Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Solutions Report

Subcontract No.
RTI Project No. 9825

Prepared by:

Shannon Smith-Ross, MPH, MS
Donna Travis
Virginia Headley, PhD (Headley and Associates)
Illinois Foundation for Quality Health Care
2625 Butterfield Road
Oak Brook, IL 60523 I

Submitted to:

Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

January 15, 2006

RTI INTERNATIONAL

Table of Contents

Section 1 - Background

Purpose

The purpose of this report is to document the proposed solutions to privacy and security-related issues that have been identified as significant barriers to the successful electronic health information exchange (HIE) within the state of Illinois. This report will outline the process used to determine and clarify these barriers and the methodology used to develop solutions to address them. Each proposed solution will include a description of its HIE context, the privacy and security areas affected, stakeholders involved, HIE barriers being addressed, stage of development and use of the solution and possible barriers to implementation.

Report Limitations

Efforts were made to ensure this report provided solutions that were comprehensive, effective, and developed with the input of as many stakeholder communities as possible. Despite these efforts, there are still factors that must be taken into account that directly impact the report content. Health information management experts provided significant input. This could have an impact on the tenor of the solutions offered. A very rigid decision-making methodology was deployed to develop the solutions outlined in the report. This methodology took considerable time and effort of the SWG along with input from the HSC and Legal Working Group (LWG). Face-to-face interaction was critical to the decision-making process. However, given that a significant portion of solution development occurred during the holiday time period, participation sometimes was less than optimal. Given this, a few concessions had to be made to get the level of input desired. More out-of-meeting work was done than originally desired. The impact of this is that some of the dynamics garnered from group interaction were forgone for the sake of expedience and inclusion.

State of HIE in Illinois

Currently, Illinois is in the infancy of widespread HIE. Significant investment in health information technology is occurring within individual healthcare organizations across the state. Increasingly, Illinois healthcare providers of all sizes and constituent population types are recognizing the need and potential benefit of HIE and are trying to create an internal infrastructure to support this. However, electronic exchange of health information has not gotten a real foothold in the state. Efforts are underway to change this. One such effort is the work being done by the Illinois Electronics Health Records Taskforce (EHRTF). The EHRTF has recently submitted its final report to the Illinois General Assembly. One of the taskforce's recommendations to the General Assembly calls for the creation of a not-for-profit organization, the Illinois Health Information Network (**ILHIN**), to establish a state-level health information exchange. The Illinois Department of Public Health would form a public-private partnership with **ILHIN** to advance EHR and health information exchange initiatives within the state if taskforce recommendations are enacted. Another key recommendation of the taskforce is for the Department/ILHIN public-private partnership to create an initiative to foster the adoption of electronic health record systems and the development of regional health information exchanges. In arriving at this recommendation, the taskforce recognized that creating a mechanism to facilitate the sharing of health information is more beneficial if more health care providers possess the technology to utilize this capability.

Section 2 – Summary of Interim Assessment of Variations Report

The Variations Working Group (VWG) along with over 20 other stakeholders representing a wide array of organizations, including providers, 3rd party payers, public health, law enforcement, and legal experts were interviewed to assess the variety of policy and procedures organizations deploy to handle privacy and security while exchanging health information. Over one hundred (100) unique business practices among 30 representative organizations were discovered. The uses of technology to capture, maintain, and share patient information varies tremendously among Illinois' organizations. As would be expected, business practices surrounding privacy and security of health information vary based on the level of technology available to an organization. However, several common themes appear regardless of the level of technology available to an organization. The varying array of interpretation and sometimes misinterpretation of HIPAA is a common issue, sometimes even within the same organization. Also, for paper-based organizations, sharing of information has been based significantly on established trusted relationships. The level and method of sharing is based on familiarity between the existing parties more so than established business agreements. As such, a telephone call from a trusted person will garner the requisite information and perhaps more than required.

One of the key findings of this study is that Illinois has very strong protections to ensure that privacy and security are maintained during the exchange of health information. However, because there is currently little electronic exchange of information between organizations, there are few operational examples of these protections as it relates to electronic HIE. Silos of technology utilization are found throughout Illinois. Many health care organizations have been able to incorporate significant technological resources to maintain patient data. This is particularly true of the major urban health care facilities in the Chicago area. However, very little effort has gone into enabling organizations to share data electronically with one another. Chief among the reasons for this is that the culture in Illinois is not particularly conducive to data sharing. Information is often deemed as proprietary and a business asset as opposed to an opportunity to improve quality of care and patient safety. As witnessed by the work of the Illinois EHRTF, this trend seems to be changing. However, culture change tends to be a slow process. The cultural change and technical infrastructure necessary for sharing of information needs to come together before the policies and procedures necessary to facilitate health information exchange begin to become more commonplace.

In identifying organizational-level practices, there are a few practices that appear to have a level of effectiveness in ensuring improved electronic exchange of health information. An effective practice means the practice allows information to be exchanged more efficiently, that is in less time or with fewer steps and/or more consistently while still maintaining the appropriate level of security and privacy. An example of such a practice would be the universal training of users prior to provision of system access. Having users trained on appropriate system use and access rights ensures that people who provide the entry of key data understand the importance of accuracy, accountability, security, and timeliness of system data and the impact of its inappropriate use. This practice falls within the Information Authorization and Access Controls domain. Another example of an effective practice is the use of encryption and a secure website to submit data between organizations such as a provider and pharmacy. Employing available

technology such as encryption and secure website protocols are necessary to defend against the threat of security breaches. This practice is part of the Information Transmission Security or Exchange Protocols. Finally, one stakeholder provides a CD containing medical information including, if necessary, protected health information, in an encrypted, standardized format to requesters who are granted authorization via a patient release. In lieu of true electronic HIE between organizations, this method is a novel precursor to higher level of sophistication that is starting to take shape in the state.

During the organizational-level practice review process, several business practices that inhibit HIE were identified. A practice that was often described by many stakeholders was the dependence on familiarity with the requester by the organization providing the information. In an environment where true electronic HIE is occurring, reliance on requester familiarity will be an inefficient, if not altogether impossible practice to continue. Utilization of non-encrypted e-mails and other forms of electronic communication also inhibit HIE. Organizations expose themselves to considerable risk when they do not incorporate viable technology options to protect patient data. Another issue facing Illinois organizations is the lack of standardization around HIPAA's minimum necessary requirements. Often, the interpretation of what is minimally necessary information to provide a requester is left up to the discretion of the organization at best, and at times the individual employee fulfilling the request. Without standards specifically addressing what is appropriately necessary in an electronic HIE environment, human intervention will have to occur on a case-by-case basis, thus creating a potential bottleneck and impeding electronic exchange. In Illinois, placement of an appropriate technical infrastructure along with significant cultural change will have to occur in order to overcome these inhibiting practices.

Section 3 – Review of State Solution Identification and Selection Process

The barriers of personal familiarity for user authentication, inappropriate use of non-secured information technology, and variable application of HIPAA minimum necessary information guidelines that were identified by the Variations Working Group (VWG) were considered to comprise too limited a list for an adequate solutions development process, given that Illinois is in such a low level of HIE development. The Solutions Working Group (SWG) began with the task of the development of a more comprehensive list of barriers than that which was derived from the process used by the VWG on its review of business practices in Illinois as they relate to the security and privacy of electronic health records. The list of barriers generated through discussion by the SWG was based on their expertise and experience in their relative professional fields, rather than scenario-driven, as was the case for the VWG. The list was organized into eight basic types of barriers:

- Organizational Culture Barriers
- Technology and Standards Barriers
- Staff Knowledge about Health Information Exchange Barriers
- Consumer Knowledge about Health Information Barriers
- In-house Resources for Information Management Barriers
- Privacy and Security Leadership Development Barriers
- Global Market Barriers
- Legal Barriers

These areas were investigated further to identify any possible root causes that could be exploited for effective solutions development. Root causes for each barrier in all barrier groups were identified by facilitated discussion. A total of 39 barriers with 148 associated root causes were identified. The complete list of all barriers identified and their specific root causes can be found in Appendix: Barriers to the Implementation of HIE in Illinois.

Following the identification of root causes for the barriers to implementation, the SWG then grouped the root causes into related areas for solutions development.

The following eight solution areas were identified:

- Benefits of regional exchange of health information
- Technology standards development
- Professional standards development
- Consumer education
- Staff education
- Inclusion of economically disadvantaged healthcare groups
- Quality assurance for electronic information exchange
- Legislation and enforcement

The comprehensive list of all root causes as they are organized into solution development areas can be found in Appendix: Root Causes to Barriers to the Implementation of HIE in Illinois.

Work by the SWG was accomplished via facilitated meetings (4), teleconferences (4), and an online survey instrument.

The Solutions Working Group, membership and stakeholder representation are indicated in the table below.

Committee Members	Organization	Area/Industry of Expertise
Margret Amataykul, MBA, RHIA, CHPS, FHIMSS	Margret\A Consulting, LLC	EHR Consultant
Maria I. Ferrera	CCA Strategies LLC	Consumer Advocate
Steven Glass	Access Community Health Network	Healthcare/Ambulatory Information Technology
Joe Granneman	Rockford Memorial Hospital	Healthcare/Inpatient Information Technology
Merida Johns, PhD, RHIA.	Bundling Board	HIM Expert
Vernel Johnson, MD	St. James Hospital	Emergency Medicine
Gary Nalley	University of Illinois Medical Center at Chicago	HIT Expert
Maria Pekar	Loyola University Health System	Attorney/Risk Management
Lou Ann Schraffenberger,MBA, RHIA, CCS, CCS-P	Advocate Health Care	HIM Expert
Donna Schnepp, MHA, RHIA	Moraine Valley College	HIM Expert/Academic
Geraldine Smothers, RHIA	Professional Dynamic Network	HIM Expert/IHEMA
Rachelle Stewart, DrPH, RHIA	University of Illinois at Chicago	Academic HIM
Neal Zeigler, MD	Baylor Medical Center	Emergency Medicine

Charge of SWG: The Solutions Working Group (SWG) is responsible for developing a detailed report on the proposed solutions to privacy and security issues that impact the wide-spread electronic exchange of health information among organizations in and around the state of Illinois focusing at a minimum on the nine domain areas of privacy and security.

Stakeholder Representation by the SWG: A significant proportion of the members of the SWG are experts in health information management and information technology systems. Other members include legal (risk management), physicians (emergency medicine), and a consumer advocate.

Solutions were proposed in facilitated discussions with the members of the SWG. Five of the eight different areas identified for the development of proposed solutions had solutions proposed by the SWG alone. These areas included benefits of regional exchange of health information, technology and professional standards development, inclusion of the economically disadvantaged healthcare groups, and quality assurance for electronic information exchange. Solutions for consumer education, staff education, and legislation and enforcement were proposed in a facilitated discussion with the members of the SWG, Legal Working Group (LWG), and HISPC Steering Committee (HSC). The lists of all solutions generated can be found in Appendix: Solutions for Root Causes of Barriers to the Implementation of HIE in Illinois.

