be communicated to the HIE? To other providers?

- What will the process be for revoking consent? How will revocation affect

information already in the HIE? How will revocation be communicated to others?

Option 2: Opt Out

Provide consumers the right to "opt out" of having their health information in an HIE. What are its advantages and disadvantages, and how would it work?

Advantages:

Consumer control. As discussed above, consumers have a very legitimate interest in controlling who sees their health information and to determine the purpose for which that health information is used. Under an opt-out system, consumers would be required to contact an HIE (or their health care providers) to be removed from the system, but that still would provide a level of control to consumers.

As the National Committee on Vital and Health Statistics noted in a February 2008 report, "where individuals have the right to put restrictions on disclosure of sensitive health information, people rarely elect to do so, but they strongly value having the right and ability to do so."[7] The Indiana Network for Patient Care (INPC), administered by the Regenstrief Institute and one of the longest operating HIEs in the country, had an opt-out system for many years; a representative of the INPC reported that very few individuals opted out of its system.

Disadvantages:

Granularity of opt-out: As with the "opt-in" option, the "granularity" of the opt-out is problematic. Will the HIE require an all-or-nothing opt-out? Will it be specific to the type of use? To the type of information? To who will access the information? The HIE architecture will have a substantial affect on the consent management options.

Expense and administrative burden: The final disadvantage is that an opt-out process may be administratively difficult to support. In administering the opt-out process, the following operational issues may be challenging:

- Who will collect consumer opt-outs? If health care providers are tasked with collecting opt-outs for their patients, they may object to the time that may be required to explain participation to their patients, to fill out the necessary paperwork, and to transmit that paperwork to the appropriate entities.

- If opt-outs are collected at the provider level, will the opt-out be effective only for that provider? Or will the opt-out apply to the entire system and be effective with regard to all providers' information?

- How will a consumer's opt-out be communicated to the HIE? To other providers?

- What will the process be for a consumer to change his or her decision and later participate in the system?

- How will subsequent opt-outs be handled? Will a later opt-out affect information already in the HIE? How will the opt-out be communicated to others?

Option 3: Notice Only

Include all consumers' health information in an HIE, with notice to or education of consumers. What are its advantages and disadvantages, and how would it work?

Advantage:

More flexibility for coordination with other HIEs and response to developing technology. Because multiple HIEs are developing in Arizona, it is important to ensure consistency among HIE policies to permit them to exchange health information with each other. The "early on the scene" HIEs may decide to adopt option 3 to facilitate coordination with other HIE policies. (If an early HIE chooses to implement an opt-in or opt-out process, it may be more difficult them to roll out an alternative policy later.) Moreover, HIE consent management technology is evolving, which hopefully will allow in the

future more granular control by consumers to sequester certain types of sensitive health information.

Results in most useful HIE: An HIE that includes all available patient information—subject to stringent privacy and security protections—is the most valuable for health care providers. When health care providers know they can rely on an HIE to provide complete information on their patients, health care providers will trust the HIE as a source of valuable information and will integrate access to the HIE into their workflows. An exchange that contains complete patient information also will be extremely valuable for public health purposes (such as bioterrorism surveillance across multiple records) and research, if those uses are approved by HIE policy decision makers.

Easy to administer: Because option 3 does not have an opt-in or opt-out process to implement, the HIE will be easier to administer. Particularly while HIEs are struggling with methods to finance the delivery of this important service, that is a significant consideration.

Of course, providing notice to consumers does entail some costs and implementation questions such as:

- How will notice be provided to consumers? Will it be provided by the HIE to the public at large? Will providers participating in the HIE be required to provide notice to their patients?

- If notice is provided by health care providers, will the HIE develop common content for all providers to use?

- How will notice be coordinated with other HIEs, particularly to support exchange between HIEs?

These costs are substantially less than in Options 1 or 2.

***Disadvantages*:**
Less consumer control: As discussed above, consumers have a legitimate concern with deciding who may see their health information and for what purpose. While e-health exchange will essentially function as an electronic version of the types of exchanges that happen in health care in paper form today, it is possible that some consumers will be more concerned now that the exchanges will occur electronically. Consumers with sensitive conditions may decide not to provide complete information when receiving care in order to keep that sensitive information out of the HIE.

Option 4: Combination
Take a blended approach, employing Options 1-3 as appropriate. What are its advantages and disadvantages, and how would it work?

Some HIEs are discussing taking a "blended" approach—including all available information in the exchange, but providing different levels of consumer control based on the use of the information. For example, an HIE may permit access by providers to information for treatment purposes without advance consumer consent, but implement an opt-in or opt-out process for other uses of information, such as for research.

Once the technology is available, an HIE could also implement a varied approach to different types of health information and for particular individuals. For example, the HIE could implement a policy of requiring affirmative opt-in for a particular provider to see substance abuse treatment information (which now would be excluded from the HIE). As consent management tools and HIE technology advance, more granularity will be possible.

Conclusion
HIEs across the country are struggling with the issue how to implement consumer consent for e-health information exchange,

because it is a complicated and many-faceted issue.

The federal government is also considering what type of consent is appropriate for the National Health Information Network (NHIN)—the effort to connect HIEs across the country. The National Committee on Vital and Health Statistics (NCVHS), a federal advisory body that advises the Department of Health and Human Services (HHS) on health data, statistics and national health information policy, issued a report on February 20, 2008, in which the NCVHS recommended that the Secretary of HHS implement a policy for the NHIN to allow individuals to "have limited control, in a uniform manner, over the disclosure of certain sensitive health information for purposes of treatment."[8] NCVHS expressed concern about "protecting patients' legitimate concerns about privacy and confidentiality, fostering trust and encouraging participation in the NHIN in order to promote opportunities to improve patient care, and protecting the integrity of the health care system." NCVHS thus recommended the development—through an open public process—to uniformly decide across the country which categories of health information (such as information related to domestic violence, genetic information, mental health information, reproductive health, and substance abuse) an individual would be permitted to sequester from access in the NHIN without express consent for a particular provider or in an emergency.

At the same time, the NCVHS recognized "that the technologies and human factors needed to implement the recommendations in this letter are not necessary readily available for the EHR systems, HIEs, and other components of the emerging NHIN." This is a situation where HIE architecture and available technology may have to catch up with desired policy outcomes.

Moreover, Arizona has the challenge of coordinating the policy decisions on consent across the state as multiple HIE networks develop throughout the state. How will the consent process be coordinated across HIEs? For example, if one HIE implements the opt-in consent option, but another implements the notice-only option, how will these HIEs be able to exchange patient information? Arizona must carefully avoid the creation of information silos, because that will not benefit consumers.

Clearly, as we move forward in developing HIEs across Arizona, we need to initiate an open and transparent dialog—involving a wide range of interested stakeholders—about consumer consent for exchange of health information. A good policy outcome will balance the needs of consumers, health care providers and HIEs, taking into account our state laws, consumer concerns about privacy and security of health information, and technological capabilities for HIE architecture. With this open and transparent dialog, we will make electronic health information exchange a reality in Arizona.

---

[1] A word about terminology in this White Paper: the term "Health Information Exchange," like "Regional Health Information Organization," refers to the entity that is facilitating or conducting the exchange of health information.
[2] A.R.S. § 12-2291, *et seq.*
[3] 45 C.F.R. Part 160 and Part 164, Subpart E (the HIPAA Privacy Rule).
[4] A.R.S. § 12-2801, *et seq.* and § 20-448.02, *et seq.*
[5] A.R.S. § 36-501, *et seq.*
[6] A.R.S. § 36-661, *et seq.* and § 20.448.01.
[7] http://www.ncvhs.hhs.gov/080220lt.pdf.
[8] Id.

Arizona Health Information Exchange (HIE)

Appendix F

REFERENCE TITLE: medical records; disclosure; release

State of Arizona
Senate
Forty-ninth Legislature
Second Regular Session
2010

SB 1258

Introduced by
Senators Leff, Aguirre; Representative Barto: Senator Allen C;
Representatives Court, Meyer, Tobin

AN ACT

AMENDING SECTIONS 12-2291, 12-2294, 12-2296, 13-2316, 36-135, 36-470, 36-509, 36-664 AND 36-3295, ARIZONA REVISED STATUTES; RELATING TO MEDICAL RECORDS.

(TEXT OF BILL BEGINS ON NEXT PAGE)

Be it enacted by the Legislature of the State of Arizona:

Section 1. Section 12-2291, Arizona Revised Statutes, is amended to read:

12-2291. Definitions

In this article, unless the context otherwise requires:

1. "CLINICAL LABORATORY" HAS THE SAME MEANING PRESCRIBED IN SECTION 36-451.

~~1.~~ 2. "Contractor" means an agency or service that duplicates medical records on behalf of health care providers.

~~2.~~ 3. "Department" means the department of health services.

~~3.~~ 4. "Health care decision maker" means an individual who is authorized to make health care treatment decisions for the patient, including a parent of a minor or an individual who is authorized pursuant to section 8-514.05, title 14, chapter 5, article 2 or 3 or section 36-3221, 36-3231 or 36-3281.

~~4.~~ 5. "Health care provider" means:

(a) A person who is licensed pursuant to title 32 OR 36 and who maintains medical records.

(b) A health care institution as defined in section 36-401.

(c) An ambulance service as defined in section 36-2201.

(d) A health care services organization licensed pursuant to title 20, chapter 4, article 9.

~~5.~~ 6. "Medical records" means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers. Medical records do not include materials that are prepared in connection with utilization review, peer review or quality assurance activities, including records that a health care provider prepares pursuant to section 36-441, 36-445, 36-2402 or 36-2917. Medical records do not include recorded telephone and radio calls to and from a publicly operated emergency dispatch office relating to requests for emergency services or reports of suspected criminal activity, but shall include communications that are recorded in any form or medium between emergency medical personnel and medical personnel concerning the diagnosis or treatment of a person.

~~6.~~ 7. "Payment records" means all communications related to payment for a patient's health care that contain individually identifiable information.

~~7.~~ 8. "Source data" means information that is summarized, interpreted or reported in the medical record, including x-rays and other diagnostic images.

Sec. 2. Section 12-2294, Arizona Revised Statutes, is amended to read:

12-2294. Release of medical records and payment records to third parties

A. A health care provider shall disclose medical records or payment records, or the information contained in medical records or payment records, without the patient's written authorization as otherwise required by law or when ordered by a court or tribunal of competent jurisdiction.

B. A health care provider may disclose medical records or payment records, or the information contained in medical records or payment records, pursuant to written authorization signed by the patient or the patient's health care decision maker.

C. A health care provider may disclose medical records or payment records or the information contained in medical records or payment records AND A CLINICAL LABORATORY MAY DISCLOSE CLINICAL LABORATORY RESULTS without the written authorization of the patient or the patient's health care decision maker as otherwise authorized by state or federal law, including the health insurance portability and accountability act privacy standards (45 Code of Federal Regulations part 160 and part 164, subpart E), or as follows:

1. To health care providers who are currently providing health care to the patient for the purpose of diagnosis or treatment of the patient.

2. To health care providers who have previously provided treatment to the patient, to the extent that the records pertain to the provided treatment.

3. To ambulance attendants as defined in section 36-2201 for the purpose of providing care to or transferring the patient whose records are requested.

4. To a private agency that accredits health care providers and with whom the health care provider has an agreement requiring the agency to protect the confidentiality of patient information.

5. To a health profession regulatory board as defined in section 32-3201.

6. To health care providers for the purpose of conducting utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917.

7. To a person or entity that provides ~~billing, claims management, medical data processing, utilization review or other administrative~~ services to the patient's health care providers OR CLINICAL LABORATORIES and with whom the health care provider OR CLINICAL LABORATORY has an agreement requiring the person or entity to protect the confidentiality of patient information AND AS REQUIRED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 164, SUBPART E).

8. To the legal representative of a health care provider in possession of the medical records or payment records for the purpose of securing legal advice.

9. To the patient's third party payor or the payor's contractor.

10. To the industrial commission of Arizona or parties to an industrial commission claim pursuant to title 23, chapter 6.

D. A health care provider may disclose a deceased patient's medical records or payment records or the information contained in medical records or payment records to the patient's health care decision maker at the time of the patient's death. A health care provider also may disclose a deceased patient's medical records or payment records or the information contained in medical records or payment records to the personal representative or administrator of the estate of a deceased patient, or if a personal representative or administrator has not been appointed, to the following persons in the following order of priority, unless the deceased patient during the deceased patient's lifetime or a person in a higher order of priority has notified the health care provider in writing that the deceased patient opposed the release of the medical records or payment records:

1. The deceased patient's spouse, unless the patient and the patient's spouse were legally separated at the time of the patient's death.

2. The acting trustee of a trust created by the deceased patient either alone or with the deceased patient's spouse if the trust was a revocable inter vivos trust during the deceased patient's lifetime and the deceased patient was a beneficiary of the trust during the deceased patient's lifetime.

