Privacy and Security Solutions for Interoperable Health Information Exchange

Final Assessment of Variation and Analysis of Solutions Report

Subcontract No.
RTI Project No. 9825

Prepared by:

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

March 30, 2007

RTI INTERNATIONAL

Table of Contents

Executive Summary

HISPC was formed through a contract between the Research Technology International (RTI) and thirty-four (34) other states, including Illinois. The goal of HISPC was to assess and provide solutions that address variations in organization-level policies and state laws that affect privacy and security practices, including those related to HIPAA, and that may pose challenges to the interoperability of health information exchange (HIE). The prevailing principle behind HISPC is that workable privacy and security approaches and business practices are imperative for comprehensive information exchange solutions to facilitate quality improvement, medical error reduction, timely surveillance, rigorous research, and improved efficiency and affordability of health care.

The Illinois Foundation for Quality Healthcare (IFQHC) was designated by the Governor of Illinois as the coordinating entity for the HISPC project. The Illinois HISPC Steering Committee (HSC) was the reporting body for Illinois' contract with RTI. In addition, the HSC received oversight from the Illinois Electronic Health Records (EHR) Taskforce, created by the Illinois General Assembly in 2005 to make recommendations on statewide EHR activity. As part of their charge, the HSC provided RTI and the EHR Taskforce with the following:

- A comprehensive review of the privacy and security laws and business practices that pose a challenge to the proliferation of HIE within the state
- A review and examples of best practices and solutions within the state that maintain privacy and security protections while encouraging interoperable HIE
- Recommendations to improve both organizational business practices and state laws regarding privacy and security that currently adversely affect interoperable HIE
- A plan to implement the subcommittee's recommendations

The HSC had under its purview several working groups to support its objectives. These working groups included a business variations working group (VWG), a legal working group (LWG), a solutions working group (SWG), and an implementation plan working group (IPWG). The HSC determined the membership of the working groups as well as reviewed and approved all work products resulting from the groups.

Business practices surrounding privacy and security of health information conducted by organizations in the state were captured and assessed by the VWG. Over one hundred (100) unique business practices among 30 representative organizations were discovered. The VWG determined that the uses of technology to capture, maintain, and share patient information vary tremendously among Illinois' organizations. As would be expected, business practices surrounding privacy and security of health information were discovered to vary based on the level of technology available to an organization. However, several common themes appeared regardless of the level of technology available to an organization. The varying array of interpretation and sometimes misinterpretation of HIPAA was a common issue, sometimes even within the same organization. Also, for paper-based organizations, sharing of information was shown to be based significantly on established, trusted relationships. The level and method of sharing was revealed to be based on familiarity between the existing parties more so than established business agreements. As such, a telephone call from a trusted person would garner the requisite information and perhaps more than required.

One of the key findings of this study of business variations is that Illinois has very strong protections to ensure that privacy and security are maintained during the exchange of health information. There are extensive laws that apply to Illinois providers, payors, and others, establishing

rights and obligations with respect to maintaining patient privacy, and confidentiality and security of patient health information. These laws drive health information exchange practices in Illinois and should be taken into account in discussing necessary information technology parameters and requirements for national electronic HIE. However, because there is currently little electronic exchange of information between organizations, there are few operational examples of these protections as they relate to electronic HIE. Silos of technology utilization were 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. The most salient reason for this is that the culture in Illinois has not been not conducive to data sharing. Information often has been deemed as proprietary and a business asset as opposed to an opportunity to improve quality of care and patient safety. Although there is evidence that this trend is shifting, the shift is occurring slowly and sporadically. The cultural change and technical infrastructure necessary for sharing information will need to come together before the policies and procedures necessary to facilitate HIE begin to become more commonplace.

Critical barriers to the implementation of interoperable electronic HIE were elucidated further by the work of the SWG. Barriers were confirmed to exist in organizational culture, in technology and standards, in lack of knowledge at the both the staff and consumer level, in organizational resources for HIT, in leadership for privacy and security protection, in the global market, and in relation to state and/or federal law, primarily in misinterpretations and non-compliance. Root causes for these barriers were determined to include needs for proof of the benefits of regional HIE, development of technical and professional standards, consumer and staff education, inclusion of economically disadvantaged providers, quality assurance in HIT, and clear and concise legislation and enforcement thereof. The SWG developed solutions to address these specific needs and systematically prioritized them based on the maximization of patient care and outcomes, feasibility of implementation, the maximization of privacy and security protection, cost effectiveness, alignment with other state and national activities, and a reduced dependency on the accomplishment of other activities. The prioritized solutions forwarded on to the IPWG for implementation planning included the following recommendations:

- Determine benchmarks for regional exchange of information - perhaps by committee of industry (HIT and administrative) stakeholders, similar to that done for HIPAA transactions
- Adopt universal standard for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary identification factors required.
- Define professional qualifications for privacy and security officers
- Establish core competencies for staff education
- Develop educational materials for consumers for providers to distribute
- 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.
- Provide recommendations for multidisciplinary teams for acquisition of new IT solutions
- Include in lead state agency/organization legal staff with expertise in privacy and security to guide integrated state efforts

1.0 Background and Purpose

1.1 Purpose and Scope

The purpose of this report is to document the assessment of the business variations that affect privacy and security of EHR in Illinois, as well as the proposed solutions to privacy and security-related issues that were identified as significant barriers to successful electronic HIE within the state of Illinois. This report will outline the processes used to identify the business variations, to determine and clarify the barriers to HIE, and to develop solutions to address these barriers. Each proposed solution will include a description of its HIE context, the privacy and security areas affected, stakeholders involved, HIE barriers addressed, stage of development and use of the solution and possible barriers to implementation.

1.2 Level of HIT Development in Illinois

The challenge of expanding EHR utilization as well as implementing electronic HIE in Illinois is underscored by the size of the health care provider network. There are 214 hospitals, approximately 40,000 physicians, 8,304 clinical laboratories and 1,160 long-term care facilities in Illinois. As described in detail in the Illinois EHR Taskforce Report and Plan (December 2006, available at http://www.idph.state.il.us/ehrtf/ehrtf_home.htm), there have been some significant efforts to build upon. Hospitals, clinics, physicians and public health professionals have been actively pursuing various electronic solutions for some time. Six Illinois hospitals made the *Hospital and Health Network's* 2006 list of the "100 most wired hospitals and health systems."(*Hospitals and Health Network Magazine,* July 2006.) Hospitals on this list were judged on their use of information technology in "five key areas: business processes, customer service, safety and quality, workforce and public health and safety." Early statewide efforts have been focused on providing better coordination of maternal and child health services. These include, among others:

Cornerstone – a data management information system developed to facilitate the integration of community maternal and child health services.