Criteria for prioritization of the solutions were obtained by facilitated discussion in a combined meeting of the HSC, LWG, and SWG. The criteria were then weighted by nominal consensus. Solutions were ranked as to the degree to which they met each criterion by nominal consensus in an online survey open for all members of the HSC, LWG and SWG. A final weighted score for each solution was obtained by taking the consensus ranking for each solution, multiplying each rank by its criterion weight, and then summing all weighted rank scores. The solution with the highest consensus prioritization score for each solution area was selected for extended analysis in the Interim Assessment of Solutions Report. Consensus ranking for all solutions can be found in Appendix: Prioritization of Solutions for the Implementation of HIE in Illinois.

The Illinois Electronic Health Records Taskforce (EHRTF) will serve as the reviewing body for the proposed solutions. The solutions will be vetted and evaluated by EHRTF prior to implementation planning. Task Force membership includes representatives from several key stakeholder areas including physicians, hospitals, pharmacies and long term health care facilities, academic health care centers, payors, information technology providers, patients and consumers. This wide array of representation will help ensure the solution reviewing process is as inclusive as possible of all key stakeholder communities.

It was determined by inter-relationship analysis of all the solution areas by the SWG that efforts to promote the benefits of regional exchange of health information would be a major driver for HIE development in Illinois. As information became available to stakeholders concerning the cost effectiveness and positive impact on patient care and outcomes, this information could then act as a catalyst for the promotion of HIE developmental activities. Additionally, the adoption and promulgation of standards, for both technology and the professional development of leaders for security and privacy, would drive the development of HIE, because both the technical ability to exchange information would be enhanced by solutions in these areas, as well as the organizational ability and will to do so. The promotion of education of both healthcare staff and consumers on electronic health records would assist even further in the development of HIE as familiarity with the technical processes developed, and trust of protections put in place became known and accepted. Major outcomes of efforts applied in benefit analysis, standards development, and education would be the facilitation of the inclusion of the economically disadvantaged, enhanced quality assurance of the systems put in place, and the adoption and enforcement of clear and timely legislation in support of security and privacy. This approach of identification of drivers and outcomes of the process defined the structure for the discussion of the solutions, as focus for implementation would be put upon those driving activities most likely

to leverage development, and major outcomes would become key indicators of successful development.

Through a facilitated discussion with the HSC, LWG and the SWG, general barriers to the implementation of any proposed solution were determined. These feasibility barriers included primarily economic and structural/organizational considerations. Economic barriers to feasibility included cost of implementation, lack of proven value of HIE, and unidentified funding streams. Organizational barriers included complexity of systems and processes for implementation, change aversion, requirement for long-term organizational commitment, indeterminate consensus among stakeholders, and unidentified resource availability. Individual solutions were ranked by group consensus as to their overall feasibility during the prioritization process. Feasibility rankings can be found for each solution in Appendix: Prioritization of Solutions for the Implementation of HIE in Illinois, under Weighted Criteria Column B, Maximize Feasibility.

Section 4 – Analysis of State Proposed Solutions

Solution (1). A comprehensive, systematic approach to the promotion of the benefits of exchange of health information was identified by the SWG to have the capacity to leverage efforts for the development of HIE in Illinois. The specific solution to benefits promotion identified to be of highest priority for action was to determine the benchmarks for regional exchange of information, perhaps by a committee of industry (HIT and administrative) stakeholders, similar to that which was done for HIPAA transactions.

- This solution would address a number of barriers in barrier categories of In-House Resources for Information Management, Organization Culture, and Technology and Standards Barriers. Specifically, barriers due to variations in information technology development from organization to organization, a barrier in In-house Resources for Information Management Barriers, could be alleviated by a standardized approach for information exchange. Variations in the organizational culture of physical/paper records, the culture of actions based on risk aversion and/or comfort rather than standards, the culture of market competition, the culture of organization type such as clinics vs. hospitals, public vs. private, etc., and the culture of ownership of data and not sharing it (in Organizational Culture Barriers) all would be affected by the creation of a level playing field brought about by benchmarking. Furthermore, benchmarked standards would by definition begin to create the infrastructure which does not exist currently in Illinois for the electronic exchange of information, such as a RHIO (a barrier in Technology and Standards Barriers).
- The establishment of benchmarks for regional exchange of information would impact all domains of privacy and security of information, as well as all stakeholders in HIE. Small pockets of exchange are occurring currently in Illinois, but efforts have been neither coordinated nor synchronized, so the development of standards for statewide applicability is essentially at a zero stage. Local standards, however, may prove to be productive starting points for the implementation of this solution.

Solution (2). The SWG determined that the single most important technical standard needed to move HIE forward in Illinois was for all accrediting agencies to adopt a universal standard for patient identification, with official, verifiable means of both primary and secondary identification defined.

- This solution addresses, through standardization, the specific barrier of the technical challenge to patient identification, one of the Technology and Standards Barriers. Furthermore, insufficient resources for language diversity to assure provision of information, and the adequate comprehension of information given, a barrier in In-house Resources for Information Management Barriers, is addressed via a technical solution for patient identification. By the creation of a universal standard for this data field, the cultural barriers of organization type and of ownership of data and not sharing it (in Organizational Culture Barriers) are reduced by the creation of a reliable means of patient identification.
- The type of information to be exchanged addressed by this solution is focused specifically on patient identification, Domain 3. Many stakeholder institutions in Illinois have electronic information management systems, and therefore have a means of patient identification. The degree of standardization that exists currently for the identification

algorithms and data fields in use throughout the state is unknown. Adoption of a universal standard would impact all stakeholders with health information management systems, as well as any stakeholder accessing health information, thus impacting all stakeholders.

Solution (3). A recurring theme in discussions by the SWG concerning barriers to HIE in Illinois was the impact of the inconsistent availability of privacy and security expertise in organizations. This theme appeared in discussions concerning barriers in the major barrier types of Privacy and Security Leadership Development, In-house Resources for Information Management, Legal, Organizational Culture, and Staff Knowledge About Health Information Exchange. The solution proposed and prioritized by the SWG to address all these barrier areas was to define the professional qualifications for privacy and security officers. Included in the definition would be the requirement for such an officer within an organization, and that officer's specific roles and responsibilities.

- By providing a standardized approach for organizations to assign roles and responsibilities for their privacy and security officers, this solution would address a number of barriers found in Privacy and Security Leadership. Organizations may exclude privacy experts in information technology solutions up front, and instead include them in the back end of the solutions process, thus complicating the acquisition and implementation of IT solutions with appropriate privacy and security protection. Organizations often assign dual functions in a single person as both legal counsel and privacy officer, which spreads staff too thin for effectiveness. Furthermore, there are no mandated national standards for privacy and security officers, there is a general lack of security officers for information technology statewide, and there is a lack of credentialing in both privacy and security officers. All of these contribute to an overall lack of organizational infrastructure for information edit checks, audits, and general quality assurance of health information. As far as barriers exist due to In-house Resources for Information Management, the variations in information technology development from organization to organization, and resource availability from organization to organization both would be impacted positively by a delineation of roles and responsibilities for privacy and security within a specified individual. Legal expertise often resides in organizations outside of health information management staff, and identified Legal Barrier. This division of responsibility would be alleviated by a joining of responsibilities under this solution. Variations in the culture of organization type, identified in Organizational Culture Barriers, would also be addressed by the creation of a standard approach to privacy and security leadership. By adoption of this standardized organizational approach to privacy and security officers, the current lack of ongoing education for staff to understand the results and/or ramifications of the release of health information, a barrier in Staff Knowledge About Health Information Exchange Barriers, also would be positively impacted by their role. This solution would provide for organizations a path to develop the adequate infrastructure and role delineation for the development and enforcement of all security, privacy, and information management policies and procedures.
- This solution does not focus so much on what information would be exchanged, as all information would be impacted by an actively engaged, expert privacy and security officer in an organization, but rather would impact the development of policies and

procedures for the exchange of health information in an organization. The domains involved in exchange policies and procedures include those for information authorization and access controls (Domain 2), information transmission security or exchange protocols (Domain 4), information audits (Domain 6), administrative and physical safeguards (Domain 7), state law restrictions (Domain 8), and information use and disclosure (Domain 9). Stakeholders most impacted would be those organizations which produce and maintain health information, not necessarily those that would just access it, as it would be the producing organizations that would be required to have an identified privacy and security officer.

Solution (4): No discussion of HIE is complete without inclusion of the human interface with all the systems for health information management: the professional staff which must provide the information to and control the flow of information through the systems. Another major recurring theme in the SWG discussions on barriers to HIE involved the impact of staff knowledge, or lack thereof, on the implementation of HIE and the protection of privacy and security. As a solution to the variations experienced in staff knowledge, expertise, and training, the SWG recommends to establish core competencies for staff education, to include not only privacy and security training, but awareness of the technical issues relevant to their job responsibilities and electronic health information.

- This solution addresses a number of barriers in the barrier group Staff Knowledge About Health Information Exchange Barriers, including a perception that there is a lack of ongoing education for staff to understand the results and/or ramifications of the release of health information, that there is a lack of standardized educational materials that have been developed for sufficient evaluation of effectiveness, that there is a lack of understanding by staff of what is appropriate and what is not in the exchange of health information, and that there is a lack of ways to share educational materials. Defined core competencies would provide the educational foundation for effective training in all aspects of health information management and exchange. An Organizational Culture Barrier identified included a culture of diminished value of staff continuing education. Having core competencies defined will enable institutions to target their training funds effectively. For Privacy and Security Leadership Development, it was seen as a barrier that there are no mandated national standards for privacy and security officers. This barrier would be addressed by the development of core competencies for these staff as well. The Legal Barrier of persons involved in the exchange of health information fear breaking the law can be directly reduced by the providing staff with the sufficient and complete information they need in order to perform their functions.
- All types of information are impacted by this solution, and all domains impacted as well, as core competencies would be defined across the full spectrum of activities involved in the execution of HIE. All stakeholders, with the exception of QIOs, consumers and state government would not be impacted, as none of these stakeholders would have staff directly involved.

Solution (5): In addition to the need for a fully informed professional staff to execute and protect HIE, the SWG also determined as a priority a need to develop educational materials for consumers for providers to distribute.