3. An adult child of the deceased patient.

4. A parent of the deceased patient.

5. An adult brother or sister of the deceased patient.

6. A guardian or conservator of the deceased patient at the time of the patient's death.

E. A person who receives medical records or payment records pursuant to this section shall not disclose those records without the written authorization of the patient or the patient's health care decision maker, unless otherwise authorized by law.

F. If a health care provider releases a patient's medical records or payment records to a contractor for the purpose of duplicating or disclosing the records on behalf of the health care provider, the contractor shall not disclose any part or all of a patient's medical records or payment records in its custody except as provided in this article. After duplicating or disclosing a patient's medical records or payment records on behalf of a health care provider, a contractor must return the records to the health care provider who released the medical records or payment records to the contractor.

Sec. 3. Section 12-2296, Arizona Revised Statutes, is amended to read:

12-2296. Immunity

A health care provider, ~~or~~ contractor OR CLINICAL LABORATORY that acts in good faith under this article is not liable for damages in any civil action for the disclosure of medical records or payment records or information contained in medical records, ~~or~~ payment records OR CLINICAL LABORATORY RESULTS that is made pursuant to this article or as otherwise

provided by law. The health care provider, ~~or~~ contractor OR CLINICAL LABORATORY is presumed to have acted in good faith. The presumption may be rebutted by clear and convincing evidence.

Sec. 4. Section 13-2316, Arizona Revised Statutes, is amended to read:

13-2316. Computer tampering; venue; forfeiture; classification

A. A person who acts without authority or who exceeds authorization of use commits computer tampering by:

1. Accessing, altering, damaging or destroying any computer, computer system or network, or any part of a computer, computer system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or to control property or services by means of false or fraudulent pretenses, representations or promises.

2. Knowingly altering, damaging, deleting or destroying computer programs or data.

3. Knowingly introducing a computer contaminant into any computer, computer system or network.

4. Recklessly disrupting or causing the disruption of computer, computer system or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system or network.

5. Recklessly using a computer, computer system or network to engage in a scheme or course of conduct that is directed at another person and that seriously alarms, torments, threatens or terrorizes the person. For the purposes of this paragraph, the conduct must both:

(a) Cause a reasonable person to suffer substantial emotional distress.

(b) Serve no legitimate purpose.

6. Preventing a computer user from exiting a site, computer system or network-connected location in order to compel the user's computer to continue communicating with, connecting to or displaying the content of the service, site or system.

7. Knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by this state, a political subdivision of this state, ~~or a medical institution~~ A HEALTH CARE PROVIDER AS DEFINED IN SECTION 12-2291, A CLINICAL LABORATORY AS DEFINED IN SECTION 36-451 OR A PERSON OR ENTITY THAT PROVIDES SERVICES ON BEHALF OF A HEALTH CARE PROVIDER OR A CLINICAL LABORATORY.

8. Knowingly accessing any computer, computer system or network or any computer software, program or data that is contained in a computer, computer system or network.

B. In addition to section 13-109, a prosecution for a violation of this section may be tried in any of the following counties:

1. The county in which the victimized computer, computer system or network is located.

2. The county in which the computer, computer system or network that was used in the commission of the offense is located or in which any books, records, documents, property, financial instruments, computer software, data, access devices or instruments of the offense were used.

3. The county in which any authorized user was denied service or in which an authorized user's service was interrupted.

4. The county in which critical infrastructure resources were tampered with or affected.

C. On conviction of a violation of this section, the court shall order that any computer system or instrument of communication that was owned or used exclusively by the defendant and that was used in the commission of the offense be forfeited and sold, destroyed or otherwise properly disposed.

D. A violation of subsection A, paragraph 6 OR 7 of this section constitutes an unlawful practice under section 44-1522 and is in addition to all other causes of action, remedies and penalties that are available to this state. The attorney general may investigate and take appropriate action pursuant to title 44, chapter 10, article 7.

E. Computer tampering pursuant to subsection A, paragraph 1 of this section is a class 3 felony. Computer tampering pursuant to subsection A, paragraph 2, 3 or 4 of this section is a class 4 felony, unless the computer, computer system or network tampered with is a critical infrastructure resource, in which case it is a class 2 felony. Computer tampering pursuant to subsection A, paragraph 5 of this section is a class 5 felony. Computer tampering pursuant to subsection A, paragraph ~~7 or~~ 8 of this section is a class 6 felony.

Sec. 5. Section 36-135, Arizona Revised Statutes, is amended to read:

36-135. Child immunization reporting system; requirements; access; confidentiality; immunity; violation; classification; definitions

A. The child immunization reporting system is established in the department to collect, store, analyze, release and report immunization data.

B. Beginning on January 1, 1998, a health care professional who is licensed under title 32 to provide immunizations, except as provided in subsection I OF THIS SECTION, shall report the following information:

1. The health care professional's name, business address and business telephone number.

2. The child's name, address, social security number if known and not confidential, gender, date of birth and mother's maiden name.

3. The type of vaccine administered and the date it is administered.

C. The health care professional may submit this information to the department on a weekly or monthly basis by telephone, facsimile, mail, computer or any other method prescribed by the department.

D. Except as provided in subsection I OF THIS SECTION, the department shall release identifying information only to the ~~person's health care professional,~~ PERSON, THE PERSON'S HEALTH CARE DECISION MAKER, parent or guardian, ~~health care services organization,~~ A HEALTH CARE PROVIDER, AN

ENTITY REGULATED UNDER TITLE 20, the Arizona health care cost containment system and its providers as defined in chapter 29 of this title, ~~or~~ a school official who is authorized by law to receive and record immunization records OR A PERSON OR ENTITY THAT PROVIDES SERVICES TO A HEALTH CARE PROVIDER AND WITH WHOM THE HEALTH CARE PROVIDER HAS A BUSINESS ASSOCIATE AGREEMENT THAT REQUIRES THE PERSON OR ENTITY TO PROTECT THE CONFIDENTIALITY OF THE INFORMATION, AS REQUIRED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 164, SUBPART E). THE DEPARTMENT MAY ALSO RELEASE IDENTIFYING INFORMATION TO AN ENTITY DESIGNATED BY THE PERSON OR THE PERSON'S HEALTH CARE DECISION MAKER, PARENT OR GUARDIAN. The department, by rule, may release immunization information to persons for a specified purpose. The department may release nonidentifying summary statistics.

E. Identifying information in the system is confidential. A person who is authorized to receive confidential information under subsection D OR PURSUANT TO RULES ADOPTED BY THE DEPARTMENT shall ~~not~~ disclose this information ~~to any other person~~ ONLY AS PERMITTED BY THIS SECTION OR RULES ADOPTED BY THE DEPARTMENT.

F. A health care ~~professional who~~ PROVIDER THAT provides information in good faith pursuant to this section is not subject to civil or criminal liability.

G. A health care ~~professional who~~ PROVIDER THAT does not comply with the requirements of this section violates a law applicable to the practice of medicine and commits an act of unprofessional conduct OR A VIOLATION OF CHAPTER 4 OF THIS TITLE.

H. Any agency or person receiving confidential information from the system who subsequently discloses that information to any other person OTHER THAN AS PERMITTED BY THIS SECTION is guilty of a class 3 misdemeanor.

I. At the request of the person, or if the person is a child the child's parent or guardian, the department of health services shall provide a form to be signed that allows confidential immunization information to be withheld from all persons including persons authorized to receive confidential information pursuant to subsection D OF THIS SECTION. If the request is delivered to the health care professional ~~prior to~~ BEFORE the immunization, the health care professional shall not forward the information required under subsection B OF THIS SECTION to the department.

J. FOR THE PURPOSES OF THIS SECTION, "HEALTH CARE DECISION MAKER" AND "HEALTH CARE PROVIDER" HAVE THE SAME MEANINGS PRESCRIBED IN SECTION 12-2291.

Sec. 6. Section 36-470, Arizona Revised Statutes, is amended to read:

36-470. Examination of specimens; written requests; reports of results; retention of test records

A. Except as otherwise provided, a clinical laboratory shall examine specimens at the authorization of any person licensed pursuant to title 32, chapter 7, 8, 13, 14, 17 or 29 or title 32, chapter 11, article 2, a person licensed to practice medicine or surgery in another state~~,~~ or a person authorized by law or department rules.

B. The result of a test shall be reported to the person who authorized it. A report of results issued from a clinical laboratory shall provide information required by the department by rule. No clinical interpretation, diagnosis or prognosis or suggested treatment other than normal values shall appear on the laboratory report form, except that a report made by a physician licensed to practice medicine and surgery in this state or another state may include this information.

C. THE RESULT OF A TEST MAY BE REPORTED TO A HEALTH CARE PROVIDER, AS DEFINED IN SECTION 12-2291, THAT HAS A TREATMENT RELATIONSHIP WITH A PATIENT, OR TO A PERSON OR ENTITY THAT PROVIDES SERVICES TO THE HEALTH CARE PROVIDER AND WITH WHOM THE HEALTH CARE PROVIDER HAS A BUSINESS ASSOCIATE AGREEMENT THAT REQUIRES THE PERSON OR ENTITY TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION AS REQUIRED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 164, SUBPART E).

~~C.~~ D. All specimens accepted by a laboratory for specified tests shall be tested on its premises, except that specimens, other than those for proficiency testing purposes, may be forwarded for examination to another laboratory licensed under this article or exempted by section 36-461, paragraph 1.

~~D.~~ E. When the laboratory performing the examination is other than the laboratory accepting the specimen, the report submitted shall include information required by the department by rule.

~~E.~~ F. Records involving laboratory services and copies of reports of laboratory tests shall be kept in a manner as prescribed by the department by rule.

~~F.~~ G. A person authorized to request clinical laboratory examinations pursuant to this section may direct that a clinical laboratory examine a person's specimens at that person's request if the authorization is given pursuant to department rules and specifies:

1. The name of the person authorized to request an examination and to receive the results of that examination.
2. The type of examinations to be performed by the laboratory.
3. The total number of examinations the authorized person may request.
4. The beginning and expiration dates of the authorization.
5. The identification of the person giving the authorization.

~~G.~~ H. The laboratory shall report test results ordered pursuant to subsection ~~F~~ G OF THIS SECTION to the person who authorized the test and to the person who requested it.

Sec. 7. Section 36-509, Arizona Revised Statutes, is amended to read:

36-509. Confidential records; civil immunity

A. A health care entity must keep records and information contained in records confidential and not as public records, except as provided in this section. Records and information contained in records may only be disclosed to:

1. Physicians and providers of health, mental health or social and welfare services involved in caring for, treating or rehabilitating the patient.

2. Individuals to whom the patient or the patient's health care decision maker has given authorization to have information disclosed.

3. Persons authorized by a court order.

4. Persons doing research only if the activity is conducted pursuant to applicable federal or state laws and regulations governing research.

5. The state department of corrections in cases in which prisoners confined to the state prison are patients in the state hospital on authorized transfers either by voluntary admission or by order of the court.

6. Governmental or law enforcement agencies if necessary to:

(a) Secure the return of a patient who is on unauthorized absence from any agency where the patient was undergoing evaluation and treatment.

(b) Report a crime on the premises.

(c) Avert a serious and imminent threat to an individual or the public.

7. Persons, including family members, actively participating in the patient's care, treatment or supervision. A health care provider may only release information relating to the patient's diagnosis, prognosis, need for hospitalization, anticipated length of stay, discharge plan, medication, medication side effects and short-term and long-term treatment goals. A health care provider may make this release only after the treating professional or that person's designee interviews the patient or the patient's health care decision maker and the patient or the patient's health care decision maker does not object, unless federal or state law permits the disclosure. If the patient does not have the opportunity to object to the disclosure because of incapacity or an emergency circumstance and the patient's health care decision maker is not available to object to the release, the health care provider in the exercise of professional judgment may determine if the disclosure is in the best interests of the patient and, if so, may release the information authorized pursuant to this paragraph. A decision to release or withhold information is subject to review pursuant to section 36-517.01. The health care provider must record the name of any person to whom any information is given under this paragraph.

8. A state agency that licenses health professionals pursuant to title 32, chapter 13, 15, 17, 19.1 or 33 and that requires these records in the course of investigating complaints of professional negligence, incompetence or lack of clinical judgment.

9. A state or federal agency that licenses health care providers.

10. A governmental agency or a competent professional, as defined in section 36-3701, in order to comply with chapter 37 of this title.

11. Human rights committees established pursuant to title 41, chapter 35. Any information released pursuant to this paragraph shall comply with the requirements of section 41-3804 and applicable federal law and shall be released without personally identifiable information unless the personally

identifiable information is required for the official purposes of the human rights committee. Case information received by a human rights committee shall be maintained as confidential. For the purposes of this paragraph, "personally identifiable information" includes a person's name, address, date of birth, social security number, tribal enrollment number, telephone or telefacsimile number, driver license number, places of employment, school identification number and military identification number or any other distinguishing characteristic that tends to identify a particular person.