Illinois National Electronic Disease Surveillance System (I-NEDSS) – a secure web-based application that establishes a secure and real-time communication link between hospitals, laboratories and other health care providers with state and local health department staff for the purposes of reporting and managing communicable disease information.

Illinois Comprehensive Automated Registry Exchange (ICARE) – a web-enabled immunization registry providing health care providers access with an Internet Browser.

Tracking Our Toddlers' Shots (TOTS) – a network based immunization registry that currently houses more than 12 million immunization records.

Federal funding has fostered several EHR initiatives. In September 2004, the U.S. Department of Health and Human Services' Agency for Healthcare Research and Quality (AHRQ) awarded $139 million in contracts and grants to promote the use of health information technology, including a number (5) of national RHIO demonstrations from which results and findings will be available this next year. AHRQ funded five Illinois projects.

In January 2005, the Illinois Hospital Research and Educational Foundation - an affiliate company of the Illinois Hospital Association - launched another statewide EHR initiative entitled the "Illinois Health Network" (IHN). Funded by a grant from the Illinois Department of Public Health (IDPH), the network "offers a web-based gateway interface that enables the secure exchange of health and business-related information and data," as described in "Illinois Health Network, What is the IHN" web page, 2006, available at http://www.illinoishealthnetwork.org/whatisihn.htm

Despite the level of HIT development in the state, Illinois is in the infancy of widespread HIE. As stated above, significant investment in HIT 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 completed by the Illinois Electronics Health Records Taskforce (EHRTF). The EHRTF has recently submitted its final report to the Illinois General Assembly, cited above. 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. IDPH would form a public-private partnership with ILHIN to advance EHR and HIE initiatives within the state if taskforce recommendations are enacted. Another key recommendation of the taskforce is for the IDPH/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. Legislation to create the ILHIN as recommended by the EHRTF passed the House of the General Assembly by unanimous vote on March 22, 2007, and was then forwarded to the Senate for continuation of the legislative process. Action in the Senate is pending current to the date of this report. The bill calling for the formation of the ILHIN has a start date of November 1, 2007 for the organization.

1.3 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, especially to the solutions proposals. 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 LWG. Face-to-face interaction was critical to the decision-making process. However, given that a significant portion of solution development occurred during the December 2006-January 2007 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.

2.0 Assessment of Variation

2.1 Methodology Section

Upon award of the HISPC contract, the Illinois Foundation for Quality Healthcare, in conjunction with IDPH, determined the make-up of the HISPC Steering Committee (HSC). The HSC was comprised of several members of the EHRTF. The primary goal of the Illinois EHRTF was to promote and provide legislative guidance for statewide use of EHRs and improved health information exchange (HIE). The HISPC project provided the EHRTF with needed information in the area of security and privacy to help achieve this goal. The HSC provided the leadership and oversight for the Illinois HISPC project. The HSC also provided recommendations of members for each of the working groups that made up the HISPC. These working groups included a business variations working group (VWG), a legal working group (LWG), a solutions working group (SWG), and an implementation plan working group (IWPG). The HSC had twelve (12) members representing eleven (11) organizations. The HSC Roster and Committee Charter are included in Appendix 1; the VWG Roster and Committee Charter are included in Appendix 2; the LWG Roster and Committee Charter are included in Appendix 3. The SWG and IWPG Roster and Committee Charter are included in Appendix 4 and discussed in Section 3.2.

The following eighteen scenarios, discussed in the Summary of Relevant Findings below and found in their entirety in Appendix 5, were developed specifically by RTI for the HISPC project to provide a standardized context for discussing organization-level business practices across all states and territories. The scenarios represented a wide range of purposes for the exchange of health information (e.g., treatment, public health, biosurveillance, payment, research, marketing, etc.) across a broad array of organizations involved in HIE and actors within those organizations. The product of the discussions was a database of organization-level business practices that formed the basis for the assessment of variation upon which all other work was based.

Each scenario described an HIE within a given context to ensure the discussion covered most of the areas in which to expect to find barriers. The scenarios were not developed with the intent to cover the universe of exchanges. Such a comprehensive approach would have been impossible given the timeframe for the project. However, the purposes and conditions represented were more than adequate to get the discussions of privacy and security policy moving forward. To further delineate and inform the discussions on privacy and security, RTI provided descriptions of nine different domains of privacy and security protection of health information, and business practice variations were discussed within the context of these nine domains:

- User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be.
- Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.
- Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.
- Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

- Information protections so that electronic personal health information cannot be improperly modified.

- Information audits that record and monitor the activity of health information systems.

- Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

- State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

- Information use and disclosure policies that arise as health care entities share clinical health information electronically.

Meetings with the VWG and facilitated individual calls to the larger stakeholder community were the two methods for acquiring business practices on security and privacy of health information. A healthcare market research firm was contracted to facilitate the meetings and calls. The VWG was formed from the recommendations of the HSC and consisted of thirteen (13) members representing eleven (11) organizations (Appendix 2). The VWG met six (6) times to discuss each of the eighteen (18) scenarios provided by RTI. During the first meeting, Patient Treatment (Scenario 1) and RHIO (Scenario 6) scenarios were presented, as they were deemed most applicable to the vast majority of work group members. Subsequent meetings only included members that were applicable to the scenarios that were to be covered during a given meeting. The meetings averaged two (2) hours in length.

Twenty-seven (27) one-on-one facilitated interview calls were made. On average these calls lasted thirty (30) minutes. The call participants represented twenty-three (23) organizations. Both during the VWG meetings and within the interview scenarios, participants were not asked only about their business practices, but also about the domains to which the practices related. They also were asked whether they felt the practices were barriers or aids to HIE. Meeting and interview notes were taken and analyzed by the project coordinators and the market research firm. Business practices were extracted from the notes and entered into the Assessment Tool provided by RTI. The project team reviewed the results and classification of the practices and made changes whenever appropriate.

The HSC, the VWG, and members of the broader stakeholder community were given the opportunity to review and confirm the validity of the identified business practices as well as add any additional practices that may have been omitted previously. The LWG, composed of seven (7) members which included privacy and security experts in private legal practice, a hospital compliance officer, Chief Counsel for IDPH, and representatives from the Illinois Hospital Association and Illinois State Medical Society, reviewed the business practices to identify possible legal drivers for the practices.