- This solution directly responds to the barrier of Consumer Knowledge About Health Information. The public fears discrimination from the use of patient identifiers, and therefore could be reluctant to allow HIE. There is a general lack of understanding by the public of electronic health records and personal medical records in general, which could contribute also to this reluctance. There is a perception by the public concerning the lack of security of electronic records, which has been made even more public through security of information breaches in other sectors, such as banking. Materials developed to allay these fears and misperceptions, as well as provide consumers with the information they need concerning their rights in the matter of their health information are critical to moving implementation of HIE forward. As stated above, there are no mandated national standards for privacy and security officers, identified as a barrier in Privacy and Security Leadership Development. The defining of the core competencies for these staff identified as necessary in Solution 4, and the active participation of privacy and security officers in the development and delivery of consumer information for their organizations will ensure consumers are provided with clear and accurate assurances of their rights.
- This solution cross-cuts all types of information to be exchanged, as consumers would need full disclosure to make informed decisions regarding their health information. Domains most specifically involved would be information authorization (Domain 2), patient identification (Domain 3), state law restrictions (Domain 8), and information use and disclosure (Domain 9). Stakeholders impacted by this solution would be providers of any type of healthcare and consumers.

Solution (6): The Stark and Anti-kick back relief regulations allow for the donation of software and in some cases, hardware and training by hospitals to physician practices. In addition to this, it is proposed by the SWG that this federal relief be extended and promoted such that hospitals are allowed and possibly induced to provide physician practices that are serving economically disadvantaged populations with not only hardware, software, and training, but also additional technical resources to implement and support the technology.

- This solution addresses the variations in resource availability from organization to organization (In-house Resource for Information Management Barriers). In particular those entities that are unable to afford an EHR will not be able to effectively exchange health information and thus would not be able to contribute or benefit from HIE. This solution helps ensure these entities are provided the technology that will serve as the necessary conduit to the ILHIN and ultimately the NHIN.
- Provision of technology through the expansion of the Stark Amendment does not directly impact any specific domain of privacy and security of information. However, it does indirectly impact all domains as it will ensure those who have been historically underserved and suffer disproportionately as well as the providers who serve them will have the same benefits provided by HIE. Stakeholders impacted would include all those who provide healthcare and for whom the Stark Amendment applies, as well as consumers who have been historically underserved.

Solution (7): As efforts to develop and implement HIE move forward, systems and procedures for quality assurance and data integrity will naturally evolve out of technical standardization and staff education. As a priority to further the development of quality assurance for HIE, he SWG proposed to provide recommendations for multidisciplinary teams for acquisition of new IT

solutions to include at least Chief Information Officer, end users (clinical department, finance, quality management, HIM), and the security and privacy officer.

- This solution addresses a lack of organizational infrastructure for information edit checks, audits, and general quality assurance of health information that was identified as a barrier in the group Privacy and Security Leadership Development. Ensuring a full spectrum of stakeholders for decision-making and choosing of information management solutions will enable organizations to acquire systems with the greatest capacity to meet all needs, including that of data integrity and quality assurance.
- This solution is another cross-cutting solution, impacting all types of information that would be exchanged. The domain impacted would be Information Audits (Domain 6). Stakeholders impacted would be those with health information management systems that would provide information in an exchange. Exceptions would include consumers, law enforcement, professional associations, QIOs, state government and academic research organizations, although all these stakeholders would be positively impacted by any improvement in data integrity as would be afforded by application of quality assurance policies and procedures.

Solution (8): In December 2006, the EHRTF recommended that the Illinois Legislature adopt legislation charging the Illinois Department of Public Health (IDPH) with responsibility for advancing Illinois' EHR and HIE initiatives and requiring the Department to establish a public-private partnership with a new not-for-profit organization, named the Illinois Health Information Network (ILHIN) and governed by stakeholders in the health care system. The EHRTF Report proposed that the first few years of ILHIN's existence will be devoted to designing the state-level HIE, supporting pre-cursor HIE activities and pilot projects, and funding initiatives to foster EHR and HIE adoption. The ILHIN also will need to monitor and make recommendations to IDPH regarding the impact of state and federal legislation on Illinois EHRs. In conjunction with this proposal to establish a lead agency for HIE development in Illinois, the SWG proposed that legal staff with expertise in privacy and security to guide integrated state efforts be included in this lead state agency/organization.

- The inclusion of privacy and security expertise at the highest level of HIE developmental efforts in Illinois will address a number of barriers identified in the Legal Barriers. These barriers include persons involved in the exchange of health information fear breaking the law, the interpretation of laws concerning health information varies from organization to organization, and there is a lack of national guidelines for the interpretation of laws concerning health information. If the ILHIN is formed as recommended, it will be authorized to provide technical and organizational assistance toward the expansion and adoption of EHR use. Inclusion of legal technical assistance to both organizations as well as state agencies with health information statutory responsibility, will facilitate the development of consistent legislation, policies, and procedures. Guidelines for interpretation and application would more likely be standardized with this central authority approach. In Privacy and Security Leadership Development Barriers, that there are no mandated national standards for privacy and security officers, and there is a lack of centralized authority or organization for the privacy and security of health information would both be directly impacted by the creation of the ILHIN and the establishment of its legal expertise also. A central authority with legal expertise will also impact barriers in Staff Knowledge About Health Information Exchange Barriers (There is a lack of

ongoing education for staff to understand the results and/or ramifications of the release of health information), and Technology and Standards Barriers (There are no national requirements for information system interoperability; There is no standardization in security protocols and interfaces).

- All types of information for exchange would be impacted by this solution. The affected domains are state law restrictions (Domain 8), and information use and disclosure (Domain 9). All stakeholders would be impacted by a top-down approach to legal standardization and application of privacy and security expertise to HIE development.

As Illinois currently lacks a statewide infrastructure for electronic health information exchange, the SWG focused its efforts on analysis of root causes of barriers. This facilitated the development of cross-cutting solutions across barrier groups. The degree to which the solutions cross-cut barrier groups is seen in Matrix 1 below. Solutions with the greatest potential for cross-cutting impact would be for the development of professional standards for privacy and security officers, as well as the inclusion of privacy and security legal expertise in the lead agency for HIE development. Actions taken to meet these solutions would bring about a pervasive organizational infrastructure created specifically for privacy and security protection during all stages of HIE development, thus affecting most barriers and virtually all stakeholders.

- Matrix 1: Solutions to Barriers

Barrier (1): Organizational Culture Barriers
Barrier (2): Technology and Standards Barriers
Barrier (3): Staff Knowledge Barriers
Barrier (4): Consumer Knowledge Barriers
Barrier (5): In-House Resources Barriers
Barrier (6): Privacy and Security Leadership Barriers
Barrier (7): Global Market Barriers
Barrier (8): Legal Barriers

	Barriers							
Solution	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions	X	X			X			
Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary required (two factor identification).	X	X			X			
Define professional qualifications for privacy and security officers	X	X	X		X	X		X
Establish core competencies for staff education	X		X			X		
Develop educational materials for consumers for providers to distribute				X		X		

Solution	Barriers							
	1	2	3	4	5	6	7	8
Extend and promote, in discussion with State's Attorney General, national Stark and anti-kick back relief regulations, so those who are advantaged can support those who are disadvantaged.					X			
Provide recommendations for multidisciplinary teams for acquisition of new IT solutions						X		
Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts		X	X			X	X	X

- Matrix 2: Solutions to Domains

Domain (1): User/entity authentication
Domain (2): Information authorization and access controls
Domain (3): Patient and provider identification
Domain (4): Information transmission security or exchange protocols
Domain (5): Protection Against Improper Modification
Domain (6): Information Audits
Domain (7): Administrative and Physical Safeguards
Domain (8): State Law Restrictions
Domain (9): Information Use and Disclosure Policies

Solution	Domains								
	1	2	3	4	5	6	7	8	9
Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions	X	X	X	X	X	X	X	X	X
Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary required (two factor identification).			X						
Define professional qualifications for privacy and security officers		X		X		X	X	X	X
Establish core competencies for staff education	X	X	X	X	X	X	X	X	X
Develop educational materials for consumers for providers to distribute		X	X					X	X
Extend and promote, in discussion with State's Attorney General, national Stark and anti-kick back relief regulations, so those who are advantaged can support those who are disadvantaged.	X	X	X	X	X	X	X	X	X
Provide recommendations for multidisciplinary teams for acquisition of new IT solutions						X			
Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts								X	X

- Matrix 3: Stakeholders to Solutions

Solution (1): Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions
Solution (2): Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary required (two factor identification).
Solution (3): Define professional qualifications for privacy and security officers
Solution (4): Establish core competencies for staff education
Solution (5): Develop educational materials for consumers for providers to distribute
Solution (6): Extend and promote, in discussion with State's Attorney General, national Stark and anti-kick back relief regulations, so those who are advantaged can support those who are disadvantaged.
Solution (7): Provide recommendations for multidisciplinary teams for acquisition of new IT solutions
Solution (8): Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts

	Solutions							
Stakeholders	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1: Clinicians	X	X	X	X	X	X	X	X
2: Physician groups	X	X	X	X	X	X	X	X
3: Federal health facilities	X	X	X	X	X	X	X	X
4: Hospitals	X	X	X	X	X	X	X	X
5: Payers	X	X	X	X	X	X	X	X
6: Public Health agencies	X	X	X	X			X	X
7: Community clinics	X	X	X	X	X	X	X	X
8: Laboratories	X	X	X	X	X		X	X
9: Pharmacies	X	X	X	X	X		X	X
10: Long term care facilities	X	X	X	X	X		X	X
11: Homecare and Hospice	X	X	X	X	X		X	X
12: Law Enforcement	X	X		X				X
13: Professional associations	X	X		X				X
14: Academic research facilities	X	X		X				X
15: Quality improvement organizations	X	X						X
16: Consumers	X	X			X			X
17: State government	X	X						X
18: Homeless Shelters	X	X	X	X	X		X	X

- Matrix 4: Solutions to Feasibility Barriers

Feasibility Barrier (1): Cost of implementation
Feasibility Barrier (2): Lack of proven value of HIE

Feasibility Barrier (3): Unidentified funding streams
Feasibility Barrier (4): Complexity of systems and processes for implementation
Feasibility Barrier (5): Change aversion
Feasibility Barrier (6): Requirement for long-term organizational commitment
Feasibility Barrier (7): Indeterminate consensus among stakeholders
Feasibility Barrier (8): Unidentified resource availability

	Feasibility Barriers							
Solution	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions		X	X	X	X	X	X	X
Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary required (two factor identification).	X			X	X	X	X	X
Define professional qualifications for privacy and security officers				X	X	X	X	
Establish core competencies for staff education	X	X	X	X	X	X	X	X
Develop educational materials for consumers for providers to distribute					X	X	X	
Extend and promote, in discussion with State's Attorney General, national Stark and anti-kick back relief regulations, so those who are advantaged can support those who are disadvantaged.	X	X	X	X	X	X	X	X
Provide recommendations for multidisciplinary teams for acquisition of new IT solutions				X		X	X	
Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts				X	X	X	X	