12. A patient or the patient's health care decision maker pursuant to section 36-507.

13. The department of public safety by the court to comply with the requirements of section 36-540, subsection N.

14. A third party payor or the payor's contractor to obtain reimbursement for health care, mental health care or behavioral health care provided to the patient.

15. A private entity that accredits the health care provider and with whom the health care provider has an agreement requiring the agency to protect the confidentiality of patient information.

16. The legal representative of a health care entity in possession of the record for the purpose of securing legal advice.

17. A person or entity as otherwise required by state or federal law.

18. A person or entity as permitted by the federal regulations on alcohol and drug abuse treatment (42 Code of Federal Regulations part 2).

19. A person or entity to conduct utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917.

20. A person maintaining health statistics for public health purposes as authorized by law.

21. A grand jury as directed by subpoena.

22. A PERSON OR ENTITY THAT PROVIDES SERVICES TO THE PATIENT'S HEALTH CARE PROVIDER, AS DEFINED IN SECTION 12-2291, AND WITH WHOM THE HEALTH CARE PROVIDER HAS A BUSINESS ASSOCIATE AGREEMENT THAT REQUIRES THE PERSON OR ENTITY TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION, AS REQUIRED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 164, SUBPART E).

B. Information and records obtained in the course of evaluation, examination or treatment and submitted in any court proceeding pursuant to this chapter or title 14, chapter 5 are confidential and are not public records unless the hearing requirements of this chapter or title 14, chapter 5 require a different procedure. Information and records that are obtained pursuant to this section and submitted in a court proceeding pursuant to title 14, chapter 5 and that are not clearly identified by the parties as confidential and segregated from nonconfidential information and records are considered public records.

C. Notwithstanding subsections A and B of this section, the legal representative of a patient who is the subject of a proceeding conducted pursuant to this chapter and title 14, chapter 5 has access to the patient's

information and records in the possession of a health care entity or filed with the court.

D. A HEALTH CARE ENTITY THAT ACTS IN GOOD FAITH UNDER THIS ARTICLE IS NOT LIABLE FOR DAMAGES IN ANY CIVIL ACTION FOR THE DISCLOSURE OF RECORDS OR PAYMENT RECORDS THAT IS MADE PURSUANT TO THIS ARTICLE OR AS OTHERWISE PROVIDED BY LAW. THE HEALTH CARE ENTITY IS PRESUMED TO HAVE ACTED IN GOOD FAITH. THIS PRESUMPTION MAY BE REBUTTED BY CLEAR AND CONVINCING EVIDENCE.

Sec. 8. Section 36-664, Arizona Revised Statutes, is amended to read:

36-664. Confidentiality; exceptions

A. A person who obtains communicable disease related information in the course of providing a health service or obtains that information from a health care provider pursuant to an authorization shall not disclose or be compelled to disclose that information except to the following:

1. The protected person or, if the protected person lacks capacity to consent, the protected person's health care decision maker.

2. The department or a local health department for purposes of notifying a good Samaritan pursuant to subsection E of this section.

3. An agent or employee of a health facility or health care provider to provide health services to the protected person or the protected person's child or for billing or reimbursement for health services.

4. A health facility or health care provider, in relation to the procurement, processing, distributing or use of a human body or a human body part, including organs, tissues, eyes, bones, arteries, blood, semen, milk or other body fluids, for use in medical education, research or therapy or for transplantation to another person.

5. A health facility or health care provider, or an organization, committee or individual designated by the health facility or health care provider, that is engaged in the review of professional practices, including the review of the quality, utilization or necessity of medical care, or an accreditation or oversight review organization responsible for the review of professional practices at a health facility or by a health care provider.

6. A private entity that accredits the health facility or health care provider and with whom the health facility or health care provider has an agreement requiring the agency to protect the confidentiality of patient information.

7. A federal, state, county or local health officer if disclosure is mandated by federal or state law.

8. A federal, state or local government agency authorized by law to receive the information. The agency is authorized to redisclose the information only pursuant to this article or as otherwise permitted by law.

9. An authorized employee or agent of a federal, state or local government agency that supervises or monitors the health care provider or health facility or administers the program under which the health service is provided. An authorized employee or agent includes only an employee or agent who, in the ordinary course of business of the government agency, has access to records relating to the care or treatment of the protected person.

10. A person, health care provider or health facility to which disclosure is ordered by a court or administrative body pursuant to section 36-665.

11. The industrial commission or parties to an industrial commission claim pursuant to section 23-908, subsection D and section 23-1043.02.

12. Insurance entities pursuant to section 20-448.01 and third party payors or the payors' contractors.

13. Any person or entity as authorized by the patient or the patient's health care decision maker.

14. A person or entity as required by federal law.

15. The legal representative of the entity holding the information in order to secure legal advice.

16. A person or entity for research only if the research is conducted pursuant to applicable federal or state laws and regulations governing research.

17. A PERSON OR ENTITY THAT PROVIDES SERVICES TO THE PATIENT'S HEALTH CARE PROVIDER, AS DEFINED IN SECTION 12-2291, AND WITH WHOM THE HEALTH CARE PROVIDER HAS A BUSINESS ASSOCIATE AGREEMENT THAT REQUIRES THE PERSON OR ENTITY TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION, AS REQUIRED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 164, SUBPART E).

B. At the request of the department of economic security in conjunction with the placement of children in foster care or for adoption or court-ordered placement, a health care provider shall disclose communicable disease information, including HIV-related information, to the department of economic security.

C. A state, county or local health department or officer may disclose communicable disease related information if the disclosure is any of the following:

1. Specifically authorized or required by federal or state law.

2. Made pursuant to an authorization signed by the protected person or the protected person's health care decision maker.

3. Made to a contact of the protected person. The disclosure shall be made without identifying the protected person.

4. For the purposes of research as authorized by state and federal law.

D. The director may authorize the release of information that identifies the protected person to the national center for health statistics of the United States public health service for the purposes of conducting a search of the national death index.

E. The department or a local health department shall disclose communicable disease related information to a good Samaritan who submits a request to the department or the local health department. The request shall document the occurrence of the accident, fire or other life-threatening emergency and shall include information regarding the nature of the significant exposure risk. The department shall adopt rules that prescribe

standards of significant exposure risk based on the best available medical evidence. The department shall adopt rules that establish procedures for processing requests from good Samaritans pursuant to this subsection. The rules shall provide that the disclosure to the good Samaritan shall not reveal the protected person's name and shall be accompanied by a written statement that warns the good Samaritan that the confidentiality of the information is protected by state law.

F. An authorization to release communicable disease related information shall be signed by the protected person or, if the protected person lacks capacity to consent, the protected person's health care decision maker. An authorization shall be dated and shall specify to whom disclosure is authorized, the purpose for disclosure and the time period during which the release is effective. A general authorization for the release of medical or other information, including communicable disease related information, is not an authorization for the release of HIV-related information unless the authorization specifically indicates its purpose as an authorization for the release of confidential HIV-related information and complies with the requirements of this section.

G. A person to whom communicable disease related information is disclosed pursuant to this section shall not disclose the information to another person except as authorized by this section. This subsection does not apply to the protected person or a protected person's health care decision maker.

~~H. If a disclosure of communicable disease related information is made pursuant to an authorization under subsection F of this section, the disclosure shall be accompanied by a statement in writing that warns that the information is from confidential records protected by state law and that prohibits further disclosure of the information without the specific written authorization of the person to whom it pertains or as otherwise permitted by law.~~

~~I.~~ H. This section does not prohibit the listing of communicable disease related information, including acquired immune deficiency syndrome, HIV-related illness or HIV infection, in a certificate of death, autopsy report or other related document that is prepared pursuant to law to document the cause of death or that is prepared to release a body to a funeral director. This section does not modify a law or rule relating to access to death certificates, autopsy reports or other related documents.

~~J.~~ I. If a person in possession of HIV-related information reasonably believes that an identifiable third party is at risk of HIV infection, that person may report that risk to the department. The report shall be in writing and include the name and address of the identifiable third party and the name and address of the person making the report. The department shall contact the person at risk pursuant to rules adopted by the department. The department employee making the initial contact shall have expertise in counseling persons who have been exposed to or tested positive for HIV or acquired immune deficiency syndrome.

~~K.~~ J. Except as otherwise provided pursuant to this article or subject to an order or search warrant issued pursuant to section 36-665, a person who receives HIV-related information in the course of providing a health service or pursuant to a release of HIV-related information shall not disclose that information to another person or legal entity or be compelled by subpoena, order, search warrant or other judicial process to disclose that information to another person or legal entity.

~~L.~~ K. This section and sections 36-663, 36-666, 36-667 and 36-668 do not apply to persons or entities subject to regulation under title 20.

Sec. 9. Section 36-3295, Arizona Revised Statutes, is amended to read:

36-3295. Registry information; confidentiality; transfer of information

~~A. The registry established pursuant to this article is accessible only by entering the file number and password on the internet web site.~~

~~B.~~ A. Registrations, file numbers, passwords and any other information maintained by the secretary of state pursuant to this article are confidential and shall not be disclosed to any person other than the person who submitted the document or the person's ~~personal representative~~ HEALTH CARE DECISION MAKER AS DEFINED IN SECTION 12-2291 OR AS PERMITTED PURSUANT TO SUBSECTION B OF THIS SECTION.

~~C.~~ B. Notwithstanding subsection ~~B~~ A OF THIS SECTION, a health care provider OR A PERSON OR ENTITY THAT PROVIDES SERVICES TO THE PATIENT'S HEALTH CARE PROVIDER, AS DEFINED IN SECTION 12-2291, AND WITH WHOM THE HEALTH CARE PROVIDER HAS A BUSINESS ASSOCIATE AGREEMENT THAT REQUIRES THE PERSON OR ENTITY TO PROTECT THE CONFIDENTIALITY OF PATIENT INFORMATION, AS REQUIRED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT PRIVACY STANDARDS (45 CODE OF FEDERAL REGULATIONS PART 164, SUBPART E) may access the registry and receive a patient's health care directive documents for the provision of health care services ~~by submitting the patient's file number and password~~.

~~D.~~ C. The secretary of state shall use information contained in the registry only for purposes prescribed in this article.

~~E.~~ D. At the request of a person who submitted the document, the secretary of state may transmit the information received regarding the health care directive to the registry system of another jurisdiction as identified by the person.

Governor's Office of Health Information Exchange

Arizona Health Information Exchange (HIE)

Appendix G

A Timeline

Health Information Technology in Arizona

- *2001* – Crossing the Quality Chasm by the IOM published landmark recommendation advocating for HIT advancement.
- *November 2001* – NCVHS recommended creation of ONC.
- *April 2004* – HHS established the position of National Coordinator for HIT created by Executive Order 13335 of the Bush Administration.
- *September 2004* – SAHIE concept developed.
- *August 2005* – Gubernatorial executive order to develop a Roadmap for HIT in Arizona. Hundreds of stakeholders in public and private sector convened to develop the Roadmap.
- *January 2006* – SAHIE Phase I funding.
- *April 2006* – Arizona Health-e Connection Roadmap finalized.
- *March 2006* – GITA received $350,000 to participate in HISPC project Phase I outreach to address barriers in the healthcare community to HIE. Outreach to over 100 stakeholders in the medical community occurred to focus on and evaluate solutions to business practices that pose as barriers to HIE.
- *January 2007* – Arizona's RHITA grant program administered by GITA distributed $1.5 million in HIT grants to 33 communities, impacting 325 providers and 178,710 healthcare consumers.
- *January 2007* – AzHeC incorporated as an independent non-profit organization to spearhead state HIT efforts.
- *January 2007* – AHCCCS awarded Medicaid Transformation Grant of $11.7 million by CMS to develop and implement web-based electronic HIE for Medicaid providers – HIeHR Utility project began.
- *March 2007* – AzHeC hosted its 1st annual Arizona Health-e Connection Summit.
- *March 2007* – SAHIE became a formal project and developed Steering Committee.
- *July 2007* – AHCCCS issued contract to AzHeC for support of HIeHR Utility project.
- *July 2007* – GITA received additional $210,000 for HISPC project Phase II to work on legal and authentication issues for sharing EHRs.
- *September 2007* – Additional CMS grant of $4.4 million awarded to AHCCCS to build a clinical decision support toolbox in conjunction with the HIeHR Utility project.
- *January 2008 – Harvard Business Review* Case Study: Transforming Arizona's Health Care System: Developing and Implementing the Health-e Connection Roadmap published.
- *March 2008* – HHS released State Level Health Information Exchange, a report on the role of states in establishing HIT. Report recommended other states follow steps taken by Arizona.
- *April 2008* – Arizona received $414,700 HISPC Phase III contract through RTI International and ONC to work on Adoption of Standards Collaborative (ASC), a multi-state collaborative.
- *May 2008* – EAzRx statewide initiative established to foster adoption and utilization of e-prescribing; AzHeC received a $100,000 grant from UnitedHealthcare to partially fund initiative; gubernatorial executive order directed state agencies to work with AzHeC on EAzRx initiative.
- *May 2008* – AzHeC hosted 2nd annual Arizona Health-e Connection Summit.
- *July 2008* – Arizona's RHITA Program, administered by GITA, awarded $685,535 to rural institutions to lead or participate in HIE community planning with an additional $298,663 in HIE educational and consulting services.
- *August 2008* – Model HIE Participation Agreement and recommended security standards for HIT and HIE developed.
- *September 2008* – AMIE Proof of Concept launched as part of AHCCCS HIeHR Utility project.
- *October 2008* – AzHeC began collaborative process to draft legislative package to remove barriers to HIE.
- *December 2008* – AMIE Proof of Concept ended; project continued.
- *February 2009* – ARRA passed; HITECH Act a component of ARRA that created $30-40 billion in unprecedented investment in and opportunity for HIT nationwide.
- *March 2009* – AzHeC hosted 3rd annual Summit, name changed to Western States Health-e Connection Summit & Trade Show to reflect expanded scope of entire Western region.
- *March 2009* – SAHIE incorporated.
- *April 2009* – AzHeC conducted statewide consumer focus groups to learn about public perceptions around HIT.
- *May 2009* – SAHIE selected Wellogic as HIE vendor.
- *July 2009* – PACeHR incorporated and began operation.
- *September 2009* – CAPAZ-MEX, a Yuma-based HIE, began.
- *November 2009* – AMIE suspended technical operations.
- *January 2010* – SAHIE and AMIE Boards to consider merger.
- *February 2010* – GOER awarded $9.4 million through ONC for HIE planning and implementation.
- *April 2010* – AzHeC hosted 4th annual Western States Health-e Connection Summit & Trade Show.
- *April 2010* – AzHeC awarded $10.8 million by ONC to develop an Arizona Regional Extension Center.