2.2 Summary of Relevant Findings

Business practices surrounding privacy and security of health information conducted by organizations in the state were captured and assessed by the VWG. Over one hundred (100) unique business practices among thirty (30) representative organizations were discovered. The VWG determined that the uses of technology to capture, maintain, and share patient information vary tremendously among Illinois' organizations. As would be expected, business practices surrounding

privacy and security of health information were discovered to vary based on the level of technology available to an organization. Variations specific to each scenario are discussed below.

2.3 Treatment (Scenario 1-4)

Scenarios 1 through 4 discussed the transfer of information in emergent and non-emergent situations, the amount of information that could be disclosed and the ability of providers to access protected-level (i.e. mental health, substance abuse, HIV/AIDS and genetic testing information) patients and their information, regardless of the provider's hospital admitting status. Specifically, the following issues were called into consideration:

- Need of emergency room physician to obtain patient authorization from emergency room accident victim in impaired mental state and ability to obtain prior mental health medication information and treatment records from a neighboring state hospital.
- Need of primary care provider to obtain patient authorization and ability to obtain and release substance abuse treatment program records to subsequent treatment providers.
- Provider's ability to obtain prior treatment records and mammography images, including HIV test result information, from provider located in another state.
- Patient's ability to obtain a deceased relative's genetic test result information.
- Various IT and security-related issues, including a treating physician's ability to access the facility's electronic health record and transcription service regarding inpatient visit, transmission of information to an offshore transcription service, use of secure web portal and encryption, email, electronic signature, and transfer of patient information back to the facility.

2.3.a. Stakeholders

The stakeholders that were solicited for input to these scenarios included representatives from third party payors, clinicians, behavioral health, law enforcement, public health and hospitals in both urban and rural settings. The hospital job functions included compliance, safety and privacy, risk management, health information and medical records.

2.3.b Domains

The domains addressed in this scenario included:

- User and Entity Authentication
    - Mental health stakeholder stated that no verbal or written user or entity authentication is required for the release of patient information in cases where information is not protected or can't be released for legal reasons.
    - Pharmacy stakeholders stated the organization releases the minimum amount of data in an emergent situation with authentication occurring verbally, physicians would provide Drug Enforcement Agency (DEA) number and law enforcement

would provide badge number and district. The authentication could also occur by requesting a callback number to confirm.

- Hospital stakeholders stated that medical records department doesn't release any information during the first contact by the requestor. To authenticate requestor's identity they require a telephone number that they can call back.

- All stakeholders stated that they request some form of identification from patients and physicians (with whom they are not familiar) before treatment or release of information.

- Information Authorization and Access Controls

  - Stakeholders stated that all users receive training before a user name and password is issued.

  - Hospital and Clinic stakeholders stated that all employees have to sign confidentiality agreements regarding disclosure of patient information.

  - Stakeholders with EHRs stated that access to patient information is based on role in the organization, with physicians having access to all patient information.

  - One hospital stakeholder stated it provides access via a secure portal to all credentialed physicians in the area, regardless if the physician has admitting privileges to that specific hospital or not.

  - Hospital stakeholders with an EHR stated that offsite access to patient files is allowed for physicians and some radiologists.

  - Some hospital stakeholders allow temporary access for non admitting credentialed physicians whereas other stakeholders don't allow access to non-admitting physicians to locked units and patient files.

  - One hospital stakeholder with an EHR that doesn't allow temporary access to non-admitting physicians will allow paper copies of pertinent patient information if it is critical to patient care.

- Patient and Provider Identification

  - Stakeholders from all groups stated in paper-only environments, patients are categorized by social security number and name.

  - Stakeholders with an EHR categorize patients using basic name and demographic information.

- Information Transmission Security or Exchange Protocols

  - Stakeholders from all groups stated that they exchange information either verbally or via fax with appropriate disclaimers in emergent situations. In non-emergent situations information can be transmitted verbally, fax or U.S. mail.

Very few of those interviewed had dedicated fax machines for specific information.

- Physician stakeholders utilizing offshore or onshore transcription services access their transcribed encounter notes via a secure web portal. Most stakeholders stated they did not use any offshore services.

- One hospital stakeholder stated that their policies strictly prohibit use of offshore transcription services.

- Stakeholders, which transmit patient medical records and laboratory results in non-emergent situations, send these records by either internal mail or U.S. mail, or release them directly to patient. Some stakeholders send mammogram or laboratory results via Fed-ex or other carrier for tracking purposes. One stakeholder provides an encrypted CD with any medical records that include protected information to requesters as long as a patient release form is signed.

- All stakeholders utilize fax disclaimers that state, "If this transmission has been received in error please destroy."

- Information Protections (against improper modifications)

  - All stakeholders with an EHR stated that electronic signatures are used to sign off on patient charts.

  - Stakeholders all stated that an addendum can be added to the original record with a date, time stamp and user's name. Most stated that patient records can only be amended within 24 hours of initial documentation. In one organization, designated individuals only can amend an unsigned report. An audit trail has to be printed and attached to the record.

- Information Audits

  - Stakeholders with an EHR stated that when files are accessed, printed, or copied an entry is created in the audit log. Those without an EHR didn't have any way of tracking records.

- Administrative or Physical Security Safeguards

  - Stakeholders stated that access to patient information is restricted by user's role within the organization.

  - Hospitals and pharmacies store all patient information in a locked room with restricted access.

  - Stakeholders stated that administrative personnel responsible for diagnostic coding of charts are responsible for noting the records with legally defined highly confidential information. Stickers, usually orange, are used on the charts to trigger careful handling of the record.

- Stakeholders stated release of non-emergent health information that includes protected information has to receive specific authorization from the patient before disclosure

- State Law Restrictions/Considerations

  - State law restrictions in Illinois impact the ability of providers to exchange certain types of patient information without first obtaining the patient's written consent. The four treatment scenarios require application of the following state and federal laws:

    - Illinois law that provides extraordinary protections for mental health information (Patient Care Scenarios 1 and 3).

    - Illinois law and federal regulations that provide extraordinary protections for substance abuse treatment records (Patient Care Scenario 2).

    - Illinois laws that provide extraordinary protections for HIV and genetic testing information (Patient Care Scenario 4).