- Matrix 5: Solution Types to Solutions

Solution (1): Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions
Solution (2): Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary required (two factor identification).
Solution (3): Define professional qualifications for privacy and security officers
Solution (4): Establish core competencies for staff education
Solution (5): Develop educational materials for consumers for providers to distribute
Solution (6): Extend and promote, in discussion with State's Attorney General, national Stark and anti-kick back relief regulations, so those who are advantaged can support those who are disadvantaged.
Solution (7): Provide recommendations for multidisciplinary teams for acquisition of new IT solutions

Solution (8): Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts

Solution Type	Solutions							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1: Governance-related solutions	X						X	X
2: Business arrangement solutions							X	
3: Technical solution		X					X	
4: Guidance/Education solutions that address misinterpretation issues			X	X	X			
5: Solutions that would require changes in existing state law/regulations						X		
6: Solutions that would require new state laws/regulations								X
7: Solutions that would address issues of non-compliance with state laws/regulations			X	X				X
8: Education solutions to address misinterpretations of state laws/regulations			X	X				
9: Solutions applicable to general privacy/security federal laws and regulations (e.g. HIPAA Privacy, HIPAA Security)								X
10: Solutions applicable to state programs (e.g., Medicaid)						X		
11: Solutions that would address issues of non-compliance with federal laws/regulations (such as non-compliance with HIPAA Privacy, HIPAA Security)			X	X				X
12: Education solutions to address misinterpretations of federal laws/regulations			X	X				
13: Solutions affecting Interstate Health Information Exchanges *NOTE*								

NOTE All the solutions proposed by the SWG were developed with a priority for interoperability development and/or support, and as such would impact any and all cross-state HIE. The choice as one of the prioritization criteria that solutions are in alignment with other state and national HIE efforts reinforced this approach to interoperable solutions development. No specific cross-state activity was addressed, however, as the primary focus of the group was on internal implementation of HIE for Illinois.

Section 5 - National-level Recommendations

Promulgation of national standards for interoperability. The Executive Order signed by President Bush in August 2006, entitled *Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs*, requires federal agencies and their health care contractors to promote the use of interoperable health information technology products, so that data can be easily shared. Two key principles are demonstrated by this executive order. First, government must take a leadership role by adopting interoperable systems. Second, the adoption of EHR is facilitated by making the use of interoperable EHR a requirement for health care providers to do business with government. On a national level, whatever can be done must be done to continue and expand the promulgation of technical standards as was done by this Executive Order.

Requests for clarification of HIPAA Privacy and Security requirements. In exchanging patient information for non-emergent treatment reasons, stakeholders have stated that they try to uphold the HIPAA "minimum necessary" guidelines. There is no clear definition of what "minimum necessary" should consist of in any given situation. The level of information provided varies not only from organization-to-organization but also between people within the same organization. Further, it appears that HIPAA's "minimum necessary" standard is being applied in practice to exchanges among providers for treatment purposes even though the HIPAA Privacy Rule does not require it. Similarly, it seems to be common practice to require the patient's written authorization in non-urgent information exchanges even though HIPAA does not require it for exchanges among providers. It may be that the state law restrictions generally prohibiting disclosure of special categories of health information without consent (e.g., for mental health, substance abuse, HIV and genetic test information) have contributed to these precautions and practices which pre-date HIPAA. Clarifications at a federal level for "minimally necessary" guidelines, and assistance in the promulgation of the guidelines are needed.

Documentation of Consent. Having a national uniform consent/authorization to release information would likely facilitate electronic exchange of information, both intra- and interstate.

Obtaining Consent/Authorization at Point of Service. Although HIPAA does not require health care providers to obtain consent or authorization to release information for treatment or payment purposes, a change to HIPAA requiring the provider to obtain the patient's legal permission authorizing release and any future release at the time of hospital admission or other initial point of service would likely facilitate future requests for release of that provider's information. Such practice would be consistent with what is viewed as an expanding practice among Illinois payors to obtain the individual's "disclosure authorization form" authorizing future releases to the insurer at the time of application, as is permitted by Illinois law. Making this a federal recommendation or standard would facilitate the interstate exchange of information.

Jurisdiction and Enforcement Issues. Noting the extensive protections in existing laws governing health care providers, insurers and others, and noting the demonstrated commitment that stakeholders have to maintaining patient confidentiality, there is a need to have more stringent requirements and sanctions in place to address business associates and others who may not read, understand, or take seriously the requirements of a business associate or subcontractor

agreement, and to otherwise deter other "bad actors" who may be outside the jurisdiction of existing laws. These concerns are amplified in the case of the overseas business partner who is not easily made subject to U.S. legal or contractual requirements. Providing additional deterrence on the federal level could facilitate and remove barriers to voluntary participation in an information exchange mechanism.

Maintaining Special Legal Protections and Ability to Segregate Different Categories of Information. A patient may be willing to authorize the release and future release of certain types of health information (for example, general treatment records) but not other types of health information (for example, drug or alcohol abuse treatment records, abortion records, or genetic testing information). Therefore, having the ability to electronically segregate, store, retrieve, and transmit different categories of information, while maintaining privacy and confidentiality protections, could facilitate electronic information exchange in several ways. First, patients may be more confident in participating in a RHIO or other exchange framework if special protections and the ability to exclude certain types of information from release are maintained. Second, having the ability to segregate or withhold information from general release may be required by laws that prohibit release of information unless certain circumstances exist (for example, a general subpoena or court order may permit release of some but not all information, as state law provides special requirements for mental health and developmental disabilities, alcohol/substance abuse, HIV and genetic testing information). Therefore, providers as well as consumers may be more willing to participate in electronic information exchange system if there are IT mechanisms that protect against unauthorized or illegal disclosures that could subject the provider to monetary or other penalties. Third, the ability to segregate and maintain special protections for categories of information that the federal and state legislatures and courts have found to require extraordinary protection is legally required absent wholesale preemption/revocation of such laws, and would also be necessary in order to be able to comply with new laws and changes to existing laws. The provision of model legislation for a national standardized approach to provide extraordinary protection would facilitate interstate exchange as well as compliance.

Changes to Stark and anti-kick back relief regulations. In order to expand the scope of the relief to target providers who serve the historically underserved, amend these regulations such that hospitals are allowed and possibly induced to provide physician practices that are serving economically disadvantaged populations with not only hardware, software, and training, but also additional technical resources to implement and support the technology.

Section 6 – Appendices

Appendix 1 - Barriers to the Implementation of e-HIE in Illinois

Analysis by the Variations Working Group revealed few barriers to electronic health information exchange, primarily because so little electronic exchange is occurring currently in Illinois. In order to have a more comprehensive list for solutions development, the SWG was asked to generate a random list of barriers to e-HIE in Illinois. These random barriers were then grouped into major barrier categories. Individual barriers to e-HIE were investigated then by the SWG to identify any possible root causes that could be exploited for effective solutions development.

- *This denotes a category of barrier*
    - *This denotes a barrier determined by the SWG*
        - *This denotes a root cause identified for the barrier, generated by asking "Why is this a barrier?"*

Problem Statement: There are barriers to e-HIE in Illinois

- Organizational Culture Barriers
    - Culture of physical/paper records
        - Workflow is designed for paper.
        - Paper provides provider a sense of security.
        - Paper provides proof of action.
        - Paper provides proof of ownership.
        - Paper is readily available (cheap).
    - Culture of ownership of data and not sharing it
        - Exchange of information between organizations is not universally accepted as appropriate.
        - Negative repercussions are feared if organization becomes more transparent by sharing information.
        - A negative impact on "bottom line" is feared if organization shares information.
        - Data of patients from underrepresented facilities/groups may be used inappropriately.
    - Culture of actions based on risk aversion/comfort rather than standards
        - Exchange of information between organizations is not universally accepted as appropriate.
        - Negative repercussions are feared if organization shares information based on network standards rather than internal risk assessment.
        - A negative impact on "bottom line" is feared if organizations shares information based on network standards rather than internal risk assessment.
    - Culture of market competition
        - A negative impact on "bottom line" is feared if organization shares information based on network standards rather than market analysis.
        - An open exchange of information may reduce competitive edge between providers and/or facilities.

- Culture of organization type, with variations due to clinics vs. hospitals, public vs. private, etc.
  - Protections to sensitive situations and information vary from organization type to organization type.
  - Protections against stigmas or other negative repercussions on patients vary from organization type to organization type.
  - Populations served vary from organization type to organization type.
- Culture of diminished value of staff continuing education
  - Staff education lacks priority in organizational plans.
  - Cheaper staff can be hired (recent grads); reduces organization obligation.

- Technology and Standards Barriers
  - There is a technical challenge to assure user authentication and successful use of system
    - There are many different technical methods available to authenticate users. A universal standard would have to be adopted in order to ensure interoperability between sites and users.
    - The different technical methods that exist to handle user authentication can be difficult to implement for health care providers with limited IT resources.
    - Current methods for strong authentication are difficult for consumers to use. Strong passwords are difficult for consumers but encryption keys are even more challenging. The financial industry is leading the adoption of strong authentication under FFIEC guidelines with limited success.
    - The interface for retrieving records would have to be standardized so that providers would not be trying to learn each individual system.
    - The electronic signature for an information system can be a problem.
    - There are far more users of information system than there are technical assistants available to address technical issues.
    - Technical documentation for information system is usually long and not user friendly.
    - Staff may occasionally use other log-on ID's for information system.
    - Staff may not sign out of information system properly.
    - Staff may not receive proper training in user authentication and system use.
  - There is a technical challenge to patient identification
    - Providers do not use the same identifiers for patients. This would require the creation of these unique identifiers and a massive master patient index associating them with the provider identifier.
    - Many patients have the same name. Some may have the same name and address. Families use names interchangeably.
    - Staff do not always validate patient identification information.
    - A picture ID may not always be required for patient identification.
    - There are many issues around duplicate medical record numbers.
    - Some patients don't have appropriate ID's.
    - Some patient may use other ID because they don't have the coverage.