Acronyms used in this timeline:

AHCCCS: Arizona Health Care Cost Containment System
AMIE: Arizona Medical Information Exchange
AzHeC: Arizona Health-e Connection
CAPAZ-MEX: Community Access Program of Arizona and Mexico
CMS: Centers for Medicare & Medicaid Services
EAzRx: Arizona's e-prescribing initiative
GITA: Arizona's Government Information Technology Agency
GOER: Arizona Governor's Office of Economic Recovery
HHS: United States Department of Health and Human Services
HIE: Health Information Exchange
HIT: Health Information Technology
HIeHR Utility Project: Health Information Exchange/Electronic Health Record Utility project
HISPC: Health Information Security and Privacy Collaboration
IOM: Institute of Medicine
NCVHS: National Committee on Vital and Health Statistics
ONC: Office of the National Coordinator for Health Information Technology
PACeHR: Purchasing & Assistance Collaborative for Electronic Health Records
RHITA: Rural Health Information Technology Adoption
SAHIE: Southern Arizona Health Information Exchange

Arizona Health Information Exchange (HIE)

Appendix H

PROJECT NAME: Risk Log

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	**Risk Description / Risk Event Statement**	**Responsible**	**Date Reported** day-month-year	**Last Update** day-month-year	**Impact** H / M / L	**Probability** H / M / L	**Timeline** N/M/F	**Status of Response** N / P / PE / EE	**Completed Actions / Notes**	**Planned Future Actions**	**Risk Status** Open / Closed / Moved to Issue
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the project. "Weather" is not a risk event statement. "Bad weather may delay the project" is a risk event statement.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	Enter here H (High); M (Medium); or L (Low) according to impact definitions	Enter here H (High) M (Medium) or L (Low) according to probability definitions	Enter here N (Near-term); M (Medium-term); or F (Far-term) according to timeline definitions	Enter here N (No Plan); P (Plan but not enacted); PE (Plan enacted but effectiveness not yet known); EE (Plan enacted and effective)	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated); moved to issue (risk has happened)
R 1	Improper exposure of personal health information.	State HIE Vendor Organization	31-Aug-2010	6-Oct-2010	H	M	M	N/A	10/6/0210: Held Open Stakeholder meeting to discuss privacy and security issues	Privacy and security are the number one priority and will remain at the forefront of all conversations with stakeholders.	Open
R 2	The approach to consent in the State of Arizona is outstanding. In 2008, legislation was proposed favoring an “opt-out” approach to electronic health information consent. However, the legislation was not passed due to inconclusive statewide strategy for health information exchange at that time.	State HIT Coordinator	31-Aug-2010	28-Dec-2010	M	M	M	P	1/12/2011: Arizona Health-e Connection is working on a similar "Opt-out" recommended approach to health information exchange to be introduced in the near term to our new legislature.	GOHIE realizes that the consent issue needs to be addressed early on in this process and will be targeted in the operational plan. This will be one of the first milestones in the overall project plan to be addressed. GOHIE must consider the national discussions within the HITPC on consent issues. Arizona must be prepared to conform to policies adopted at the national level that will be incorporated in Stages 2 and 3 of meaningful use.	Open
R 3	A participant agreement must be developed for distribution and stakeholder buy-in. The participant agreement should address all legalities associated with implementation of a statewide HIE to minimize the liability to the Governor’s office and other project stakeholders.	State HIE Vendor Organization / GOHIE	31-Aug-2010	28-Dec-2010	M	M	M	P	12/20/2010: A local HIE Vendor Organization (HinAZ) considered to be a large player in the Arizona HIE marketplace is expected to complete their data sharing agreement with their partners in January 2011. 12/28/2010 : Data sharing agreements must be developed for the NW-HIN Direct project in Arizona as well. We will enourage the use of the DURSA as a baseline starting point for the agreement.	The Governor’s Office intends to approach legal counsel when developing and finalizing the participation agreement. Arizona Health-e Connection already has an existing Data Sharing Participation Agreement in place which will likely be leveraged by the Governor’s Office as a foundation for any finalized Participation Agreement.	

PROJECT NAME: Risk Log

Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact H / M / L	Probability H / M / L	Timeline N/M/F	Status of Response N / P / PE / EE	Completed Actions / Notes	Planned Future Actions	Risk Status Open / Closed / Moved to Issue
R 4	Implementing an HIE platform that is not financially viable for long term sustainability.	State HIE Vendor Organization / GOHIE	31-Aug-2010	31-Aug-2010	H	M	F	P		GOHIE is the catalyst to implementing the HIE system sooner than was originally anticipated within Arizona. The community of stakeholders are charged with identifying the appropriate costs of HIE services and with what the market can bear for long term sustainability. GOHIE will facilitate this process during the 4-year implementation and create a transition plan for long term system ownership. The appropriate mix of hospital, payer, and provider contributions must be established for this system to be viable.	Open
R 5	The proposed overall project costs greatly exceed the funding available within the ONC HIE grant. Improper pricing of services in comparison of value and the cost of the services could negatively impact participation, thus increasing costs to those that are participating.	State HIT Coordinator	31-Aug-2010	31-Aug-2010	M	M	F	P		The Governor's Office will help facilitate the initial and ongoing cost structures associated with the implementation of the statewide HIE. Cost sharing and sustainability is something which must be addressed by the stakeholders and health care community so the system is affordable and is not a significant burden on those participating.	Open
R 6	Acute care hospitals may choose to implement community sharing initiatives in their service area and bypass the statewide HIE.	State HIT Coordinator	31-Aug-2010	6-Oct-2010	L	M	F	N/A	10/6/2010: A shift in how we view HIE in Arizona has made us re-evaluate this risk. A renewed understanding of "enablement" of HIE within the State to meet Stage 1 lowers the impact of this risk. Also, having addition exchange options, besides a statewide HIE, such as NW-HIN direct also lowers the impact of this risk. It is still true that certain hospitals, payers ,and other organizations partcipating and funding a statewide HIE sustainability are critical and their continued participatation is very important.	The Governor's Office will work with all of the hospitals to ensure that they will participate with the statewide HIE. Engaging the hospitals early in their technology planning processes will help ensure that independent efforts to connect physicians to hospitals will not affect the community from participating in the statewide HIE.	Open

PROJECT NAME: Risk Log

Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact H / M / L	Probability H / M / L	Timeline N/M/F	Status of Response N / P / PE / EE	Completed Actions / Notes	Planned Future Actions	Risk Status Open / Closed / Moved to Issue
R 7	Payers may choose to implement data sharing initiatives for their provider network.	State HIT Coordinator	31-Aug-2010	31-Aug-2010	M	L	M	N/A		The Governor's Office will engage payers in the design and service deployment of the statewide HIE. The goal is to identify the value for payers by participating in the exchange and implementing select services (i.e., electronic claims, eligibility verification, etc.) in the early stages to keep payers engaged in developing a statewide HIE.	Open
R 8	Vendor(s) selected have difficulties providing core capabilities within the required time frame to meet meaningful use.	State HIT Coordinator	31-Aug-2010	31-Aug-2010	H	M	N	P	12/28/2010: State HIE Core services will be implemented and phased in a structured manner by the Vendor/Organization selected. Part of the RFP process will be deliverable assurances which align to meaningful use dates and criteria.	Rigorous due diligence process followed by strict vetting of core system capabilities. Work with experienced stakeholders statewide to ensure capabilities align with current community systems. A clear definition of requirements prior to implementation with vendor(s) and stakeholders will happen in the initial phases.	Open
R 9	Not engaging with vendor(s) in a timely fashion will put hospital and vendor incentives at risk as well as GOHIE's ability to meet ONC requirements.	GOHIE	31-Aug-2010	28-Dec-2010	H	H	N	P	1/15/2011: Have met with many vendors to discuss capabilities and needs. We have now been told by ONC that our plan is likely getting close to formal approval. Therefore we will soon be moving forward with RFP activities for Core Services outlined in our stategic plan.	Focus on defining requirements, prioritizing stakeholder needs, and developing the RFP early on must be a high priority. In addition, clear definition of the procurement process will be imperative.	Open
R 10	Vendor(s) inability to meet milestones from both a time and capability standpoint will put the entire state at risk.	GOHIE	31-Aug-2010	31-Aug-2010	H	M	F	P		GOHIE will work with the vendors to define the requirements to ensure the expectations are clear for all parties. A clear and concise implementation roadmap will be developed in collaboration with the vendors and stakeholders. Clear escalation procedures will be agreed upon by all parties for accountability purposes.	Open

PROJECT NAME: Risk Log

Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact H / M / L	Probability H / M / L	Timeline N/M/F	Status of Response N / P / PE / EE	Completed Actions / Notes	Planned Future Actions	Risk Status Open / Closed / Moved to Issue
R 11	Early lack of individual provider participation in a statewide HIE	GOHIE	18-Jan-2011	18-Jan-2011	H	M	N	P		GOHIE will promote the work of the RECs and initially focus on those providers and stakeholder organizations that are enthusiastic about the payment incentive programs and Meaningful Use and build early wins with those organizations to demonstrate the ability for success of the programs. Because this is a risk of potential high impact, Arizona will prioritize these communications needs and closely monitor progress to ensure that additional resources can be directed to achieve a high degree of participation	Open
R 12	Provider reluctance to participate in a statewide HIE	GOHIE	18-Jan-2011	18-Jan-2011	H	M	N	P		GOHIE recognizes that the long-term success and sustainability of Arizona's statewide HIE depends upon widespread participation among providers and data trading partners and will remain flexible in its policies and mandates to encourage incremental participation and build trust and support over time. GOHIE will work with the AHCCCS Medicaid Program, private payers, patient organizations and other health care stakeholders active on the State HIE Advisory Committee to encourage adoption of EHR and achievement of Meaningful Use.	Open

PROJECT NAME: Risk Log

Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact H / M / L	Probability H / M / L	Timeline N/M/F	Status of Response N / P / PE / EE	Completed Actions / Notes	Planned Future Actions	Risk Status Open / Closed / Moved to Issue
R 13	Lack of options to facilitate Meaningful Use in 2011	GOHIE	18-Jan-2011	18-Jan-2011	H	L	N	P		Arizona will use the Direct Project as a foundational strategy for providers to achieve Meaningful Use. A statewide medical provider directory will be implemented via procurement. Because this is a risk of potential high impact, Arizona is prepared to implement this strategy immediately and has prioritized its implementation over originally planned activities early in 2011. Additionally, these efforts will be coordinated with the Communications Plan to ensure that providers are aware of this option and include feedback mechanisms that will allow GOHIE to make adjustments necessary to ensure success	Open
R 14	Readiness of the Direct Projec	GOHIE	18-Jan-2011	18-Jan-2011	H	H	N	P		Arizona recognizes that the Direct Project Help Desk and Technical Assistance services may be strained during the pilot Communities of Practice projects and regional collaborations. Arizona will work with the ONC to leverage any resources to support the statewide deployment of exchange capabilities via the Direct Project. Because this is a risk of high potential impact, Arizona will begin working with ONC immediately and focus its early 2011 efforts to have the appropriate elements in place as soon as the Direct Project is able to be deployed.	Open