  - Under each of these Illinois laws, release of information would be restricted without patient "consent," with limited exceptions. None of these laws contain a broad exception that would permit information exchange without consent for "treatment purposes," as permitted under HIPAA. Therefore, each Patient Care Scenario required further analysis under these special protection laws to determine whether the particular type of information requested could be released under the particular circumstances.

    - Applying Illinois law to the releasing facility in Scenarios 1 and 3, mental health information could be released if the patient is able to sign a valid "consent." Scenario 1 raised a further question concerning the ability of the health care provider to obtain a possibly impaired patient's consent at the time that the information was required for treatment purposes. In such cases, the "emergency" exception contained in the Illinois law would permit the releasing facility to disclose relevant information if the patient is not able to sign a consent. The Illinois law would also permit release without consent to "a consulting therapist," if the receiving facility or physician fell within the definition of being a consulting "therapist" providing "mental health services."

    - State and federal law generally prohibits release of alcohol or substance abuse treatment program information, with limited exceptions. The law does allow for the release of such information with the patient's "consent" or in the case of medical emergency. However, since Scenario 2 involved a non-emergent transfer of records and there are no other applicable exceptions under the Illinois law, the patient's valid "consent" would be required for the treatment program to release the requested records to subsequent providers.

- With limited exceptions, Illinois law prohibits release of genetic testing information other than to the individual or to persons authorized by the individual, or the individual's legally authorized representative, pursuant to a written "release." In Scenario 4, the patient requested a deceased relative's genetic testing information that might have been relevant to the patient's current diagnosis and treatment. Since Illinois law does not provide any applicable exception to the general prohibition against disclosure, only the deceased relative's legally authorized representative would be able to sign a valid release for the genetic testing results under the Illinois law. (Note that absent the special state law protections, the HIPAA Privacy Rule would permit the release of the deceased patient's information to the patient's physician pursuant to the Privacy Rule's permissive disclosure for "treatment" provisions.)

- Similarly, Illinois law prohibits disclosures that would identify persons tested, or the results of HIV tests, with limited exceptions. If the treatment records requested in Scenario 4 contained such information, the releasing facility would need to have a "legally effective release" in order to comply with the Illinois law.

- Also impacting the timely and effective HIE is the need to comply with the particular state law that defines the elements of an effective "consent," depending on the type of information to be released. For example, under Illinois law, the requirements for valid "consent" for release of mental health information (Scenario 1) and for release of substance abuse records (Scenario 2) are similar to HIPAA's authorization requirements, although there are some additional required elements found in those special records laws (e.g., witness signature and expiration date). However, the Illinois law requirement of a "legally effective release" for HIV and genetic testing information (Scenario 4) does not specify any particular elements or form for such a release to be valid.

- In addressing inter-state exchanges of information, and to the extent that the information request does not include information afforded extraordinary legal protections under the releasing facility's state laws (for example, the request for prior mammogram images in Scenario 4), HIPAA would permit the inter-state exchange among providers without the patient's consent or other special form of authorization. However, if the information requested is afforded extraordinary protections under applicable state or federal law (for example, mental health information under Scenarios 1 and 3, substance abuse treatment information under Scenario 2, or HIV or genetic testing results under Scenario 4), the law of the releasing facility's state would need to be addressed. If the releasing facility was located in a state other than Illinois, it is presumed that there would be similar restrictions as I n Illinois, as well as the need to comply with the particular laws of that state. In practice, many providers incorporate the required elements that apply to the types of information that they maintain into that particular facility's authorization form. In each of the four treatment scenarios, the form signed by the patient would have to comply with the

releasing facility's state law requirements, and it is presumed that the releasing facility's authorization form could be obtained.

- In each of the scenarios involving information afforded extraordinary protections under Illinois law (e.g., mental health information in Scenario 1, substance abuse treatment records in Scenario 2, and the HIV and genetic testing information in Scenario 4), the facility receiving the requested information would be prohibited from making further disclosures without the patient's written consent. These and other similar states' restrictions would need to be addressed in structuring an intra or inter-state information exchange system and/or uniform consent form that would apply to subsequent health care providers and subsequent requests or releases of the patient's information.

- In considering the ability of providers to obtain advance consent for health information exchange (for example, authorizing release to subsequent treatment providers not yet known), the current legal requirements under Illinois law governing release of mental health information require the recipient (the person or agency) to be named in the consent form, and require that a specific duration or expiration date be stated. Similarly, the laws addressing release of alcohol and substance abuse treatment records require identification of the name or title of the individual, or the name of the organization, to whom disclosure is to be made as well as a specific expiration date, event, or condition (which must not be longer than reasonably necessary to serve its purpose.) These state law requirements are more stringent than HIPAA's authorization requirements, and may hinder the ability of providers obtaining advance consent at the initial point of service where the record is created (e.g., during the prior hospital admission in Scenario 1 or participation in the treatment program in Scenario 2). In comparison, the HIPAA Privacy Rule authorization provisions require only the identification of persons or "class of persons" who are authorized to receive the information, thus making obtaining advance consent for future information exchanges easier to accomplish under HIPAA than under those current state law provisions.

- Scenario 3 involved a psychiatrist who sees a patient in a skilled nursing facility but has not yet been given authorization or ability to access the facility's electronic record. The physician then proceeded to see the patient and dictated notes, which were then electronically transmitted for oversees transcription, then to his office, and then back to the facility. The facility was unable to incorporate the physician's report into the patient's record because it was encrypted. The LWG noted that under Illinois law, it is the facility's obligation to maintain an active record that is accessible to authorized personnel and includes all notes and observations made by direct care providers. The law further requires physicians to make notations at the time of each visit. (See the Nursing Home/Long Term Care Regulations cited in Appendix 6.) Therefore, this scenario raised issues concerning the facility's obligation to have appropriate policies and mechanisms to authorize and permit providers to access and document the record. In the event a facility had delegated responsibility for dictation to the physician who then subcontracted with an oversees organization, HIPAA would require a

business associate agreement between the facility and the physician and a subcontract between the physician and the transcription company (unless the facility-physician relationship is viewed as falling outside the business associate requirements, in which case HIPAA would require a business associate agreement between the physician and the transcription company). The business associate/contractor agreements would hold the business associate/contractor to the same privacy and security obligations that apply to covered entities under HIPAA. This scenario raised a number of concerns, including the difficulty in enforcing business associate agreements, the perceived lack of accountability on the part of business associates (particularly those residing oversees), the difficulty and impracticality of trying to negotiate indemnification provisions (which are not required by HIPAA) into business associate agreements as a means of monetarily establishing accountability, and the perceived general lack of control or accountability on the population of individuals who are outside of the jurisdiction of HIPAA and other state and federal laws that provide for accountability and the imposition of sanctions for the misuse of patient information.