- There are no national requirements for information system interoperability
  - HL7 is a health care interface protocol for transferring data between disparate systems but has only be accepted as an ANSI standard. This allows for many variations on the implementation of the standard by each health care software vendor within their software.
  - This lack of an enforced standard has driven the complexity of creating and maintaining interfaces up. Most providers do not have the IT resources available and rely solely on the vendors for this service. This has driven the cost of interfaces up substantially and can render them financially impractical.
  - HL7 does not have sufficient security built into the system to be used on a grand scale. The intention of this interface protocol was to provide means for systems to transfer information on a network that was already secure. There are no standards defined for encryption, authentication or message integrity checking. This standard would have to be modified to add these capabilities or third party security products would be needed to supplement.
  - The electronic health record is still new.
  - Technology advancements are much greater than the speed of learners for many of the users.
  - New systems will be as disconnected as current systems.
  - There are delays in congress concerning health care information technology.
- There are insufficient standards for data elements
  - The patient record is usually made up of data from different specialized, ancillary systems. These systems all have proprietary data structures and elements to suite their specific applications. These elements would have to be standardized across all health care software vendors to have support for a combined record. Various data elements required for proper treatment may not be available without standardized elements or worse they could be in different formats creating a possibility of medical errors.
  - There are currently multiple standard sets, with some variation in definitions.
  - There are emerging data elements (new items needed).
- There is no standardization in security protocols and interfaces
  - There are numerous standards for secure communication but one will need to be selected for the specific purpose of security protocols and interfaces.
  - HL7 has no provisions for security or integrity and this should be added for this implementation.
  - There are delays from security/standards groups.
  - There are delays in congress concerning health care information technology.
  - There is competition among software vendors.
  - There is massive data in huge legacy systems that must be considered.
- There is a technical challenge for the national implementation of ICD-10

        - The health care software vendors have not all adopted ICD-10 codes as of yet. Diagnosis codes based on previous ICD-9 codes will not match the ICD-10 codes causing conflicting data between all of the systems.
        - There are delays in congress concerning the passage of ICD-10.
        - There is strong opposition from payors and vendors who have to pay for changes to system software.
    - Organizations lack adequate infrastructure and role delineation for the development and enforcement of security, privacy, and information management policies and procedures
        - There is an enormous gap in the security conscience of the health care provider community. According to a HIMMS survey in 2005, only 53% of providers were declaring their compliance with the HIPAA security rules. There cannot be variations in compliance with security regulations between providers or a shared record will create opportunities for massive abuse and fraud.
        - HIPAA security has not created the motivation for providers to seek out solutions to security problems. There have only been 3 HIPAA security convictions in almost 3 years.
        - HIPAA security officers are typically selected from unwitting candidates who happen to be familiar with a PC but not appropriate risk identification and mitigation techniques.
        - Security, Privacy, Policy, and Procedures are interrelated.
        - There is competition among health care leaders that have skills in security, privacy and health information management.
        - There is no consistency of how security and privacy management should be handled in an institution (power issue).
    - There is a lack of secured websites and use of secured e-mail
        - The underutilization of secured website and encrypted e-mail is a result of implementations without appropriate security personnel or procedures.
        - Secure e-mail is more difficult for the provider to utilize so it is often discarded as a solution.
        - There are many different standards for secure e-mail available and one would have to be chosen as a standard. If a standard existed, it may provide the motivation necessary for providers to utilize it.
        - There is a lack of ongoing education regarding the security of websites and e-mail.
        - There are multiple choices for e-mail.
        - Firewalls do not exist in every organization.
        - There is insufficient training on how to send secure e-mail.
        - E-mail is so easy to share.
    - There is no existing infrastructure in Illinois for the electronic exchange of information, such as a RHIO
        - A RHIO would have to define the standards that are addressed in this document. Defining these standards may be simplified by working in smaller environments and developing feedback for further integration projects.

        - There are no strong private groups that share information currently in a regional health information exchange.
        - There is a lack of funding for regional exchange of health information.
        - There is a lack of trust for the development of RHIOs.
        - There is a lack of leadership for the development of RHIOs.

- Staff Knowledge About Health Information Exchange Barriers
    - There is a lack of ongoing education for staff to understand the results/ramifications of the release of health information
        - There is a general lack of understanding by health care staff of security issues around technology. The technology has become so pervasive that security implications aren't even considered.
        - There are limited funds for education and training of health care staff in health information security and privacy.
        - There is a lack of leadership for education of health care staff in health information security and privacy.
        - There is a perceived lack of funding for education of health care staff in health information security and privacy.
        - There have been no real sanctions on inappropriate release of protected health information.
    - There is a lack of understanding by staff of what is appropriate and what is not in the exchange of health information
        - The understanding of appropriate information exchange is critical to avoid breaches of confidentiality. These breaches would undermine public support and confidence in any type of health information exchange.
        - There is a lack of ongoing educational funding for staff education.
        - There is a variation in leadership practices regarding staff education.
        - There is a lack of staff education provided by facilities.
        - Staff are not aware of appropriate sources to consult for security and privacy of health information.
    - There is a lack of ways to share educational materials
        - Some educational materials may be proprietary.
        - There are ways of sharing educational material, but a lack of information/leadership to execute.
    - There is a lack of standardized educational materials that have been developed for sufficient evaluation of effectiveness
        - Educational needs vary by organization, individuals, geographic, and available resources.
        - No specific group has been identified as the industry authority to consult regarding educational material for health information management.
        - Those who have developed educational material for health information management have not been asked to share information with others.
        - There is resistance to use information for education in health information management that is developed by others.

- Consumer Knowledge About Health Information Barriers

- There is a perception by the public concerning the lack of security of electronic records
  - There is a perception about the insecurity of electronic records because there have been stories about major security breaches in the media. The recent UCLA breach is an example. Identity theft is the fastest growing crime in America. Over 9 million people reported identity theft in 2005 alone.
  - The public is fearful of how information may be used against them.
- The public fears discrimination from the use of patient identifiers
  - There is a general anxiety around health information being used as an employment or health insurance screen. This anxiety will have to be taken into account with any solution being considered.
- There is a general lack of understanding by the public of electronic health records and personal medical records
  - There is not enough education for consumers.

- In-house Resources for Information Management Barriers
  - There are variations between shifts in both practices and available resources
    - Shift variation in practice is related to the educational barrier listed previously. All staff need to be educated on appropriateness of information, procedures for access and security of the records.
    - The majority of healthcare resources are on the first shift, consistent with normal business hours.
  - There are insufficient resources for language diversity to assure provision of information, and comprehension of information given
    - The personal record needs to be accessible to everyone in order to be successful.
    - Staff that speak two languages/secondary languages are not frequently targeted in healthcare settings.
  - There are variations in resource availability from organization to organization
    - Providers without the appropriate resources will not be able to participate in the shared record. These resources could be defined as monetary or technical.
    - There is a lack of funds and/or resources in some organizations.
    - Resources are limited in rural areas.
    - Resources are limited in poor communities.
  - There are variations in information technology development from organization to organization
    - Some organizations do not have any form of electronic data in which to interface. Most organizations do not have a full EMR implemented yet.
    - There is a lack of funds for across the board information technology development.
    - Some organizations lack the ability to attract professional resources due to geographics.

- Privacy and Security Leadership Development Barriers

- Organizations have dual functions in legal counsel and privacy officer, which spreads staff too thin for effectiveness
  - Appropriate policies and procedures for privacy and security may not get created or adhered to without proper attention. This could lead to security breaches or inappropriate access.
- Organizations exclude privacy experts in information technology solutions up front, and instead include them in the back end of the solutions process
  - It is always more effective to build privacy and security into a solution than to tack it on after implementation. These implementations often have other flaws that cannot be addressed after the implementation has been completed.
  - There is a lack of awareness of who are the privacy experts i.e. HIM Professionals, other.
- There is a general lack of security officers for information technology
  - The expertise in IT security is essential to performing risk analysis and mitigation. This is a rapidly evolving field that requires people with a detailed knowledge of information security. The potential for security breaches will increase substantially without oversight from these types of professionals.
  - The security officers concept/position is still evolving.
- There is a lack of credentialing in both privacy and security officers
  - The designated HIPAA Security Officer in some organizations was only chosen because they had a working knowledge of computers. Computer skill is only a portion of information security. It requires a skill set that includes risk analysis, legal procedures and legislation as well.
  - Healthcare organizations in rural areas may be partly at risk due to lack of healthcare credentialing.
  - Organizations in rural areas may not attract professional resources.
  - Credentialing is still fairly new for the privacy and security of health information profession.
- There are no mandated national standards for privacy and security officers
  - Anyone can be a privacy or security officer. The people in these positions have had these new duties added on to their existing role in the organization. They have had no formal training and may not even understand the ramifications of their new position.
  - The public will gain more confidence in a solution if it is created by people with credentials in privacy and security.
  - The probability of missing potential flaws in privacy and security management increases with untrained individuals.
  - This national standard for privacy and security officers should also include the reporting structure of these positions. Some of the people that have had this role added to their existing job may not be in a position to actually effect policy.
  - HIPAA provides the mandatory rules.
  - Management practices for privacy and security officers vary.
  - Variations are not consistent from privacy and security officer position.

- There is a lack of centralized authority or organization for the privacy and security of health information
  - The policy decisions concerning security protocols around a combined record need to be centralized so that the associated risks can be properly identified and managed. It would cause conflicts to have a violation in one county be allowable in another for example.
  - Privacy and security are still legal matters and very complex .
  - Laws are constantly changing.
  - There are multiple organizations involved in the privacy and security of health information (CMS, JCAHO, etc.)
- There is a lack of organizational infrastructure for information edit checks, audits, and general quality assurance of health information
  - There would need to be some type of random audit checking to determine if access to a record was appropriate. Providers would need to have a clinical need to view information or there would be violations from the curious to the criminal. How many people would access the records of a VIP if they were available electronically?
  - There are multiple health information quality assurance systems.
  - There are multiple people involved in the development of quality assurance of health information.
  - Key players are often missing in the planning strategy for quality assurance of health information.

- Global Market Barriers
  - Offshore organizations' access to health information complicates user authentication and access rights
    - Many organizations use offshore services that have access to health information. International privacy laws do not exist and holding these organizations accountable can be difficult.
    - The offshore services companies are attempting to comply with many different privacy laws around the world. This is a difficult task because of the differences in legislation between countries.
    - There is a disconnect between actual users of the system and the system experts.
    - Procedures for privacy and security protection offshore may differ from those in this country.
  - Competitive market forces in software development complicate standardized information exchange solutions
    - Health care software vendors have been known to add expenses or complicate exchanging information with another vendor in order to steer a provider into purchasing their product. They often do not allow the provider to attempt the interface because of the revenue that can be generated from this service.
    - Competitive market forces in software development will add costs to the participation of the provider in the electronic record.

- Legal Barriers
  - Persons involved in the exchange of health information fear breaking the law
    - If a provider has not received proper education in privacy and security protection they tend to be ultra conservative with their responses to a request for exchange of information. They are not sure of the legality of an exchange so they won't comply.
    - There are penalties and consequences of inappropriate exchange of health information, and you may lose your job.
    - The organization could be fined for inappropriate exchange of health information.
    - Staff are not trained in appropriate exchange of health information.
  - The interpretation of laws concerning health information varies from organization to organization
    - The HIPAA security legislation language is extremely vague. This causes speculation by each organization and they all end up with a different interpretation. This has been magnified by the fact that there have only been 3 cases on which to determine case law and add definition to the legislation.
  - There is a lack of national guidelines for the interpretation of laws concerning health information
    - The HIPAA security legislation language is extremely vague. This causes speculation by each organization and they all end up with a different interpretation. This has been magnified by the fact that there have only been 3 cases on which to determine case law and add definition to the legislation.
  - Legal expertise resides in organizations outside of health information management staff
    - Provider staff need education on the operational privacy and security procedures that directly affect them. They will be making the daily decisions that affect the privacy and security of health information. These decisions may not be appropriate or in line with policies and procedures if the expertise is not available to them.
    - Health information management staff often times do not have direct access to the legal expertise.
    - Health information management may have to go through two or more persons to access legal expertise.
    - Legal expertise costs money and is expensive.