PROJECT NAME: Risk Log

Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact H / M / L	Probability H / M / L	Timeline N/M/F	Status of Response N / P / PE / EE	Completed Actions / Notes	Planned Future Actions	Risk Status Open / Closed / Moved to Issue
R 15	Reluctance of EHR vendors to adopt the Direct Project standards	GOHIE	18-Jan-2011	18-Jan-2011	M	L	N	P		Arizona recognizes that support of the Direct Project standards is currently not a requirement for EHR certification. Arizona will aggregate provider EHR adopters to apply market pressures to vendors. Arizona will develop a list of participating EHR vendors and work with the RECs to refine the communication of EHR requirements to providers as guidance in the EHR vendor selection process. Arizona will concurrently explore other EHR alternatives to support State 1 Meaningful Use requirements.	Open
R 16	Delay of broadband deployment in underserved areas	GOHIE	18-Jan-2011	18-Jan-2011	M	L	M	P		GOHIE will continue to work closely with the BTOP grant entities to monitor progress toward filling existing gaps and assist health care providers in accessing newly developed broadband capacity.	Open
R 17											
R 18											
R 19											
R 20											
R 21											
R 22											
R 23											
R 24											
R 25											
R 26											
R 27											
R 28											
R 29											
R 30											
R 31											
R 32											
R 33											

Arizona Health Information Exchange (HIE)

Appendix I

Arizona Health-e Connection

MODEL HEALTH INFORMATION EXCHANGE PARTICIPATION AGREEMENT

Arizona Health-e Connection (AzHEC), in conjunction with Coppersmith Schermer & Brockelman PLC, prepared this Model Health Information Organization (HIO) Participation Agreement (Model Agreement) as a guide to organizations developing health information exchange arrangements. This document is intended for information only and does not constitute legal advice. Organizations should consult their own counsel for advice on health information organization (HIO) matters and agreements. This Model HIO Participation Agreement may be reproduced, in whole or in part, with attribution to Arizona Health-e Connection.

This Model Agreement addresses key issues for HIO participation, with the expectation that the document would be adapted to reflect the specific structure, business model, policies and requirements of any given HIO. The Model Agreement reflects the following assumptions:

1. Federated HIO. The Model Agreement is based on a federated HIO, with the HIO facilitating transfer of protected health information (PHI). The Model Agreement does not contemplate the HIO storing PHI on behalf of participants or creating and storing a clinical care summary as an initial activity.

2. Permitted Use. The Model Agreement provides for Addenda that can be used to outline specific HIO Permitted Uses. The initial Permitted Use described in the Model Agreement is to allow health care providers and authorized users access to PHI to provide patient treatment. It is anticipated that additional Addenda would be developed to reflect additional Permitted Uses (such as HIO use for research or public health purposes) and related terms and conditions if such uses are approved by the HIO's governance structure.

3. Single Model Agreement. The Model Agreement is a single document that covers both data providers (such as hospitals, clinical laboratories or physicians) and data recipients (under the initial Permitted Use, health care providers). The Model Agreement reflects the fact that data providers and data recipients may be the same individual or entity, such as a hospital or physician, when the initial Permitted Use is patient treatment. However, the Model Agreement can be split into separate agreements for data providers and data recipients if an HIO finds the separate documents more expedient.

4. Evolving Requirements; Attachments and Policies. The Model Agreement reflects the ongoing evolution of technical, legal and practical HIO requirements. As a result, the Model Agreement includes attachments for key obligations, such as system requirements and security requirements. These attachments could be expanded to include requirements in other areas, such as technical support, patient consent and privacy practices, depending upon the HIO's specific needs. However, in order to maintain flexibility to adapt to changing standards and circumstances, the Model Agreement also contemplates that the HIO will establish and post policies and procedures that will be incorporated by reference and updated over time. We note, however, that data providers and data recipients are far more willing to enter into an HIO Participation Agreement when key policies are known and confirmed in advance.

5. The HITECH Act Requirements. On February 17th, President Obama signed the American Recovery and Reinvestment Act of 2009 (the stimulus bill). A portion of the bill called the Health Information Technology for Economic and Clinical Health Act (the HITECH Act) made substantial changes

to the HIPAA Privacy and Security Rules, including applying most of those rules directly to HIPAA business and specifying that HIOs are business associates. The HITECH Act also establishes mandatory federal breach reporting requirements for HIPAA covered entities and their business associates. This new version of the Model HIO Participation Agreement integrates these requirements.

We hope this is useful guidance.

Beth Schermer and Kristen Rosati,
Coppersmith Schermer & Brockelman PLC

Arizona Health-e Connection

MODEL HEALTH INFORMATION ORGANIZATION PARTICIPATION AGREEMENT

PARTICIPANT	**HEALTH INFORMATION ORGANIZATION**
_____	_____
[Address]_____	[Address]_____
[City/State/Zip]_____	[City/State/Zip] _____
[Email]_____	[Email] _____
[Phone]_____	[Phone]_____
[Fax]_____	[Fax]_____

Background:

1. _____("HIO") is a [non-profit organization/governmental organization] that owns and operates an Internet-based system that provides for secure electronic health information exchange (the "Exchange").

2. Participants in the Exchange include Data Recipients (who may be Health Care Providers) that will access Data through the Exchange and Data Suppliers that will provide Data through the Exchange. A Participant may be both a Data Recipient and a Data Supplier. Participant is [check the applicable type]:

__ **BOTH.** Participant is both a Data Recipient and a Data Supplier.

__ **DATA RECIPIENT.** Participant is a Data Recipient that will participate in the Exchange to obtain health care information for a Permitted Use.

__ **DATA SUPPLIER**. Participant is a Data Supplier that makes or will make clinical Data available for access by Data Recipients (such as Health Care Providers and Authorized Users) for a Permitted Use.

Agreement:

1. HIO Activity. HIO will manage and administer the Exchange subject to the Terms and Conditions of this Agreement and applicable laws and regulations. HIO agrees to fulfill the obligations of Exchange as set forth in this Agreement, its Exhibits and Addenda.

2. Participant Activity. Participant, in its capacity as a Data Recipient and/or its capacity as a Data Supplier, as applicable, will participate in the transmission of Data through the Exchange ("Data Exchange") and the submission or use of such Data, as applicable, subject to this Agreement, its Exhibits and Addenda.

3. Complete Agreement. This Agreement includes, and incorporates by reference:

3.1 Exhibit A (Terms and Conditions);
3.2 Exhibit B (Authorized User Consent to Terms);
3.3 Exhibit C (Security Requirements);
3.4 Exhibit D (Data Recipient System Requirements);
3.5 Exhibit E (Data Supplier—Data Submission and System Requirements);
3.6 Exhibit F (HIPAA Business Associate Agreement);
3.7 Exhibit G (HIO Fees)
3.8 Any Project Addenda attached to this Agreement and signed by the HIO and Participant; and
3.9 The HIO Policies and Standards found at www.xxxx.xxxx.

4. Effective Date. The Effective Date for this Agreement is _____. The Agreement will continue until terminated as set forth in Exhibit A, Section 10.

PARTICIPANT

By:_____
Its:_____

National Provider Identifier (if Participant is a Health Care Provider): _____

Date:_____

HEALTH INFORMATION EXCHANGE

By: _____
Its:_____

Date: _____

EXHIBIT A
TERMS AND CONDITIONS OF PARTICIPATION

1.0 DEFINITIONS

Authorized User means an individual authorized by HIO or by a Data Recipient under this Agreement to use the Exchange to access Data for a Permitted Use and who has signed an Authorized User Consent to Terms in the form set forth in Exhibit B.

Data means protected health information, or information that identifies a patient, provided to HIO by Data Suppliers. For the purposes of this Agreement, protected health information is defined by the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

Data Exchange means electronically providing or accessing Data through the Exchange.

Data Recipient means an individual or entity that has entered into an HIO Participation Agreement and whose Authorized Users will receive Data using the HIO.

Data Supplier means an organization, such as a hospital, physician, clinical laboratory, pharmacy claims aggregation company, governmental agency or other entity that makes Data available for access through the Exchange and has entered into an HIO Participation Agreement. A Data Supplier also may be a Data Recipient.

Health Care Provider means a physician, group practice, hospital or health system, or other health care organization or professional that provides treatment to Patients and has entered into an HIO Participation Agreement. A Health Care Provider also may be a Data Supplier, a Data Recipient and an Authorized User.

Patient means an individual who has received or will receive treatment or health care services from a Health Care Provider.

Participant means a Data Recipient and/or Data Supplier that has entered into a HIO Participation Agreement, including the Participant named as a party to this Agreement.

Permitted Use is the reason or reasons for which Participants and Authorized Users may access Data in the Exchange. For the purpose of this Agreement, Permitted Use is defined in the Project Addenda.

Project Addendum means an exhibit to this Agreement, signed by the HIO and Participant, that describes a specific project for use of the Exchange, the Permitted Use, applicable standards and

safeguards, and related terms. Future projects, phases or expanded use of the Exchange also will be set forth in Project Addenda signed by HIO and Participant.

2.0 HIO OBLIGATIONS

2.1 Services Provided by HIO.

(a) Exchange Operation. HIO will maintain and operate the Exchange. HIO may contract with subcontractors to maintain and operate the Exchange or to provide support services. HIO will require that its subcontractors comply with the applicable terms and conditions of this Agreement, applicable laws and regulations.

(b) Access to Exchange for Permitted Use. HIO will make the Exchange available to Participants, including: (i) Data Recipients and their Authorized Users, who may access Data through the Exchange only for a Permitted Use; and (ii) Data Suppliers that provide Data for access by Data Recipients through the Exchange. HIO may establish arrangements with other health information exchanges to allow Data Recipients access to additional Data for a Permitted Use. Any change to a Permitted Use must be documented in an Addendum and signed by the HIO and Participant.

(c) Exchange Availability. HIO will make all reasonable efforts to make the Exchange available to Participants 24 hours a day, 7 days a week; however, the Exchange availability may be temporarily suspended for maintenance or unscheduled interruptions. HIO will use its best efforts to provide reasonable advance notice of any such suspension or interruptions of Exchange availability and to restore Exchange availability. Data Recipients who are Health Care Providers are responsible for securing patient health information through other means during any periods when the Exchange is not available.

(d) Support Services. During the term of this Agreement, HIO will provide support services to assist Participant in the installation, implementation, and maintenance of the software and use of the Exchange and may establish a fee schedule for these services which will be posted at www.xxx.xxx. The Exchange help desk will be available at the number and for the hours set forth at www.xxx.xxx. All support services will be subject to the HIO fees set forth on **in Section 6 or posted at xxx.xxx.xxx.**

2.2 HIO Records; Use of Data.

(a) HIO Records. HIO will maintain records relating to the operation of the HIO, including records of the date, time and records accessed by a Data Recipient in each Data Exchange as set forth in its Policies and Standards described in Section 2.3. Unless otherwise required by an Addendum, HIO will not maintain, and will not be responsible for maintaining, records of the content of any Data Exchange or inspecting the content of Data.

(b) HIO Use and Disclosure of Information. HIO will not disclose Data or information relating to Data Exchanges to third parties except: (i) as provided by this Agreement; (ii) as required by law or subpoena; or (iii) as directed in writing by the originating party or intended recipient. HIO may access Data and information relating to Data Exchanges only for the operation of the Exchange, testing, performance verification, and investigations and actions relating to compliance with this Agreement, HIO Policies and Standards and applicable laws and regulations.

2.3 Policies and Standards. HIO will establish policies and standards (respectively, "Policies and Standards") that will govern HIO's and Participant's activity on the Exchange, and these Policies and Standards will be available at www.xxx.xxx. HIO encourages Participant to provide input in the development of Policies and Standards through HIO working groups and committees. These Policies and Standards govern HIO and Participant use of the Exchange and the use, submission, transfer, access, privacy and security of Data.

(a) Changes to Policies and Standards. HIO may change or amend the Policies and Standards from time to time at its discretion and will post notice of proposed and final changes at www.xxx.xxx. HIO will provide Participants notice of such changes to Policies and Standards by electronic mail. Any changes will be effective 60 days following adoption by HIO, unless HIO determines that an earlier effective date is required to address a legal requirement, a concern relating to the privacy or security of Data or an emergency situation. HIO also may postpone the effective date of a change if the HIO determines, in its sole discretion, that additional implementation time is required. Participant will have no ownership or other property rights in the Policies and Standards or other materials or services provided by HIO.