- Information Use and Disclosure

    - Hospital stakeholders stated in accident investigations test results for alcohol and barbiturates are released to law enforcement investigating motor vehicle accidents after the appropriate forms have been received. Patient authorization is not needed.

    - Stakeholders release the "minimum necessary" information to requestors. The interpretation of "minimum necessary" is left up to the person giving the information.

    - Stakeholders stated they would not release any treatment or medication information to other health care entities without patient consent or healthcare power of attorney.

    - Hospital stakeholders stated that patient records that are received from outside of the hospital are included as part of the permanent records under a tab labeled "other" in the back of the chart and the information can't be disclosed. Those with an EHR scan the information into the patient's record.

    - Stakeholders stated that medical records for deceased relatives require a death certificate, consent of next of kin, or power of attorney.

2.3.c. Critical Observations

Based on interviews and discussions with the VWG, it was found that many healthcare provider organizations use the telephone and fax machines as their primary means of exchanging patient-level information with one another. Stakeholders tend to rely heavily on pre-established relationships when exchanging information. Often times, voice recognition alone is enough for authentication of the person receiving the information.

For organizations that utilize an EHR, significantly more procedures are in place to protect patient information. Users receive training and sign confidentiality statements before being allowed access to EHR systems; however, no reference was made to ongoing employee training on policy and procedure changes.

Some organizations indicated they distinguish highly confidential protected patient information using colored stickers on the chart. This is a significant issue as this now means the information has been highlighted rather than held to a higher standard of privacy.

Several stakeholders indicated that insurance cards or green cards used as identification are not always a reliable way to authenticate patient identity. Because of the fraudulent use and sharing of insurance identification cards to receive medical treatment, medical records may not accurately reflect the actual care received. A medical record could possibly include information of more than one individual. Conversely, one individual could have information spread among several medical records under different names.

In exchanging patient information for non-emergent treatment reasons, the stakeholders 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 that pre-date HIPAA.

Another practice identified by stakeholders is the segregating of patient records received from other health care providers in the patient's chart and the statement the records of other providers are "not subject to redisclosure." While such practice would be consistent with the special protections afforded to certain classes of information under state law, if applied generally to all types of health information such practice seems inconsistent with the HIPAA Privacy Rule requirement that records created by others are considered to be part of the patient's "designated record set" and subject to disclosure, at least in the case of patient requests. Illinois law also requires health care facilities to permit patients to access and authorize release of the records maintained by the facility (See *Code of Civil Procedure* 735 ILCS 5/8-2001 and 2003, referenced in Appendix 6). As may be the case with the practice of requiring patient authorization in treatment situations where HIPAA would not require it, the identified practice of not disclosing records obtained from other providers pre-dates HIPAA and may be driven by state law restrictions that prohibit redisclosure without consent in certain special record situations. There also seems to be misunderstanding and inconsistent treatment concerning what records constitute and are part of the patient's "record" (or "designated record set" under HIPAA) and thus required to be maintained and released in appropriate circumstances. The conversion to electronic information systems where some or all records and information may be maintained electronically in one or more locations and in different formats increases the need for appropriate legal analysis and education.

The opinion of the LWG was that these types of inconsistent application of legal principles are not unique to Illinois, and the future institution of either a state or national information exchange mechanism will provide an opportunity to educate health care providers and others on legal requirements and good clinical practices associated with maintaining and appropriately releasing patient information for appropriate purposes. Education and awareness should be viewed as a means to encourage universal HIE.

There are not standardized forms to request or disclose patient information. As such, organizations potentially share varying degrees of information for the same type of request. Furthermore, a general lack of standardization of information management inter-organizationally has created silos of development that will impede the transition from paper to EHR management. The overall culture of consideration of health information to be proprietary in nature has also contributed to the formation of these information silos. This change in culture is occurring, albeit slowly. However, culture change is a prerequisite to any technical infrastructure development with its concomitant policy, procedures, and practices.

In identifying state law restrictions that may have the effect of restricting the future interoperability of a state or national health information exchange program, the LWG noted that while the federal HIPAA regulations would currently permit health care providers to exchange information among themselves without patient consent for treatment and payment purposes, the more stringent restrictions that are in place in order to protect certain classes of information may be one reason for the seeming unwillingness of providers to openly share information in non-emergent treatment or payment situations. However, in each of the special classes of information identified under Illinois law, information may be released with the patient's consent, and that it would also be possible in most cases to obtain advance consent for future HIE for a particular purpose, such as emergent or non-emergent care.

There is a high level of existing awareness and adherence to strict confidentiality standards by health care providers and other stakeholders in Illinois. In analyzing potential legal "barriers" to HIE, the LWG did not necessarily believe that the various state (and federal) laws that provide protections and extraordinary protections for health information should be viewed as "barriers," but rather the existence of such laws need to be addressed in creating the framework for national information exchange. Using technology to further existing privacy and confidentiality protections should be viewed as a means of promoting confidence and participation in national electronic HIE, and not a barrier.

The LWG identified various privacy laws that impact the release and exchange of health information in Illinois (See Appendices 4 and 5). Not only are these laws drivers for protective practices demonstrated by the various stakeholders interviewed in connection with this project, but absent some sort of federal preemption or revocation of all the individual states' privacy laws and special protections afforded by existing federal laws for certain categories of information, the fact that these laws exist and the issues raised in the analysis of business variations were considered by the SWG and IPWG.

Specifically, the following issues were identified as areas for further discussion:

- Documentation of "Consent". Having a uniform consent/authorization to release information would likely facilitate electronic exchange of information.

- Electronic Documentation, Storage and Transmittal of Consent/Authorization. Having the patient's signed consent/authorization electronically stored and quickly accessible for future requests and information exchanges would also likely facilitate electronic information exchange.

- 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, obtaining 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. See for example, the provisions of the Illinois Insurance Information and Privacy Protection Act permitting insurers to obtain authorization for the purpose of collecting information in connection with application up to 30 months from the date signed and for the term of coverage in connection with benefit claims. [215 ILCS 5/1007].