Appendix 2 - Root Causes of Barriers to the Implementation of e-HIE in Illinois

Barriers to e-HIE areas were investigated by the SWG to look into any possible root causes that could be exploited for effective solutions development. Root causes for each barrier in all barrier groups were identified by facilitated discussion, as discussed in Appendix: Barriers to the Implementation of e-HIE in Illinois. Then the SWG grouped the root causes into related areas for solutions development and developed statements to reflect the desired end-state outcomes for the solutions.

The following eight solution areas were identified:

- Benefits of regional exchange of health information
- Technology standards development
- Professional standards development
- Consumer education
- Staff education
- Inclusion of economically disadvantaged
- Quality assurance
- Legislation and enforcement

The individual root causes identified by the SWG were grouped as follows into specific solution areas.

Causes which would be addressed by proof of benefits of regional information exchange:

- Some organizations do not have any form of electronic data in which to interface.
- Most organizations do not have a full EMR implemented yet.
- Workflow is designed for paper.
- Paper provides provider a sense of security.
- Paper provides proof of action.
- Paper provides proof of ownership.
- Paper is readily available (cheap).
- Negative repercussions are feared if organization shares information based on network standards rather than internal risk assessment.
- A negative impact on “bottom line” is feared if organizations shares information based on network standards rather than internal risk assessment.
- A negative impact on “bottom line” is feared if organization shares information based on network standards rather than market analysis.
- An open exchange of information may reduce competitive edge between providers and/or facilities.
- Protections against stigmas or other negative repercussions on patients vary from organization type to organization type.
- Negative repercussions are feared if organization becomes more transparent by sharing information.
- A negative impact on “bottom line” is feared if organization shares information.

- Exchange of information between organizations is not universally accepted as appropriate.
- Exchange of information between organizations is not universally accepted as appropriate.
- A RHIO would have to define the standards that are addressed in this document.
- Defining these standards may be simplified by working in smaller environments and developing feedback for further integration projects.
- There are no strong private groups that share information currently in a regional health information exchange.
- There is a lack of funding for regional exchange of health information.
- There is a lack of trust for the development of RHIOs.
- There is a lack of leadership for the development of RHIOs.

Desired end-state outcome for solutions to these causes: **Benefits for regional electronic exchange of health information are demonstrated and promoted.**

Causes which would be addressed by adoption of technical standards:

- The personal record needs to be accessible to everyone in order to be successful.
- Populations served vary from organization type to organization type.
- Data of patients from underrepresented facilities/groups may be used inappropriately.
- Providers do not use the same identifiers for patients. This would require the creation of these unique identifiers and a massive master patient index associating them with the provider identifier.
- Many patients have the same name. Some may have the same name and address. Families use names interchangeably.
- A picture ID may not always be required for patient identification.
- There are many issues around duplicate medical record numbers.
- Some patients don't have appropriate ID's.
- Some patient may use other ID because they don't have the coverage.
- The policy decisions concerning security protocols around a combined record need to be centralized so that the associated risks can be properly identified and managed. It would cause conflicts to have a violation in one county be allowable in another for example.
- The patient record is usually made up of data from different specialized, ancillary systems. These systems all have proprietary data structures and elements to suite their specific applications. These elements would have to be standardized across all health care software vendors to have support for a combined record. Various data elements required for proper treatment may not be available without standardized elements or worse they could be in different formats creating a possibility of medical errors.
- There are emerging data elements (new items needed).
- HL7 is a health care interface protocol for transferring data between disparate systems but has only be accepted as an ANSI standard. This allows for many variations on the implementation of the standard by each health care software vendor within their software.
- The health care software vendors have not all adopted ICD-10 codes as of yet. Diagnosis codes based on previous ICD-9 codes will not match the ICD-10 codes causing conflicting data between all of the systems.

- There are delays in congress concerning the passage of ICD-10.
- There is massive data in huge legacy systems that must be considered.
- It is always more effective to build privacy and security into a solution than to tack it on after implementation. These implementations often have other flaws that cannot be addressed after the implementation has been completed.
- There are currently multiple standard sets, with some variation in definitions.
- This lack of an enforced standard has driven the complexity of creating and maintaining interfaces up. Most providers do not have the IT resources available and rely solely on the vendors for this service. This has driven the cost of interfaces up substantially and can render them financially impractical.
- HL7 does not have sufficient security built into the system to be used on a grand scale. The intention of this interface protocol was to provide means for systems to transfer information on a network that was already secure. There are no standards defined for encryption, authentication or message integrity checking. This standard would have to be modified to add these capabilities or third party security products would be needed to supplement.
- New systems will be as disconnected as current systems.
- The underutilization of secured website and encrypted e-mail is a result of implementations without appropriate security personnel or procedures.
- Secure e-mail is more difficult for the provider to utilize so it is often discarded as a solution.
- There are many different standards for secure e-mail available and one would have to be chosen as a standard. If a standard existed, it may provide the motivation necessary for providers to utilize it.
- There are multiple choices for e-mail.
- Firewalls do not exist in every organization.
- There are many different technical methods available to authenticate users. A universal standard would have to be adopted in order to ensure interoperability between sites and users.
- The different technical methods that exist to handle user authentication can be difficult to implement for health care providers with limited IT resources.
- Current methods for strong authentication are difficult for consumers to use. Strong passwords are difficult for consumers but encryption keys are even more challenging. The financial industry is leading the adoption of strong authentication under FFIEC guidelines with limited success.
- The electronic signature for an information system can be a problem.
- There are numerous standards for secure communication but one will need to be selected for the specific purpose of security protocols and interfaces.
- HL7 has no provisions for security or integrity and this should be added for this implementation.
- There are delays from security/standards groups.
- Health care software vendors have been known to add expenses or complicate exchanging information with another vendor in order to steer a provider into purchasing their product. They often do not allow the provider to attempt the interface because of the revenue that can be generated from this service.

- Competitive market forces in software development will add costs to the participation of the provider in the electronic record.
- There is a lack of funds for across the board information technology development.
- There is strong opposition from payors and vendors who have to pay for changes to system software.
- Many organizations use offshore services that have access to health information.
- There is competition among software vendors.
- The offshore services companies are attempting to comply with many different privacy laws around the world. This is a difficult task because of the differences in legislation between countries.
- Procedures for privacy and security protection offshore may differ from those in this country.

Desired end-state outcome for solutions to these causes: **Technical standards for electronic health information exchange are developed and adopted.**

Causes which would be addressed by adoption of professional development standards:

- There is a disconnect between actual users of the system and the system experts.
- Staff that speak two languages/secondary languages are not frequently targeted in healthcare settings.
- Some organizations lack the ability to attract professional resources due to geographics.
- Providers without the appropriate resources will not be able to participate in the shared record. These resources could be defined as monetary or technical.
- Legal expertise costs money and is expensive.
- Protections to sensitive situations and information vary from organization type to organization type.
- There is a lack of awareness of who are the privacy experts i.e. HIM Professionals, other.
- Appropriate policies and procedures for privacy and security may not get created or adhered to without proper attention. This could lead to security breaches or inappropriate access.
- Anyone can be a privacy or security officer. The people in these positions have had these new duties added on to their existing role in the organization. They have had no formal training and may not even understand the ramifications of their new position.
- This national standard for privacy and security officers should also include the reporting structure of these positions. Some of the people that have had this role added to their existing job may not be in a position to actually effect policy.
- Management practices for privacy and security officers vary.
- Variations are not consistent from privacy and security officer position.
- The expertise in IT security is essential to performing risk analysis and mitigation. This is a rapidly evolving field that requires people with a detailed knowledge of information security. The potential for security breaches will increase substantially without oversight from these types of professionals.
- The security officers concept/position is still evolving.
- The designated HIPAA Security Officer in some organizations was only chosen because they had a working knowledge of computers. Computer skill is only a portion of

information security. It requires a skill set that includes risk analysis, legal procedures and legislation as well.

- Credentialing is still fairly new for the privacy and security of health information profession.
- There would need to be some type of random audit checking to determine if access to a record was appropriate. Providers would need to have a clinical need to view information or there would be violations from the curious to the criminal. How many people would access the records of a VIP if they were available electronically?
- There is a general lack of understanding by health care staff of security issues around technology.
- HIPAA security officers are typically selected from unwitting candidates who happen to be familiar with a PC but not appropriate risk identification and mitigation techniques.
- Security, Privacy, Policy, and Procedures are interrelated.
- There is competition among health care leaders that have skills in security, privacy and health information management.
- E-mail is so easy to share.
- There are far more users of information system than there are technical assistants available to address technical issues.

Desired end-state outcome for solutions to these causes: **Professional standards for privacy and security leadership are developed.**

Causes which would be addressed by standardization of staff education:

- Shift variation in practice is related to the educational barrier listed previously. All staff need to be educated on appropriateness of information, procedures for access and security of the records.
- The majority of healthcare resources are on the first shift, consistent with normal business hours.
- Provider staff need education on the operational privacy and security procedures that directly affect them. They will be making the daily decisions that affect the privacy and security of health information. These decisions may not be appropriate or in line with policies and procedures if the expertise is not available to them.
- If a provider has not received proper education in privacy and security protection they tend to be ultra conservative with their responses to a request for exchange of information. They are not sure of the legality of an exchange so they won't comply.
- There are penalties and consequences of inappropriate exchange of health information, and you may lose your job.
- Staff are not trained in appropriate exchange of health information.
- Staff education lacks priority in organizational plans.
- Cheaper staff can be hired (recent grads); reduces organization obligation.
- The probability of missing potential flaws in privacy and security management increases with untrained individuals.
- The technology has become so pervasive that security implications aren't even considered.