(b) Security. HIO will implement Policies and Standards that are reasonable and appropriate to provide that all Data Exchanges are authorized, to protect Data from improper access, tampering or unauthorized disclosure and to secure compliance with applicable laws and regulations. Such Policies and Standards will include administrative procedures, physical security measures, and technical security services that are reasonably necessary to secure the Data. HIO and Participant will comply with the security Policies and Standards established by HIO, including the requirements set forth on Exhibit C.

(c) Investigations, Corrections, Reports. HIO will adopt Policies and Standards for the investigation, resolution and reporting of Patient complaints, security breaches or other concerns relating to compliance with this Agreement, HIO Policies and Standards and applicable laws and regulations ("Compliance Concerns"). HIO will provide notice to Participants, pursuant to HIO policy and as required by law or regulation, of any Compliance Concern related to Participant's Authorized Users' use of the Exchange, and Participant will cooperate with HIO in its investigation of any Compliance Concern and corrective action.

2.4 Obligations to Comply with Law. HIO will comply with all federal, state and local laws applicable to HIO. This includes Title XII, Subtitle D of the Health Information Technology for Economic

and Clinical Health (HITECH) Act, codified at 42 U.S.C. §§ 17921-17954, and regulations issued by HHS to implement the HITECH Act, which are applicable to business associates, as of the date by which business associates are required to comply with such referenced statutes and HHS regulations.

3.0 DATA RECIPIENT OBLIGATIONS. The obligations of this Section 3.0 apply to Participant if either the "Both" or the "Data Recipient" line is checked on summary page of the Agreement. These obligations do not apply to Participants who have only checked the "Data Supplier" line on the summary page of the Agreement, as those Participants will not have access to the Data in the Exchange.

3.1 Data Exchange. By engaging in Data Exchange, Data Recipient agrees that its participation in any Data Exchange, and use of the Exchange by Data Recipient and its Authorized Users, will comply with the terms of this Agreement and applicable laws and regulations. Data Recipient also agrees that Data Recipient has secured any required Patient permission to access the Data Exchange as set forth in Section 3.4.

3.2 Permitted Use. Data Recipient and its Authorized Users will use the Exchange only for a Permitted Use. Data Recipient and its Authorized Users will comply with this Agreement and all applicable laws and regulations governing the use, privacy and security of Data received through the Exchange. Data Recipient will decide in its discretion whether to use the Exchange, and to what extent.

3.3 Authorized Users. Data Recipient will identify and authenticate its Authorized Users, in accord with HIO's Policies and Standards, who may use the Exchange for the Permitted Use on behalf of Data Recipient and will require each Authorized User to execute an Authorized User Consent to Terms set forth in Exhibit B. Authorized Users will include only those individuals who require access to the Exchange to facilitate Data Recipient's use of the Data for a Permitted Use. Participant is responsible for Authorized Users complying with the terms and conditions of this Agreement and applicable laws and regulations.

3.4 Patient Permission for Data Exchange and Treatment; Notice. The parties acknowledge that certain uses of Data, including without limitation Treatment, Payment and certain Health Care Operations (as defined by the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164, Subpart E) do not require specific consent by a Patient under HIPAA or Arizona Law. However, Data Recipient is responsible for securing any Patient consent or authorization to access to Patient's Data through the Exchange as required by HIO Policies and Standards, as identified in a Project Addendum, or as otherwise required by law.

3.5 System Operations. Data Recipient, at its own expense, will provide and maintain the equipment, software, services and testing necessary to effectively and reliably participate in the Exchange as set forth in Exhibit D, except for such software expressly provided by HIO pursuant to Section 8.

3.6 Documentation of Information for Patient Treatment; Record Retention, Storage and Backup. If Data Recipient, is a Health Care Provider, it will maintain at its own expense records of Data accessed through the Exchange and used by Health Care Provider for Patient Treatment. Health Care Provider will maintain these records for all periods required by law. Health Care Provider will determine the form for such records, which may include incorporation of Data into Health Care Provider's medical record electronically, by hard copy or by other form of summary, notation or documentation.

3.7 Privacy, Security and Accuracy. Data Recipient will maintain sufficient safeguards and procedures, in compliance with Exhibit C, HIO Policies and Standards, and applicable laws and regulations, to maintain the security and privacy of Data received through the Exchange.

4.0 DATA PROVIDER OBLIGATIONS. The obligations of this Section 4.0 apply to Participant if either the "Both" or the "Data Supplier" line is checked on the summary page of the Agreement. These obligations do not apply to Participants who have only checked the "Data Recipient" line on the summary page of the Agreement.

4.1 Data Exchange and Data Submission. By engaging in Data Exchange, Data Supplier agrees that: (a) its participation in any Data Exchange will comply with the terms of this Agreement and applicable laws and regulations; (b) the Data provided or transferred by Data Supplier can be related to and identified with source records maintained by Data Supplier; and (c) Data Supplier has secured all authorizations for the submission of Data as set forth in Section 4.3. Data Supplier will make Data available for the Exchange in accordance with the scope, format and specifications set forth in Exhibit E.

4.2 Permitted Use. Data Supplier and its employees and agents will use the Exchange only to provide Data for a Permitted Use. Data Supplier, its employees and agents will comply with this Agreement and all applicable laws and regulations governing the use, privacy and security of Data made available to the Exchange.

4.3 Patient Permission for Data Submission and Data Exchange. Data Supplier and HIO acknowledge that Data Supplier will make Data available for access through the Exchange only for a Permitted Use. The parties acknowledge that certain uses of Data, including without limitation Treatment, Payment and certain Health Care Operations (as defined by the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164, Subpart E) do not require specific consent by a Patient under HIPAA or Arizona Law for these purposes. However, Data Supplier is responsible for securing any consent to supply Patient's Data to the Exchange as required by HIO Policies and Standards, as identified in a Project Addendum, or as otherwise required by law.

4.4 Data Return. HIO does not store or maintain Data and therefore has no obligation to return to Data Supplier any Data transferred or accessed pursuant to the terms of this Agreement.

4.5 Data Provided; System Operations.

(a) Systems Necessary to Participate in Exchange. Data Supplier will provide and maintain the equipment, software, services and testing necessary to effectively and reliably submit Data for access through the Exchange as set forth in Exhibit E, except for such software expressly provided by HIO pursuant to Section 8. The financial responsibility of Data Supplier and HIO in making such Data available and for providing and maintaining the equipment, software, services and testing are set forth in Exhibit E.

(b) Record Retention, Storage and Backup. Data Supplier, at its own expense, will maintain Data backup and retention to maintain adequate records of Data submitted to the Exchange for access by Data Recipients.

(c) Privacy, Security and Accuracy. Data Supplier will maintain sufficient safeguards and procedures, in compliance with the terms of this Agreement, HIO Policies and Standards, and applicable laws, to maintain the security, privacy and accuracy of Data. Data Supplier will promptly correct any errors discovered in Data it transmits to the Exchange and notify HIO of any such corrections pursuant to HIO Policies and Standards.

5.0 COMPLIANCE WITH LAWS; CONFIDENTIALITY

Both HIO and Participant, and their agents and employees, will comply with the federal and state laws and regulations applicable to this Agreement, including without limitation, laws on the use, security and privacy of Data, Patient consent for the use and transfer of Data and requirements for Data Exchanges. HIO and Participant, and their agents and employees, will maintain the confidentiality of Data as required by state and federal law. HIO's use of Data will be subject to this Agreement and the Business Associate Agreement set forth in Exhibit F.

6.0 FEES AND PAYMENT

Participant will pay HIO fees as set forth on Exhibit G.

7.0 PROPRIETARY INFORMATION

During the term of this Agreement, each party may have access to information about the other party that: (a) relates to past, present or future business activities, practices, protocols, products, services, information, content, and technical knowledge; and (b) has been identified as confidential (collectively, 'Proprietary Information") by such party. For the purposes of this provision, Proprietary Information will not include Data.

7.1 Non-disclosure. The parties will: (a) hold Proprietary Information in strict confidence; (b) not make the Proprietary Information available for any purpose other than as specified in the Agreement or as required by law or subpoena; and (c) take reasonable steps to ensure that the Proprietary Information is not disclosed or distributed by employees, agents or consultants (who will

have access to the same only on a "need-to-know basis) to third parties in violation of this Agreement. If HIO or Participant receives a request for Proprietary Information, the party receiving the request will provide the other party notice of the request and an opportunity to seek a protective order limiting the nature and scope of the information to be disclosed, and the disclosing party is only permitted to disclose Proprietary Information to the extent required by law.

7.2 Exclusions. Proprietary Information will not include information that: (a) at the time of disclosure, is known or becomes known or available to general public through no act or omission of the receiving party; (b) was in the receiving party's lawful possession before it was provided to the receiving party by the disclosing party; (c) is disclosed to the receiving party by a third party having the right to make such disclosure; or (d) is independently developed by the receiving party without reference to the disclosing party's Proprietary Information.

7.3 Equitable Remedies. The parties agree that a breach of this Section will cause the disclosing party substantial and continuing damage, the value of which will be difficult or impossible to ascertain, and other irreparable harm for which the payment of damages alone will be inadequate. Therefore, in addition to any other remedy that the disclosing party may have under this Agreement, at law or in equity, in the event of such a breach or threatened breach by the receiving part of the terms of this Section, the disclosing party will be entitled, after notifying the receiving party in writing of the breach or threatened breach, to seek both temporary and permanent injunctive relief without the need to prove damage or post bond.

8.0 SOFTWARE LICENSE

8.1 Right to Use. HIO grants to Participant for the term of this Agreement a royalty-free, non-exclusive, nontransferable, non-assignable, non-sub-licensable, and limited right to use the software identified by HIO in its technical operation Standards for the sole purpose of participating in the Exchange under the terms and conditions of this Agreement ("**Software**"). THE SOFTWARE SHALL NOT BE USED FOR ANY OTHER PURPOSE WHATSOEVER, AND SHALL NOT OTHERWISE BE COPIED OR INCORPORATED INTO ANY OTHER COMPUTER PROGRAM, HARDWARE, FIRMWARE OR PRODUCT. THE SOFTWARE IS LICENSED"AS IS" AND HIO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR TITLE. Participant acknowledges that the Software may have been licensed to HIO by third parties, and that the license granted under this Agreement is subject in every respect to HIO's grant of license from such third parties. As additional software is developed by or for HIO for the Exchange, it shall become subject to this Agreement upon written notice to Participant, and such notice shall constitute an amendment to this Agreement and any the applicable Project Addendum and shall be binding upon the parties and subject to all terms and conditions of this Agreement. This Section 8.0 applies only to Software that is provided by HIO to Participant and not to any other software that Participant may use in providing treatment to Patients or for Participant's business operations.

8.2 No Transfer or Modification. Participant will not sell, rent, sublicense or otherwise share its right to use Software. Participant will not modify, reverse engineer, decompile, disassemble or otherwise attempt to learn the source code, structure or ideas upon which Software is based.

9.0 ELECTRONIC SIGNATURES

9.1 Signatures and Signed Documents. Participant, at HIO's request, will implement for its Authorized Users an electronic identification consisting of symbols or codes that are to be affixed to or contained in a Data Exchange made by the Participant ("Signatures"). Participant agrees that any Signature of such party affixed to or contained in any Data Exchange will be sufficient to verify that the party originated such Data Exchange. Any properly transmitted Data Exchange made pursuant to this Agreement shall be considered a "writing" or "in writing" and any such Data Exchange when containing, or to which there is affixed, a Signature ("Signed Documents") shall be deemed for all purposes: (a) to have been "signed;" and (b) to constitute an original when printed from electronic files or records established and maintained in the normal course of business.

9.2 Validity of Signed Documents. Participant will not contest the validity or enforceability of Signed Documents under the provisions of any applicable law relating to whether certain agreements are to be in writing or signed by the party to be bound thereby. Signed Documents, if introduced as evidence on paper in any judicial, arbitration, mediation, or administrative proceedings will be admissible as between the parties to the same extent and under the same condition as other business records originated and maintained in paper form.

10.0 TERM AND TERMINATION

10.1 Term and Termination. The term of this Agreement will begin on the Effective Date and will continue until terminated as set forth in this Section 10. This Agreement will terminate under any of the following circumstances:

(a) Violation of Law or Regulation. If either HIO or Participant determines that its continued participation in this Agreement would cause it to violate any law or regulation applicable to it, or would place it at material risk of suffering any sanction, penalty, or liability, then that party may terminate its participation in this Agreement immediately upon written notice to the other party.

(b) For Cause. If HIO or Participant determines that the other party or any of its employees, agents or contractors have breached this Agreement, then that party may terminate its participation in this Agreement on 30 days' advance written notice to the other party, provided that such notice identifies such area of non-compliance, and such non-compliance is not cured within 15 days of receipt of the notice of non-compliance. HIO may immediately terminate this Agreement upon written notice to Participant if HIO determines that Participant or its Authorized Users, employees or agents have used Data or the Exchange for any purpose other than the Permitted Use or in violation of security or privacy provisions under this Agreement or applicable laws and regulations.