- Form of Consent. The consent/authorization form could specify information and under what circumstances the provider (or record locator service, data warehouse, or other intermediary) is authorized to release the information, and to whom, and for what purpose. For the most part, HIPAA's authorization form requirements are consistent with the special requirements under Illinois' special record laws requiring consent or valid release prior to future disclosure of information, although certain additional statements would be required in order to permit release of certain categories of information. (See Appendix 7.) If each provider obtained, at the point of service, an authorization/release that complied with the laws of that provider's state, then, upon appropriate "request" (whether it be via a RHIO or record locator service), that provider's records could be "released." If the patient does not consent or authorize a particular type of release (for example, release of genetic testing information or abortion records), then that provider's information could not be shared or exchanged in the future, unless the patient authorized the release at that time. The form could permit the patient to decide, to the extent permitted by law, the circumstances under which his or her information may be shared. For example, the particular authorization form completed and signed by a patient could provide advance consent to the release of all health information to other care providers for treatment (and payment and operations) purposes without the need for any further written permission. Or, the patient could authorize release of all information if needed to provide emergency medical treatment (and payment). The form could acknowledge and/or authorize releases that are otherwise permitted or required by law (for example, for research and public health activities, etc.).

- 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 – see Appendix 7). 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. By way of example the Illinois Hospital Licensing Act regulations state that: "It is recommended that the unique confidentiality requirements of a psychiatric record be recognized and safeguarded in any unitized record keeping system of a general hospital." [77 Ill. Adm. Cod 250.2290.]

- 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, the LWG discussed whether 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 sub-contractor 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 oversees business partner who is not easily made subject to U.S. legal or contractual requirements. Providing additional deterrence could facilitate and remove barriers to voluntary participation in an information exchange mechanism.

- Ability to Audit. The security and IT issues raised in connection with these concerns include the ability to audit and track breaches and other misuses of information. Addressing the ability to track and prevent misuse, and correct any resulting damage to the patient, would likely result in greater consumer and stakeholder confidence and promote acceptance of a national system for electronic HIE.

2.4 Payment (Scenario 5)

Scenario 5 discussed the interaction of third party payors and health care providers. Insurance company caseworkers require access to patient information to properly manage cases of the patients in which insurance coverage is provided. In particular, caseworkers are required to approve/authorize inpatient encounters and thus need a certain level of access to patient information in order to properly make this assessment. Scenario 5 addressed the possible business practices that are required if a healthcare provider utilizes an EHR and provides access to the EHR to insurance company caseworkers.

2.4.a. Stakeholders

The stakeholders that were solicited for input to this scenario included representatives from commercial payors, and security officers and risk managers from hospitals in both urban and rural settings.

2.4.b. Domains

The domains addressed in this scenario included:

- Information Access and Access Controls
    - Payor does not request access to any provider's EHR for approval or authorization.
    - Healthcare providers do not provide electronic access to any of their patient systems to external entities that are not officially affiliated with the healthcare provider.
- User and Entity Authentication
    - Payor authentication of patient requesting approval/authorization for inpatient encounters by verification of member identification number, name, birth date and address is done via a telephone call or letter from the patient to the payor.
    - Payors authenticate provider's identity via the telephone or internet by verifying provider identification.
- State Law Restrictions
    - With limited exception, the state laws that govern release of mental health and developmental disabilities information, substance abuse treatment records, and HIV and genetic test information in Illinois require valid patient consent to release information to third party payors. For example, the *Mental Health and Developmental Disabilities Confidentiality Act* provides for limited disclosures of health information necessary for a patient to receive insurance benefits, but only when it is not possible to obtain the patient's consent because the patient is not capable of providing consent or is not available to do so. [740 ILCS 110/6.] HIPAA also requires patient authorization and consent for special types of HIE, such as psychotherapy notes.

- Under the Medical Patient Rights Act, the nature or details of services provided to patients cannot be disclosed to anyone (other than the patient or his designee) without the patient's written authorization except in limited circumstances [410 ILCS 50/3(d)]. For instance, consistent with HIPAA, disclosures are allowed to "persons directly involved in treating the patient or processing the payment for that treatment"…and to "those persons responsible for peer review, utilization review, or quality assurance." *Id.*

- The Illinois Insurance Information and Privacy Protection Act sets forth the requirements for authorization forms used by insurers with those they insure in order to disclose and obtain information from others in connection with an insurance transaction. The law also provides that the length of time the authorization remains valid varies with the purpose of obtaining the requested information. An authorization signed for the purpose of collecting information in connection with a claim for health benefits is effective for the term of coverage of the policy [215 ILCS 5/1007].

2.4.c. Critical Observations

Disclosures are exempt from HIPAA's authorization requirements when they relate to treatment, payment or health care operations. Similarly, state law exempts disclosures from the authorization requirement for the purpose of processing claims and mandates insurance authorizations which broadly cover such requests for the terms of a given policy. Scenario 5 involved such a disclosure where a health plan's nurses are seeking patient medical data for the purpose of authorizing payment. In similar scenarios, plan nurses might also seek information for the purposes of utilization review or care coordination activities, which are consistent with HIPAA's definition of "health care operations." HIPAA's minimum necessary standards apply to disclosures for purposes of payment and health care operations, but do not apply to disclosures pursuant to an authorization.

It appears for purposes of payment, the industry relies on inquiry-specific authorizations, despite the presence of the above exemptions in both federal and state law for such purposes and single authorizations that can last the life of a policy when related to claims payment. This may be because providers and payors want to avoid disagreements or negotiations regarding whether the minimum necessary standard has been met and/or want to avoid implementing procedures and standards reflecting "minimum necessary." Healthcare providers and third party payors stated that they share only the "minimum necessary" data with other entities. However, the definition of "minimum necessary" appeared to vary widely among organizations and even within the same organization.

It is unlikely that the above business practices would change in an electronic environment. Third party payor representatives stated that they would not solicit for nor take advantage of any access granted to a hospital's EHR. This just is not part of their current procedure. If the carrier did not already have the information as part of their own data set (claims data), they would request information using a paper-based procedure for release of information. An electronic environment could, however, facilitate the transmission of such data once the authorizations were in hand.

In regards to healthcare providers, hospitals have not routinely provided access to their EHRs by external entities such as third party payors. There are specific policies and procedures in place for

access to protected health information (PHI) by employees and physicians of the hospital. However, electronic access is not granted typically to non-employees of the hospital. And although this was against policy for provider and the insurer, a health plan's caseworker did share the fact that nurses in office-based physician practices have provided information to caseworkers by allowing them to view pertinent decision-making data under the nurse's login. However, it was stated that the nurse did not share her login information and the nurse was present during the reviewing process. Before access to records could be permitted, the disclosing covered entity would need to make sure an appropriate pathway existed consistent with state and HIPAA privacy requirements and administrative safeguards.