- There are limited funds for education and training of health care staff in health information security and privacy.
- There is a lack of leadership for education of health care staff in health information security and privacy.
- There is a perceived lack of funding for education of health care staff in health information security and privacy.
- Educational needs vary by organization, individuals, geographic, and available resources.
- No specific group has been identified as the industry authority to consult regarding educational material for health information management.
- Those who have developed educational material for health information management have not been asked to share information with others.
- There is resistance to use information for education in health information management that is developed by others.
- The understanding of appropriate information exchange is critical to avoid breaches of confidentiality. These breaches would undermine public support and confidence in any type of health information exchange.
- There is a lack of ongoing educational funding for staff education.
- There is a variation in leadership practices regarding staff education.
- There is a lack of staff education provided by facilities.
- Staff are not aware of appropriate sources to consult for security and privacy of health information.
- Some educational materials may be proprietary.
- There are ways of sharing educational material, but a lack of information/leadership to execute.
- There is an enormous gap in the security conscience of the health care provider community. According to a HIMMS survey in 2005, only 53% of providers were declaring their compliance with the HIPAA security rules. There cannot be variations in compliance with security regulations between providers or a shared record will create opportunities for massive abuse and fraud.
- The electronic health record is still new.
- Technology advancements are much greater than the speed of learners for many of the users.
- There is a lack of ongoing education regarding the security of websites and e-mail.
- There is insufficient training on how to send secure e-mail.
- The interface for retrieving records would have to be standardized so that providers would not be trying to learn each individual system.
- Technical documentation for information system is usually long and not user friendly.
- Staff may occasionally use other log-on id's for information system.
- Staff may not sign out of information system properly.
- Staff may not receive proper training in user authentication and system use.
- Staff do not always validate patient identification information.

Desired end-state outcome for solutions to these causes: **Staff education is standardized**

Causes which would be addressed by consumer education:

- There is a general anxiety around health information being used as an employment or health insurance screen. This anxiety will have to be taken into account with any solution being considered.
- There is not enough education for consumers.
- There is a perception about the insecurity of electronic records because there have been stories about major security breaches in the media. The recent UCLA breach is an example. Identity theft is the fastest growing crime in America. Over 9 million people reported identity theft in 2005 alone.
- The public is fearful of how information may be used against them.
- The public will gain more confidence in a solution if it is created by people with credentials in privacy and security.

Desired end-state outcome for solutions to these causes: **Consumer education is essential for implementation.**

Causes which would be addressed by inclusion of economically disadvantaged healthcare groups in information exchange development:

- There is a lack of funds and/or resources in some organizations.
- Resources are limited in rural areas.
- Resources are limited in poor communities.
- Healthcare organizations in rural areas may be partly at risk due to lack of healthcare credentialing.
- Organizations in rural areas may not attract professional resources.

Desired end-state outcome for solutions to these causes: **Health care groups that are economically disadvantaged are included in e-HIE and its development**

Causes which would be addressed by development of quality assurance for information exchange:

- There are multiple health information quality assurance systems.
- There are multiple people involved in the development of quality assurance of health information.
- Key players are often missing in the planning strategy for quality assurance of health information.

Desired end-state outcome for solutions to these causes: **Quality assurance is an integral part of organizational structure.**

Causes which would be addressed by development of clear, complete and timely legislation and enforcement:

- International privacy laws do not exist and holding these organizations accountable can be difficult.
- Health information management staff often times do not have direct access to the legal expertise.

- Health information management may have to go through two or more persons to access legal expertise.
- The organization could be fined for inappropriate exchange of health information.
- The HIPAA security legislation language is extremely vague. This causes speculation by each organization and they all end up with a different interpretation. This has been magnified by the fact that there have only been 3 cases on which to determine case law and add definition to the legislation.
- HIPAA provides the mandatory rules.
- Privacy and security are still legal matters and very complex .
- Laws are constantly changing.
- There are multiple organizations involved in the privacy and security of health information (CMS, JCAHO, etc.).
- There have been no real sanctions on inappropriate release of protected health information.
- HIPAA security has not created the motivation for providers to seek out solutions to security problems. There have only been 3 HIPAA security convictions in almost 3 years.
- There is no consistency of how security and privacy management should be handled in an institution (power issue).
- There are delays in congress concerning health care information technology.

Desired end-state outcome for solutions to these causes: **Legislation and enforcement is clear, complete and timely**

Appendix 3 - Solutions for Root Causes of Barriers to the Implementation of e-HIE in Illinois

After analysis of the root causes for barriers to the implementation of e-HIE in Illinois as to end-state outcomes for solutions to achieve, specific solutions were generated by discussion with members of the SWG, as well as with the LWG and HSC in a joint meeting to discuss education and legislation areas.

Solutions to achieve: Benefits of electronic health information exchange are demonstrated and promoted. Three areas for development were identified by the SWG: 1) Benefits of electronic information need to be quantified (including funding) and support provided for incremental development; 2) Benefits of exchange of information need to be determined and promoted; and 3) Regional exchange of information needs to be formalized, certified or accredited, and funded

- Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions
- Develop and distribute a standardized approach for cost-benefit analysis to stakeholders for free or low cost
- Develop "marketing" tools for providers on benefits
- Analyze available software in non-endorsement way to provide information in a comparative analysis
- Identify state funding streams for implementation
- Identify federal funding streams for implementation
- Provide a resource that compiles available grant funding streams
- Create the Illinois Health Information Network (ILHIN)

Solutions to achieve: Technical standards for electronic health information exchange are developed and adopted. Five areas for development were identified by the SWG: 1) Technical standards for patient identification and authentication are universally adopted; 2) Data and vocabulary standards need to be universal and formalized; 3) Standards need to be developed for user-friendly and universal secure communications and e-HIE; 4) Standards for interoperability need to be reconciled; 5) Standards need to be compatible with global standards

- Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary required (two factor identification).
- Provide personal digital certificates to patients
- Establish techincial standards for networks, similar to other IEEE standards, for identification algorithms for patient identification
- Develop interface engine for translating medical record identifiers across providers
- Adopt and promulgate for Illinois HITSP Interoperability specifications (ANSI): “Functional Requirements for Nationwide Health Information Network” or other appropriate standards
- Determine the applicability CCHIT certification of software vendors

Solutions to achieve: Professional standards for privacy and security leadership are developed

- Define professional qualifications for privacy and security officers
- Define organizational reporting structure for privacy and security officers to ensure accountability and responsibility
- Expand credentialing to licensure such as for other allied health professionals
- Standardize certification curriculum (CISSP from ISC (ISO), GSEC from SANS)
- Create more qualified professionals for security and privacy leadership (other than on-the-job-training) through a provided or subsidized training program

Solutions to achieve: Consumer education is essential for implementation

- Develop educational materials for providers to distribute
- Establish state lead to get message out on benefits in both print and other media
- Involve private sector and other stakeholders in message development
- Establish responsibility for patient education at level of delivery
- Engage specialty organizations, e.g. AARP
- Establish "core competencies" for patient education, including privacy rights
- Address the public's focus on identity theft issues

Solutions to achieve: Staff education is standardized

- Establish schedule for training, e.g. as for annual HIPAA training
- Establish core competencies
- Provide for privacy and security knowledge at the highest levels of organizations
- Provide information resources so that technology is used to overcome HIPAA "myths"
- Include in core competencies, for both routine staff as well as management, education in regulatory matters specific to exchange of health information
- Provide policy development standards to maximize/optimize organizational participation and buy-in
- Include privacy and security competencies in credentialing and licensing requirements
- Recommend minimum levels of continuing education/clock hours for competency training

Solutions to achieve: Health care groups that are economically disadvantaged are included in e-HIE and its development

- Expand and promote, in discussion with State's Attorney General, national Stark and anti-kick back relief regulations, so those who are advantaged can support those who are disadvantaged.
- Provide pressure/incentives on/for vendors to provide technical support for economically disadvantaged
- Leverage ILHIN sanctions against vendors who fail to support or don't fulfill contractual obligations
- Obtain special fee structures for broadband connectivity in rural areas (telecommunications service relief); and expand tele-health initiatives to both rural and densely populated urban areas
- Exploit other ways of information exchange for disease management (other than internet, such as cable and satellite connectivity), especially in densely populated areas

- Certify ASPs, to legitimize their functions, further the ASP model, and reduce costs of implementation/acquisition
- Provide special attention to underserved and rural providers in all HIT educational efforts
- Address professional shortages with targeted outreach, such as was done in the historical AHEC program for medical professionals with medical school training in outreach areas of Rockford, Peoria, Champaign
- Provide training sessions for clinical administrators for HIT - onsite and/or remote
- Provide grant-writing assistance
- Provide technical assistance
- Obtain unbiased assessment of national DOQ-IT program to gain better understanding of what is possible to accomplish, and determine expansion potential of program
- Investigate public/private obstacles to DOQ-IT for QIOs to adopt, evaluate and support with federal and state incentives/projects
- Push out HIE to poor urban areas
- Expand scope of licensure for nurse practitioners
- Investigate regional approach to HIT support
- Include in Medicaid conditions of participation the requirement for access to a credentialed professional for privacy and security function

Solutions to achieve: Quality assurance is an integral part of organizational structure

- Require electronic "chart" pulls for accreditation
- Provide recommendations for vendor selection include standards for increasing the ease of audit function for data integrity
- Provide recommendations for vendor selection include standards for increasing the ease of audit function for legal integrity
- Require routine quality assurance reviews for accreditation
- Provide recommendations for multidisciplinary teams for acquisition of new IT solutions to include at least CIO, end users (clinical department, finance, quality management, HIM), security/privacy officer

Solutions to achieve: Legislation and enforcement is clear, complete and timely

- Enforce penalties for breaches and other violations
- Identify “wrong-doers” and what is keeping them from following the regulations
- Develop laws that are clear and succinct
- Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts
- Standardize state approach to national approach
- Assess State’s regulations in terms of other states’ regulations or any proposed “model” legislation
- Encourage flexibility in regulations to allow for changing technology
- Begin regulatory review with “special” categories of health information for national standardization
- Establish security standards body, with well-defined authority and responsibilities

Appendix 4 – Prioritization of Solutions for the Implementation of e-HIE in Illinois

A survey was created to obtain input from the SWG, LWG, and HSC members on the ranking of all of the solutions generated based on the following criteria:
(A) Maximize patient care and outcomes [1.0]
(B) Maximize feasibility [0.8]
(C) Maximize privacy and security protection [0.7]
(D) Maximize cost effectiveness [0.5]
(E) Achieve alignment with national and other state activities [0.5]
(F) Have reduced dependency on other activities [0.3]

These criteria were developed by consensus discussion, and then weighted by nominal group technique in a joint meeting between the SWG, LWG and HSC. The relative weight scores of each criterion are indicated in the brackets above.

Because the solution area for the inclusion of economically disadvantaged healthcare groups had so many possible solutions generated by discussion, the number of choices for this solution area was reduced by nominal group technique from 17 choices to 9 choices for prioritization, without any reference to specific criteria. All other solution areas had all generated solutions ranked according to the criteria.

Through the use of an online survey, members of the groups individually ranked each solution against each criterion, giving the highest rank to the solution which met the criterion most, and the lowest rank to the solution which met the criterion the least. The score for the highest rank was equal to the total number of choices for the given solution area. All rank values for each solution were then added, and the solutions were then consensus ranked based on the total ranking score. To achieve the final prioritization score, each solution's consensus rank value was multiplied by the respective criterion weight score, and all weighted ranks were added for a total, as indicated in the tables below. The solution with the highest consensus prioritization score for each solution area was selected for extended analysis in the Interim Assessment of Solutions Report.