(c) Without Cause. HIO or Participant may terminate this Agreement without cause upon 30 days' advance written notice of termination to the other party.

10.2 Termination Process and Access to Exchange and Data. Upon the effective date of termination of this Agreement, HIO will cease providing access to the Exchange for the Participant and its Authorized Users, and Participant and its Authorized Users will stop using the Exchange.

10.3 Effect of Termination.

(a) Rights and Duties. Any termination will not alter the rights or duties of the parties with respect to Signed Documents transmitted before the effective date of the termination or with respect to fees outstanding and payable under this Agreement. Upon termination of this Agreement, Exhibit A, Sections 7.0, 8.0, 10.2, 10.3(b), 11, 12, Exhibit E and any other obligations that by their nature extend beyond termination, cancellation or expiration of this Agreement, will survive such termination, cancellation or expiration and remain in effect.

(b) Return of Proprietary Information; Software; Fees. Within 30 days of the effective date of termination, each party will return to the other all Proprietary Information belonging to the other or certify the destruction of such Proprietary Information if agreed to by the party who originated the Proprietary Information. Within 30 days of the effective date of termination, Participant will de-install and return to HIO all software provided by HIO to Participant under this Agreement. If Participant has prepaid any Fees or Expenses as of the effective date of termination, Participant will be entitled to a pro rata refund of such advance payment. No Data will be returned to a Data Supplier upon termination of this Agreement.

11.0 LIMITED WARRANTIES AND DISCLAIMERS

11.1 Limited Warranty and Disclaimer of Other Warranties. HIO will use its best efforts to correctly transmit Data Exchanges between Participants on a timely basis. HIO MAKES NO REPRESENTATION OR WARRANTY THAT THE DATA DELIVERED TO THE PARTICIPANT WILL BE TIMELY, CORRECT OR COMPLETE. HIO MAKES NO WARRANTY OR REPRESENTATION REGARDING THE ACCURACY OR RELIABILITY OF ANY INFORMATION TECHNOLOGY SYSTEM USED FOR THE EXCHANGE. **HIO DISCLAIMS ALL WARRANTIES REGARDING ANY PRODUCT, SERVICES, OR RESOURCES PROVIDED BY IT, OR DATA EXCHANGES TRANSMITTED, PURSUANT TO THIS AGREEMENT INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

12.0 LIMITATION OF LIABILITY; INDEMNIFICATION

12.1 Limitation of Liability. Neither HIO nor Participant will be liable to the other for lost profits or Data, or any special, incidental, exemplary, indirect, consequential or punitive damages (including loss of use or lost profits) arising from any delay, omission or error in a Data Exchange or

receipt of Data, or arising out of or in connection with this Agreement, whether such liability arises from any claim based upon contract, warranty, tort (including negligence), product liability or otherwise, and whether or not either party has been advised of the possibility of such loss or damage.

12.2 Release of Liability. Participant releases HIO from any claim arising out of any inaccuracy or incompleteness of Data or any delay in the delivery of Data or failure to deliver a Data Exchange when requested except for those arising out of HIO's gross negligence.

12.3 Indemnification.

(a) HIO Indemnification for Infringement. HIO will indemnify and hold harmless Participant, its employees and agents from any damages, expenses and costs, including reasonable attorneys fees, arising out of claims by third parties that the use of the Exchange and any Software provided by HIO infringes any patents, copyrights or trademarks or is a misappropriation of trade secrets, provided that Participant notifies HIO in writing promptly upon discovery of any such claim and gives HIO complete authority and control of, and full cooperation with, the defense and settlement of such claim.

(b) Indemnification for Breach of Agreement. Participant will indemnify and hold harmless HIO, its employees and agents from any damages, expenses and costs, including reasonable attorneys fees, from claims by third parties arising from claims arising from Participant's or its Authorized Users' breach of this Agreement, including the unauthorized or improper use of the Exchange or Participant's or its Authorized Users' use or disclosure of Data for any purpose other than a Permitted Use. HIO will indemnify and hold harmless Participant, its employees and agents from any damages, expenses and costs, including reasonable attorneys fees, from claims by third parties arising from claims arising from HIO's breach of this Agreement, including the unauthorized or improper use of the Exchange or HIO's use or disclosure of Data for any purpose other than a Permitted Use or as otherwise allowed under this Agreement.

12.4 Not a Medical Service. The Exchange does not make clinical, medical or other decisions and is not a substitute for professional medical judgment applied by Participant or its Authorized Users. Participant and its Authorized Users are solely responsible for confirming the accuracy of all Data and making all medical and diagnostic decisions.

13.0 GENERAL PROVISIONS

13.1 No Exclusion. HIO represents and warrants to Participant, and Participant represents and warrants to HIO, that neither party nor their respective employees or agents have been placed on the sanctions list issued by the office of the Inspector General of the Department of Health and Human Services pursuant to the provisions of 42 U.S.C. 1320a(7), have been excluded from government contracts by the General Services Administration or have been convicted of a felony or any crime

relating to health care. HIO and Participant will provide one another immediate written notice of any such placement on the sanctions list, exclusion or conviction.

13.2 Severability. Any provision of this Agreement that is determined to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

13.3 Entire Agreement. This Agreement constitutes the complete agreement of the parties relating to the matters specified in this Agreement and supersedes all earlier representations or agreements with respect to the subject matter of this Agreement, whether oral or written with respect to such matters. No oral modification or waiver of any of the provisions of this Agreement is binding on either party.

13.4 No Assignment. Neither HIO nor Participant may assign its rights or obligations under this Agreement without the advance written consent of the other party, except for a transfer or assignment to a parent, subsidiary or affiliate wholly owned by the party.

13.5 Governing Laws. This Agreement is governed by and interpreted in accordance with Arizona laws, without regard to its conflict of law provisions. The parties agree that jurisdiction over any action arising out of or relating to this Agreement shall be brought or filed in the State of Arizona.

13.6 Force Majeure. No party is liable for any failure to perform its obligations under this Agreement, where such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic, or communications failure).

13.7 Notices. All notices, requests, demands, and other communications required or permitted under this Agreement will be in writing. A notice, request, demand, or other communication will be deemed to have been duly given, made and received: (a) when personally delivered; (b) on the day specified for delivery when deposited with a courier service such as Federal Express for delivery to the intended addressee; or (c) three business days following the day when deposited in the United States mail, registered or certified mail, postage prepaid, return receipt requested, addressed as set forth below on the first page of the Agreement. Nothing in this section will prevent the parties from communicating via electronic mail, telephone, facsimile, or other forms of communication for the routine administration of the Exchange.

13.8 No Agency. HIO provides the Exchange services to Participant but does not act as Participant's agent. Participant will not be deemed an agent of another Participant as a result of participation in this Agreement.

13.9 No Relationship between Participants; No Third Party Rights. Nothing in this Agreement confers any rights or remedies under this Agreement on any persons other than HIO and Participant,

and nothing in this Agreement is intended to create a contractual relationship or otherwise affect the rights and obligations among Participants. Nothing in this Agreement will give any third party, including other Participants, any right of subrogation or action against any party to this Agreement.

END OF EXHIBIT A

EXHIBIT B

AUTHORIZED USER AGREEMENT TO TERMS OF ACCESS TO DATA THROUGH HIO

[Insert name of Health Information Organization] (HIO) facilitates the electronic availability of protected health information (Data) through a Health Information Exchange (the Exchange) to individuals and organizations contracting with the HIO in order to assist Health Care Providers in providing treatment to Patients. Participant (defined below) has entered into a Participation Agreement with HIO in order to facilitate this exchange of Data for these purposes.

You have been identified by Participant as an Authorized User of Data through the HIO. The HIO will agree to provide access to Data to you through the Exchange, only if you agree to the terms and conditions of this Agreement. **Agreement**

1. Compliance with Agreement

THIS IS A BINDING AGREEMENT. By signing below, you agree to comply with all terms and conditions for access to Data under this Agreement, the Participant's Participation Agreement, and all HIO policies and procedures. Failure to comply with these terms and conditions may be grounds for discipline, including without limitation, denial of your privileges to access Data through the HIO and termination of your employment or agency by Participant.

2. Permitted Use and Restrictions on Use.

2.1 Participant is a Health Care Provider who provides Treatment to Patients, as defined by the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E. As Participant's Authorized user, you may access the Exchange only to obtain Data to provide Treatment for Participant's Patients. You may not use the Exchange, or any hardware or software relating to use of the Exchange, for purposes that are outside the scope of your duties with Participant to provide Treatment to Patients.

2.2 This Consent grants you a nonexclusive, nontransferable right to use the HIO Exchange. This right is subject to the following restrictions:

a. This right is specific to you. You may not share, sell or sublicense this right with anyone else.

b. You may not change, reverse engineer, disassemble or otherwise try to learn the source code, structure or ideas underlying the Exchange's software or introduce a virus to the

Exchange. You may not connect or install unauthorized or uncertified equipment, hardware or software or improperly use the hardware or software relating to use of the Exchange.

3. Protection of Data.

3.1 Scope of Access. As an Authorized User, You may have access to Data that includes protected health information that is subject to confidentiality, privacy and security requirements under state and federal law and regulations. You agree that you will only access Data consistent with your access privileges, and pursuant to all requirements under this Agreement, the Participant's Participation Agreement, HIO policies and procedures, and applicable laws and regulations.

3.2 Protection of Data. As an Authorized User, you have an obligation to maintain the confidentiality, privacy and security of the Data.

a. You will not disclose Data except as required for your job with Participant and subject to all terms of this Agreement.

b. You will not access or view any information other than what is required for you to do your job.

c. You will not make any unauthorized copies of Data. You will not save Confidential Information to portable media devices (Floppies, ZIP disks, CDs, PDAs, and other devices).

d. You will not to email any Data to another email account.

e. You will not release your authentication code or device or password to any other person, including any employee or person acting on your behalf. You will not to allow anyone else to access the Exchange under your authentication code or device or password. You agree not to use or release anyone else's authentication code or device or password. You agree to notify HIO and Participant immediately if you become aware or suspect that another person has access to your authentication code or device or password.

f. You agree not to allow your family, friends or other persons to see the Data on your computer screen while you are accessing the Exchange. You agree to log out of the Exchange before leaving your workstation to prevent others from accessing the Exchange.

g. You agree never to access Data for "curiosity viewing." This includes viewing Data of your children, other family members, friends, or coworkers, unless access is necessary to provide services to a Patients with whom you or the physician(s) with whom you work have a treatment relationship with that Patient.

h. You will protect the accuracy of the Data submitted or received through the Exchange and will not insert information that you know is not accurate.

4. Audit and Review. HIO and Participant have the right at all times and without notice to access the Exchange and any hardware or software relating to the Exchange to review and audit your use of the Exchange and compliance with the terms of this Agreement. This includes any hardware or software located at your office, your home, or any other site from which you access the Exchange.

5. Sanctions. You understand that failure to comply with the terms of this Agreement, may result in disciplinary action against you, which may include loss of access to the Exchange as an Authorized User or termination of your employment or contract with Participant.

6. Duration. This Agreement will be in effect from the time it is signed until HIO or Participant terminates your status as an Authorized User or until you violate the terms of this Agreement. Any terms of this Agreement necessary to protect the Exchange and Data will survive the termination of this Agreement.

Agreed to by:

_____

Authorized User Signature

_____

Authorized User Printed Name

Date_____

Participant: _____

END OF EXHIBIT B

EXHIBIT C

PARTICIPANT SECURITY REQUIREMENTS

In addition to any obligations set forth in the Agreement and HIO Policies and Standards, Participant will observe the following requirements. HIO may amend or supplement these requirements on written notice to Participant.

1. Each of Participant's servers connecting to the HIO gateway will comply with HIO's authentication requirements, implementing Secure Sockets Layer (SSL) encryption and using certificates approved by HIO.

2. Participant will authenticate each Authorized User at the point of access and will implement password policies, both based on applicable laws and regulations and HIO Policies and Standards. Participant may elect to implement stronger authentication mechanisms at its discretion. Participant will review and update its list of Authorized Users as required under HIO Policies and Standards.

3. Participant will limit access of each Authorized User to a Permitted Use and according to Role Based Access principles. Participant will impose appropriate sanctions for its employees or agents who violate applicable security Policies and Standards or the Authorized User Terms of Consent or make improper use of the Exchange, including revocation of an Authorized User's authorization to access the Exchange as may be appropriate under the circumstances.

4. Participant will maintain access logs that capture end user identification information.

5. Participant will implement message-level security using WS-Security or other security technology acceptable to HIO.

6. Participant will implement firewalls and intrusion detection per HIO Policies and Standards.

7. Participant will implement other safeguards to protect servers based on information security best practices, such as the SANS Institute (www.sans.org) recommendations.