Criteria for the payment authorization of inpatient admissions are determined by coverage eligibility, level of trauma, diagnosis, and laboratory test results. These data elements could be more easily acquired through an EHR. Existing business practices surrounding the authorization to approve inpatient admissions could be considered potential barriers to the widespread adoption of an EHR. On the other hand, moving to an electronic environment can facilitate the availability of authorizations, if preferred by covered entities and patients, as well as the development of alternative mechanisms consistent with minimally necessary standards.

Should the industry want to change business practices and eliminate the need for authorizations, mechanisms would be required to ensure that a minimal set of information is exchanged. An electronic pathway would require sufficient authentication, verification and technical safeguards (pursuant to HIPAA's Security rules) to ensure appropriate use. Specifically, an EHR environment heightens the need for (i) authentication procedures for users; (ii) protections such as temporary passwords with periodic reauthorizations for limiting access to specific individuals; (iii) standard definitions of minimally necessary information by purpose or type of request, including mechanisms which allow access only for finite times or limit access to specific components of patient medical histories (carte blanche access to a patient's medical record by a health plan would not be allowed); (iv) mechanisms to audit access to information through electronic logs to provide audit trails; and (v) limitations that require special authorizations when payors require access to more extensive longitudinal data or more sensitive medical information.

In summary, an EHR can facilitate access to authorizations or can develop features to reflect minimal necessary standards to access medical information for purposes of payment or health care operations. If the above features are not incorporated in an EHR system, health plans and providers in Illinois will continue to use telephone, fax or paper-based written authorizations.

2.5 RHIO (Scenario 6)

Scenario 6 discussed the participation of stakeholders in a Regional Health Information Organization (RHIO) with participation by multiple organizations in electronic HIE.

2.5.a. Stakeholders

The stakeholders that were solicited for input to this scenario included representatives from commercial payors, and security officers and risk managers from hospitals in both urban and rural settings, public health, law enforcement, pharmacy, clinicians, laboratories, community and health centers.

2.5.b. Domains

The domains addressed in this scenario included:

- Information Authorization and Access Controls
    - Payor will not allow any access to any of their information.
    - Hospitals currently allow access to their EHR from physicians with admitting privileges.
- User and Entity Authentication
    - All stakeholders that allow any access from outside entities currently utilize user login and passwords. Pharmacy stakeholders have randomly assigned passwords.
- State and Federal Law Restrictions
    - The state laws discussed in previous sections would have to be complied with in terms of obtaining the patient's consent or authorization for the particular purpose or use of the type of information being exchanged with a RHIO, to the extent that the information remains identifiable.
    - HIPAA would also require patient authorizations for certain disclosures. A RHIO in possession with significant amounts of electronic data would need to comply with HIPAA Security, either as a covered entity, or as a business associate of various covered entities that are participating in the RHIO.

2.5.c. Critical Observations

Efforts towards RHIO development in Illinois are starting to take shape. For example, the organization Northern Illinois Physicians for Connectivity has held meetings with area stakeholders to begin the framework for RHIO development. As is the case with most RHIOs in their infancy, issues such as the exact mechanisms, policies and procedures for sharing and accessing patient health information, defining who owns the data, and assigning responsibility for data validity, organizational-

level privacy and security of data, appropriate use of data, and breach notification protocols have not been established. Among the stakeholders that were interviewed, there were not currently any business practices surrounding RHIO activities. As the first Illinois RHIOs develop, regardless of the legal structure of the RHIO (e.g., separate corporate entity or contractual venture), the participants of the RHIO would need to enter into a participation agreement that sets forth the agreed upon terms for all of the foregoing.

All of the provider stakeholders stated that, in a hypothetical situation, they would share only the minimally necessary data with other entities unless required to do so by law. However, in the case of RHIO participation, payors stated they would not share any of their proprietary data. Hospitals stated they would be more likely to share information but only among the physicians that have admitting privileges and never with other hospitals. Public health officials said they would only share de-identified aggregated data.

The participation agreement would likely set forth the information that the RHIO would require the participants to share with other participants, as well as define the permitted purposes for which the particular category of information could be accessed by another stakeholder. These "rules of the road" will need to comply with federal and state law, but may require the stakeholders to change their business processes and obtain authorizations from their patients. In addition, they will require a consistent approach among the stakeholder-participants. For instance, for a RHIO to contain as comprehensive a record as possible regarding a patient, a provider will likely need to obtain an authorization from the patient to allow certain sensitive information to be accessed by other providers who are accessing the integrated record, even for treatment purposes. Otherwise, that information will need to be segregated technically from the other, "less sensitive" information. In any case, providers and other stakeholders will need to be cautioned that the "integrated" record being accessed may not be complete in all circumstances.

The statement that provider stakeholders would share only the "minimally necessary" data with other entities may be a hindrance in compiling an integrated record and fulfilling the true potential of the RHIO. If the RHIO is seen as a data repository of patient records, it is serving as a business associate of the providers. The providers should be encouraged (and perhaps mandated to the extent practicable, consistent with the patients' wishes) to submit as much information regarding the patient as possible. Compiling as complete a record as possible is likely to be one of the primary goals of a RHIO and this "disclosure" by a provider to the RHIO does not implicate the "minimum necessary" standard of HIPAA or the authorization requirement of either HIPAA or Illinois law because the disclosure is for treatment purposes. Further disclosures by the RHIO to other stakeholders for other purposes, such as to public health authorities for public health investigations, or to providers for research purposes, or to payors for payment purposes, must take into consideration the relevant body of law and determine whether an authorization is required or preferred. Again, these types of rules would likely be set forth in a participation agreement such that all providers have the same expectations.

As discussed previously with the other scenarios, the use of an EHR system to facilitate the exchange of information can also facilitate the compliance with the relevant state and federal laws and assist in documenting such compliance through the audit and monitoring logs functionality of these software programs.

2.6 Research (Scenario 7)

Scenario 7 discussed the collection of data for an Institutional Review Board (IRB)-approved research project at a medical center involving an investigational drug for children with behavioral health issues. A request in the scenario is made for additional use of the data for research beyond the scope of the original study to include tracking of patients and use of raw data for a white paper.