Consensus ranking of solutions to achieve:

Benefits of regional exchange of health information	**Weighted Criteria**						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions	8(1.0)	7(0.8)	8(0.7)	4(0.5)	8(0.5)	8(0.3)	27.6
Develop and distribute a standardized approach for cost-benefit analysis to stakeholders for free or low cost	7(1.0)	8(0.8)	5(0.7)	6(0.5)	5(0.5)	7(0.3)	24.5
Develop "marketing" tools for providers on benefits	1(1.0)	5(0.8)	7(0.7)	5(0.5)	6(0.5)	6(0.3)	17.2

Benefits of regional exchange of health information	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Analyze available software in non-endorsement way to provide information in a comparative analysis	3(1.0)	2(0.8)	3(0.7)	1(0.5)	7(0.5)	5(0.3)	12.2
Identify state funding streams for implementation	6(1.0)	6(0.8)	4(0.7)	7(0.5)	2(0.5)	4(0.3)	19.3
Identify federal funding streams for implementation	4(1.0)	4(0.8)	2(0.7)	8(0.5)	3(0.5)	2(0.3)	14.7
Provide a resource that compiles available grant funding streams	2(1.0)	1(0.8)	1(0.7)	3(0.5)	1(0.5)	1(0.3)	5.8
Create the Illinois Health Information Network (ILHIN)	5(1.0)	3(0.8)	6(0.7)	2(0.5)	4(0.5)	3(0.3)	15.5

Technical standards development	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary required (two factor identification).	6(1.0)	6(0.8)	6(0.7)	6(0.5)	6(0.5)	6(0.3)	22.8
Provide personal digital certificates to patients	1(1.0)	1(0.8)	3(0.7)	1(0.5)	1(0.5)	2(0.3)	5.5
Establish techincial standards for networks, similar to other IEEE standards, for identification algorithms for patient identification	5(1.0)	5(0.8)	5(0.7)	2(0.5)	5(0.5)	5(0.3)	17.5
Develop interface engine for translating medical record identifiers across providers	3(1.0)	4(0.8)	2(0.7)	3(0.5)	4(0.5)	3(0.3)	12.0
Adopt and promulgate for Illinois HITSP Interoperability specifications (ANSI): "Functional Requirements for Nationwide Health Information Network" or other appropriate standards	4(1.0)	3(0.8)	4(0.7)	4(0.5)	3(0.5)	4(0.3)	13.9
Determine the applicability CCHIT certification of software vendors	2(1.0)	2(0.8)	1(0.7)	5(0.5)	2(0.5)	1(0.3)	8.1

Professional standards development	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Define professional qualifications for privacy and security officers	5(1.0)	5(0.8)	5(0.7)	5(0.5)	4(0.5)	4(0.3)	18.2
Define organizational reporting structure for privacy and security officers to ensure accountability and responsibility	4	3	4	2	3	1	12.0
Expand credentialing to licensure such as for other allied health professionals	2(1.0)	1(0.8)	1(0.7)	1(0.5)	1(0.5)	2(0.3)	5.1
Standardize certification curriculum (CISSP from ISC (ISO), GSEC from SANS)	3(1.0)	4(0.8)	3(0.7)	4(0.5)	5(0.5)	3(0.3)	13.7
Create more qualified professionals for security and privacy leadership (other than on-the-job-training) through a provided or subsidized training program	1(1.0)	2(0.8)	2(0.7)	3(0.5)	2(0.5)	5(0.3)	8.0

Staff education development	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Establish schedule for training, e.g. as for annual HIPAA training	2(1.0)	2(0.8)	1(0.7)	4(0.5)	5(0.5)	4(0.3)	10.0
Establish core competencies	8(1.0)	8(0.8)	7(0.7)	7(0.5)	6(0.5)	7(0.3)	27.9
Provide for privacy and security knowledge at the highest levels of organizations	5(1.0)	6(0.8)	8(0.7)	8(0.5)	8(0.5)	8(0.3)	25.8
Provide information resources so that technology is used to overcome HIPAA "myths"	1(1.0)	4(0.8)	4(0.7)	6(0.5)	2(0.5)	3(0.3)	11.9
Include in core competencies, for both routine staff as well as management, education in regulatory matters specific to exchange of health information	7(1.0)	5(0.8)	6(0.7)	5(0.5)	1(0.5)	6(0.3)	20.0
Provide policy development standards to maximize/optimize organizational participation and buy-in	4(1.0)	3(0.8)	5(0.7)	2(0.5)	4(0.5)	2(0.3)	13.5
Include privacy and security competencies in credentialing and licensing requirements	6(1.0)	1(0.8)	3(0.7)	1(0.5)	7(0.5)	5(0.3)	14.4
Recommend minimum levels of continuing education/clock hours for competency training	3(1.0)	4(0.8)	2(0.7)	3(0.5)	3(0.5)	1(0.3)	10.9

Consumer education development	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Develop educational materials for providers to distribute	6(1.0)	7(0.8)	3(0.7)	5(0.5)	6(0.5)	2(0.3)	19.8
Establish state lead to get message out on benefits in both print and other media	5(1.0)	5(0.8)	5(0.7)	4(0.5)	5(0.5)	3(0.3)	17.9
Involve private sector and other stakeholders in message development	4(1.0)	6(0.8)	2(0.7)	7(0.5)	7(0.5)	7(0.3)	19.3
Establish responsibility for patient education at level of delivery	7(1.0)	3(0.8)	4(0.7)	2(0.5)	1(0.5)	7(0.3)	15.8
Engage specialty organizations, e.g. AARP	1(1.0)	2(0.8)	1(0.7)	6(0.5)	4(0.5)	5(0.3)	9.8
Establish "core competencies" for patient education, including privacy rights	3(1.0)	4(0.8)	6(0.7)	3(0.5)	2(0.5)	1(0.3)	13.2
Address the public's focus on identity theft issues	2(1.0)	1(0.8)	7(0.7)	1(0.5)	3(0.5)	4(0.3)	10.9

Inclusion of economically disadvantaged healthcare groups	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Promote and expand, in discussion with State's Attorney General, national Stark and anti-kick back relief regulations, so those who are advantaged can support those who are disadvantaged.	9(1.0)	9(0.8)	5(0.7)	9(0.5)	9(0.5)	9(0.3)	31.4
Provide pressure/incentives on/for vendors to provide technical support for economically disadvantaged	8(1.0)	2(0.8)	7(0.7)	6(0.5)	6(0.5)	5(0.3)	22.0
Leverage ILHIN sanctions against vendors who fail to support or don't fulfill contractual obligations	2(1.0)	1(0.8)	5(0.7)	1(0.5)	1(0.5)	4(0.3)	8.5

Inclusion of economically disadvantaged healthcare groups	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Obtain special fee structures for broadband connectivity in rural areas (telecommunications service relief); and expand tele-health initiatives to both rural and densely populated urban areas	3(1.0)	3(0.8)	2(0.7)	8(0.5)	3(0.5)	1(0.3)	12.6
Exploit other ways of information exchange for disease management (other than internet, such as cable and satellite connectivity), especially in densely populated areas	1(1.0)	8(0.8)	1(0.7)	7(0.5)	4(0.5)	3(0.3)	14.5
Certify ASPs, to legitimize their functions, further the ASP model, and reduce costs of implementation/acquisition	5(1.0)	5(0.8)	4(0.7)	5(0.5)	7(0.5)	6(0.3)	19.6
Provide special attention to underserved and rural providers in all HIT educational efforts	7(1.0)	6(0.8)	8(0.7)	4(0.5)	8(0.5)	8(0.3)	25.8
Address professional shortages with targeted outreach, such as was done in the historical AHEC program for medical professionals with medical school training in outreach areas of Rockford, Peoria, Champaign	6(1.0)	4(0.8)	6(0.7)	2(0.5)	5(0.5)	7(0.3)	19.0
Provide training sessions for clinical administrators for HIT - onsite and/or remote	4(1.0)	7(0.8)	9(0.7)	3(0.5)	2(0.5)	2(0.3)	19.0

Quality assurance of health information exchange	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Require electronic "chart" pulls for accreditation	2(1.0)	1(0.8)	1(0.7)	1(0.5)	1(0.5)	1(0.3)	4.8
Provide recommendations for vendor selection include standards for increasing the ease of audit function for data integrity	4(1.0)	4(0.8)	3(0.7)	4(0.5)	4(0.5)	5(0.3)	14.8
Provide recommendations for vendor selection include standards for increasing the ease of audit function for legal integrity	1(1.0)	3(0.8)	4(0.7)	2(0.5)	3(0.5)	3(0.3)	9.6
Require routine quality assurance reviews for accreditation	5(1.0)	2(0.8)	2(0.7)	3(0.5)	5(0.5)	2(0.3)	12.6
Provide recommendations provided for multidisciplinary teams for acquisition of new IT solutions to include at least CIO, end users (clinical department, finance, quality management, HIM), security/privacy officer	3(1.0)	5(0.8)	5(0.7)	5(0.5)	2(0.5)	4(0.3)	15.2

Legislation and enforcement	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Enforce penalties for breaches and other violations	9(1.0)	3(0.8)	7(0.7)	3(0.5)	2(0.5)	3(0.3)	19.7
Identify “wrong-doers” and what is keeping them from following the regulations	5(1.0)	2(0.8)	6(0.7)	2(0.5)	1(0.5)	2(0.3)	12.9
Develop laws that are clear and succinct	6(1.0)	1(0.8)	4(0.7)	4(0.5)	5(0.5)	8(0.3)	16.5
Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts	8(1.0)	6(0.8)	9(0.7)	6(0.5)	8(0.5)	6(0.3)	27.9
Standardize state approach to national approach	4(1.0)	8(0.8)	3(0.7)	9(0.5)	9(0.5)	9(0.3)	24.2

Legislation and enforcement	Weighted Criteria						
	(A) 1.0	(B) 0.8	(C) 0.7	(D) 0.5	(E) 0.5	(F) 0.3	Total Score
Assess State's regulations in terms of other states' regulations or any proposed "model" legislation	2(1.0)	9(0.8)	1(0.7)	8(0.5)	7(0.5)	1(0.3)	17.7
Encourage flexibility in regulations to allow for changing technology	1(1.0)	5(0.8)	2(0.7)	5(0.5)	4(0.5)	5(0.3)	12.4
Begin regulatory review with "special" categories of health information for national standardization	3(1.0)	7(0.8)	5(0.7)	7(0.5)	6(0.5)	7(0.3)	20.7
Establish security standards body, with well-defined authority and responsibilities	7(1.0)	4(0.8)	8(0.7)	1(0.5)	3(0.5)	4(0.3)	19.0