8. Participant will perform periodic automated and random manual review and verification of audit logs for both operational monitoring and system security as required by HIO Policies and Standards.

END OF EXHIBIT C

EXHIBIT D

DATA RECIPIENT—SYSTEM REQUIREMENTS

1. System Requirements.

HIO will provide a secure viewer application to Data Recipients to retrieve and view Data for their Patients. The secure viewer application is web-based and requires a secure system with an Internet connection and an Internet browser. HIO requires the following minimum system configuration options for running the HIO viewer on a browser.

[*Insert specific System Requirements*]

2. Additional Financial Requirements.

[*Insert Additional Financial Requirements supplementing Exhibit A, Section 3*]

3. Maintenance and Support Requirements.

[*Insert Maintenance and Support Requirements*]

END OF EXHIBIT D

EXHIBIT E

DATA SUPPLIER—DATA SUBMISSION, SYSTEM REQUIREMENTS AND FINANCIAL RESPONSIBILITIES

1. Data Provided.

Data Supplier will submit Data as set forth in the Addenda.

Data submitted shall be mapped to HIO standard terminologies and code systems according to the message specifications. HIO may provide message specifications and terminology standards as a reference when creating data maps. HIO and Data Supplier will cooperate with each other to mutually validate the data maps created.

2. System Requirements.

[*Insert System Requirements*]

3. Financial Responsibilities.

[*Insert Financial Responsibilities*]

4. Maintenance and Support Requirements.

[*Insert Maintenance and Support Requirements*]

END OF EXHIBIT E

EXHIBIT F

BUSINESS ASSOCIATE AGREEMENT

HIO and Participant agree to the terms and conditions of this Business Associate Agreement in order to comply with the use and handling of Protected Health Information ("PHI") under the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E ("Privacy Rule") and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C ("Security Rule"), both as amended from time to time. Unless otherwise provided, all capitalized terms in this Business Associate Agreement will have the same meaning as provided under the Privacy Rule and Security Rule.

For purposes of this Business Associate Agreement, Protected Health Information ("PHI") or Electronic Protected Health Information ("ePHI") includes only individually identifiable health information handled by HIO that is provided to the Exchange by Participant.

1. USES AND DISCLOSURES OF PHI: HIO will use or disclose PHI only for those purposes necessary to perform Services under the Agreement, or as otherwise expressly permitted in the Agreement, its Exhibits including this Business Associate Agreement, or its Addenda, or as required by law, and will not further use or disclose PHI. HIO agrees that anytime it provides PHI to a subcontractor or agent to perform Services, HIO first will ensure that each such subcontractor or agent agrees to the same terms, conditions, and restrictions on the use and disclosure of PHI as contained in this Business Associate Agreement.

2. HIO USE OR DISCLOSURE OF PHI FOR THE HIO'S OWN PURPOSES: HIO may use or disclose PHI for HIO's management and administration, or to carry out its legal responsibilities. HIO may disclose PHI to a third party for such purposes if: (1) The disclosure is required by law; or (2) HIO secures written assurance from the receiving party that the receiving party will: (i) hold the PHI confidentially; (ii) use or disclose the PHI only as required by law or for the purposes for which it was disclosed to the recipient; and (iii) notify the HIO of any breaches in the confidentiality of the PHI. HIO also may aggregate the PHI with other PHI in its possession or otherwise de-identify PHI according to the requirements of 45 C.F.R. §164.514(b).

3. SAFEGUARDS: HIO will implement and maintain appropriate safeguards to prevent any use or disclosure of PHI for purposes other than those permitted by this Business Associate Agreement. HIO also will implement administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of any ePHI that HIO creates, receives, maintains, and transmits on behalf of Participant.

4. UNAUTHORIZED USES OR DISCLOSURES and BREACHES:

a. Reporting Security Incidents. HIO will report to Participant any successful unauthorized access, use, disclosure, modification, or destruction of ePHI or interference with system operations in an information system containing ePHI of which HIO becomes aware within 15 business days of HIO's learning of such event. HIO will also report the aggregate number of unsuccessful attempts to access, use, disclose, modify, or destroy ePHI or interfere with system operations in an information system containing ePHI of which HIO becomes aware, provided that such reports will be provided only as frequently as the parties mutually agree, but no more than once per month. If the definition of "Security Incident" under the Security Rule is amended to remove the requirement for reporting "unsuccessful" attempts to use, disclose, modify or destroy ePHI, HIO will cease reporting unauthorized attempts as of the effective date of such amendment.

b. Reporting Breaches of Unsecured PHI. If HIO has a Breach of Unsecured PHI, both as defined in this Section, HIO will report such Breach as provided in this Subsection.

(1) Definitions:

Breach is the unauthorized acquisition, access, use, or disclosure of PHI, unless the unauthorized person to whom such PHI is disclosed would not reasonably have been able to retain the PHI. However, a Breach does not include any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of HIO if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual with HIO and such PHI is not further acquired, accessed, used, or disclosed by any person.

Unsecured Protected Health Information (PHI) is PHI that is not secured through the use of technologies or methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, which technologies or methodologies are specified in guidance issued by the Secretary of HHS at 74 Fed. Reg. 19006 (April 27, 2009), and as updated from time to time.

(2) Reporting to Participant. HIO will report the Breach of Unsecured PHI to the Participant within 15 days of HIO's learning of the Breach. HIO learns of the Breach when an employee, officer, or agent of HIO learns of the Breach (unless such employee, officer or agent is responsible for the Breach and did not inform anyone else at HIO). Such report will include the following information: (i) the identification of each individual whose unsecured PHI has been, or is reasonably believed by HIO to have been, accessed, acquired, or disclosed during the Breach, including their contact information if available to the HIO; (ii) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known; (iii) a description of the types of Unsecured PHI involved in the Breach (such as name, Social Security number, date of birth, home address, or account number); (iv) a brief description of what HIO is doing or has done to investigate the Breach, mitigate losses to individuals and Participant, and protect against any further breaches; and (v) contact procedures for individuals to ask questions or learn additional information about the Breach, which shall include a toll-free telephone number and an e-mail, website, or postal address at HIO. If HIO will report to individuals directly under Subsection (3), HIO will include its notice (in draft or final form, if already sent).

(3) Reporting to Individuals. If PHI originating from more than one Participant is involved in a Breach, the HIO will conduct the reporting on behalf of such Participants, so as to avoid duplicative reporting to individuals by Participants.

(a) Timing of Report: HIO will make such report without unreasonable delay and in no event later than 60 days after HIO learns of the breach. However, HIO may delay reporting to individuals if a law enforcement official determines that reporting will impede a criminal investigation or cause damage to national security, in which case reporting may be delayed in the same manner as provided under 45 C.F.R. § 164.528(a)(2).

(b) Content of Report: HIO will include the following information in the report to individuals: (i) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known; (ii) a description of the types of Unsecured PHI involved in the Breach (such as name, Social Security number, date of birth, home address, or account number); (iii) a brief description of what HIO is doing or has done to investigate the Breach, mitigate losses to individuals, and protect against any further breaches; (iv) steps individuals should take to protect themselves from potential harm resulting from the Breach; and (v) contact procedures for individuals to ask questions or learn additional information about the Breach, which shall include a toll-free telephone number and an e-mail, website, or postal address at HIO.

(c) Method of Reporting to Individuals: HIO will provide the report to individuals in writing, by first class mail, sent to the last known address of the individual (or to the next of kin if the individual is deceased). If an individual has specified a preference for electronic mail in communications with the HIO, then HIO will use electronic mail. In cases where there is insufficient or out-of-date information to provide the written notice required, HIO will include a conspicuous posting on its website; or if it does not have a website, provide the required information to major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The website posting or media announcement will include a toll-free phone number so that affected individuals may learn whether or not their unsecured PHI may have been included in the breach.

(d) Reporting to the Media: If HIO believes that the Unsecured PHI of more than 500 individuals residing within its jurisdiction of operation has been accessed, acquired, or disclosed in the Breach, HIO will provided notice to major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. The media announcement will include a toll-free phone number so that affected individuals may learn whether or not their unsecured PHI may have been included in the breach.

(e) Reporting to HHS: If HIO believes that the Unsecured PHI of more than 500 individuals residing within its jurisdiction of operation has been acquired or disclosed in the Breach, HIO will notify the Secretary of HHS immediately, and will indicate in its notice to HHS that the report is made on behalf of the Participants of the HIO to avoid duplicative reporting.

(4) Reimbursement to Participant for Reporting Costs: HIO will reimburse Participant for any reasonable expenses Participant incurs in notifying individuals of a Breach caused by HIO or its subcontractors or agents.

5. INDIVIDUAL ACCESS TO PHI: If an individual makes a request to HIO for access to PHI, HIO will within 10 business days forward such request in writing to Participant. Participant will be responsible for making all determinations regarding the grant or denial of an individual's request for PHI and HIO will make no such determinations.

6. AMENDMENT OF PHI: If an individual makes a request to HIO for amendment of PHI, HIO will within 10 business days forward such request in writing to Participant. Participant will be responsible for making all determinations regarding amendments to PHI and HIO will make no such determinations.

7. ACCOUNTING OF DISCLOSURES OF PHI: If an individual makes a request to HIO for an accounting of disclosures of PHI, HIO will within 10 business days forward such request in writing to Participant. Participant will be responsible for preparing and delivering the accounting to the individual. Upon request, HIO will make available to Participant information about HIO's disclosures of PHI, if any, that must be included to respond to individual requests for accounting of disclosures of PHI under applicable law.

8. ACCESS TO BOOKS AND RECORDS: HIO will make its internal practices, books and records on the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services to the extent required for determining Participant's compliance with the Privacy Rule. Notwithstanding this provision, no attorney-client, accountant-client or other legal privilege will be deemed waived by HIO or Participant as a result of this Section.

9. TERMINATION: Participant may terminate the Agreement upon written notice to HIO if HIO breaches a material term of this Business Associate Agreement and HIO fails to cure the breach within 30 days of the date of notice of the breach.

10. RETURN OR DESTRUCTION OF PHI: Participant understands that PHI provided to the Exchange may be integrated into the medical record of Data Recipients that access the Exchange. Moreover, HIO does not maintain or store PHI. As such, it is not feasible for HIO to return or destroy PHI upon termination of the Agreement. [HIO agrees to follow the provisions of this Business Associate Agreement for as long as it retains PHI, and will limit any further use or disclosure of PHI to those purposes allowed under this Business Associate Agreement, until such time as HIO either returns or destroys the PHI.]

END OF EXHIBIT F

EXHIBIT G

HIO FEES AND PAYMENT

1. Program Fee. Participant will pay a program fee ("Fee") to HIO in the amount of _____ _____ ($_____) per ***calendar quarter/ per month***. If this Agreement is in effect for part of a quarter/month, the Fee will be prorated on a daily basis. HIO may modify the Fee from time to time, but such modification will not become effective until Participant has received at least 60 days advance written notice of such modification. Such notice will specify the effective date of the modified Fee.

2. Technical Support Service Fee: Participant will pay HIO for technical support services as follows:

2 Payment. The Fee shall be payable in advance on or before the fifth day of each quarter/month. After 15 days, such payments shall accrue interest at the lesser of 1% per month or the highest rate allowed by applicable law.

END OF EXHIBIT G

PROJECT ADENDUM NO. 1

Project Name and Effective Date	Health Information Exchange for Treatment Purposes Effective: _____
Data Submitted for Exchange	[Insert description of Data for submission]
Permitted Uses	Health Care Provider and Authorized Users may access the Exchange to obtain Data for the Treatment (as defined in this Addendum) of Health Care Provider's Patients. If Health Care Provider includes Data in its Medical Record, Health Care Provider and Authorized Users may use Data only for those purposes permitted by law.
Authorized Users	Authorized Users are employees, independent contractors or agents of a Health Care Provider who (i) have been authenticated and given access in compliance with HIO Policies & Standards by the Participant; (ii) have executed an Authorized User Consent to Terms, and (iii) require access to Data to facilitate the provision of treatment by the Health Care Provider to Patients.
Specific Safeguards and Privacy Requirements	All Participants shall adhere to the HIO Policies and Standards available at www.xxx.xxx.
Licensed Software	
Certification Requirements	
Definitions for Project Addendum No. 1	1. "**Treatment**" means the provision, coordination or management of health care services by one or more Health Care Providers, as defined by HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 164, Subpart E. 2. "**Medical Record"** means all communications related to a Patient's physical or mental health or condition that are recorded in any form or medium and that are maintained by the Health Care Provider for purposes of Patient diagnosis or Treatment, including medical records that are prepared by the Health Care Provider or other providers, as defined by A.R.S. § 12-2291.

PARTICIPANT

By: _____
Its: _____
Date: _____

HEALTH INFORMATION EXCHANGE

By: _____
Its: _____
Date: _____