2.6.a. Stakeholders

The stakeholders that were solicited for input to this scenario included representatives from public health agencies, hospitals and third party payors.

2.6.b. Domains

The domains addressed in this scenario included:

- Information Use and Disclosure
    - Hospitals have policies in place for researchers that request additional tracking outside of approved research protocols. Any request for additional data collection would constitute another study and therefore another IRB review. All clinical investigations require fully informed patient consent and the submission of all forms and consents to the IRB for study approval. The IRB has representatives from health care, medical practice, pharmacy, consumer, and religious advocates.
    - Public health agencies release only aggregated data without patient identification to researchers. Policy is in place for public health agency to institute patient contact if deemed necessary as result of research.
    - Third party payors may have policies in place which prohibit the release any of their data for research purposes, or they may have in place IRB approval processes as described for hospitals, with any changes or additions to studies requiring repeat of the patient authorization process.

2.6.c Critical Observations

Existing legal requirements for IRBs for the approval of all research involving human subjects provide a significant level of protection for the informed consent by participants for the use and disclosure of PHI obtained during research activities.

For example, the HIPAA Privacy Rule requires either the patient/research subject's written authorization or compliance with the Rule's special research provisions establishing conditions for uses and disclosures per IRB/Privacy Board waiver of authorization (including waiver criteria and Common Rule IRB review procedures), and for uses and disclosures for preparatory reviews (e.g., to create the research protocol), and for research solely involving decedent's information. The Privacy Rule builds upon existing Federal "Common Rule" and FDA regulations governing the conduct of human subjects research. (See list of laws creating special protections and protocols for research activities and the use and disclosure of patient information for research included in Appendix 6.)

The Privacy Rule contains provisions addressing information that has been "de-identified", and it also contains special provisions for the use of "limited data sets" without patient authorization for research purposes. The Privacy Rule protections do not extend to de-identified information. A limited data set is information that has been stripped of most of the same identifiers required to be considered de-identified, except that some limited identifiable information may remain, such as certain geographic information and dates. Limited data sets may be used for research without patient authorization if a data use agreement has been entered into between the covered entity and the recipient. Generally speaking, the Privacy Rule provides that research participants be given more information about how their information may be used for research and creates uniform standards that apply, whether or not the research is subject to the existing Common Rule and/or FDA regulations.

The Common Rule regulations apply to human research supported, conducted or regulated by certain federal agencies. The FDA regulations apply to clinical investigations that are under the FDA's jurisdiction (whether or not federally funded). Both sets of regulations require IRB review to ensure minimization of risks, including patient privacy. Both address the use of the informed consent document to inform prospective research participants about a study and require the informed consent document to address how confidentiality will be maintained, and both require an IRB to determine that adequate privacy and confidentiality provisions exist. The Common Rule regulations contain provisions relating to the waiver of informed consent and the criteria that must be met relating to waiver of informed consent. The FDA regulations do not contain a waiver provision (as such is not generally appropriate for clinical research trials); however, there are exceptions for emergency research or use of an investigational product.

As a result of these existing legal requirements, business practices developed for the implementation of research protocols have neutral impact on the implementation of electronic HIE, as those protections would be required to remain in place regardless of format of information. For entities such as third party payors who have made policy decisions to not allow their data to be used for outside research purposes, a more over-arching barrier is present in that such policies to protect proprietary information may prevent participation by such entities in the wider purpose of HIE for any reason, not just research.

Scenario 7 involved a clinical research trial conducted with the information of minor children with private funding from a pharmaceutical company pursuant to IRB review. In applying the legal requirements discussed above, the minor participants' parent or legal guardian would be the person providing informed consent to participate and authorization to use the information for research purposes. The child's assent may also be required by the IRB pursuant to the FDA regulations. With respect to the request to use the information for additional purposes not originally covered in such legal documents, and as noted by the stakeholders, either further authorization or IRB approval (of waiver or alteration of authorization) would generally be required for future uses of PHI that were not previously authorized, such as the investigator's request to extend the research period and/or use the information for a different research purpose.

2.7 Law Enforcement (Scenario 8)

Scenario 8 discussed the interaction of law enforcement and health care providers. In the scenario, law enforcement requested a copy of a patient's blood alcohol test results to investigate an accident, as it was believed that the patient may have been the cause of the accident, and law enforcement would need this information to properly assess the situation. Scenario 8 addressed the possible business practices required in the exchange of health information between a health care provider and law enforcement agencies and the ability of parents to access an adult child's health information.

2.7.a. Stakeholders

The stakeholders solicited for input to this scenario included representatives from urban and rural hospitals and law enforcement. The hospital job functions represented included: compliance, safety and privacy, risk management, health information, and medical records.

2.7.b. Domains

The domain addressed in this scenario includes:

- Information Authorization and Access Controls
    - Health care providers do not provide access to patient information without patient consent, or, in the case of law enforcement, a subpoena. If a subpoena is provided, no patient consent would be required.
    - One provider indicated that documentation of what was released to law enforcement would be kept in the back of the medical records.
- State Law Restrictions/Considerations
    - The Illinois Motor Vehicle Act defines when information can and cannot be released in an accident, and requires disclosure of blood or urine tests performed for individuals receiving medical treatment in a hospital emergency room for injuries resulting from motor vehicle accidents upon police request [*Illinois Vehicle Code*, 625 ILCS 5/11-501.4-1].

2.7.c. Critical Observations

Hospital providers stated they do not give access to parents of patients who are 17 years or older without that patient's authorization. The authorization could be verbal. These stakeholders said that the identity of the insurance guarantor is immaterial to the release of patient information, even if the guarantor is the parent of the patient. Hospital stakeholders reported that patient information, when the patient is a minor and not pregnant, can be released to parents. Stakeholders commented, in this particular scenario, that the parents could only be provided payment information, since the child is 19 years old. This policy would only change if the patient were incapacitated.

The LWG discussed that some of these practices involving the rights of parents and minors may not always be consistent among health care providers, and may not always be in line with legal requirements governing the respective rights of parents and minors with respect to accessing and authorizing the release of health information. For example, generally speaking, once a child is age 18 he or she is able to consent to his or her own medical treatment (and thus control release of such information). In addition, there are a number of state laws governing exceptions to parental consent and control over a minor's health information, depending on the minor's status (e.g., married, pregnant or a parent, etc.) and on the type of health services involved (e.g., mental health, drug or alcohol abuse, sexually transmitted disease, etc.). The statutes are not always clear as to when information either may be released to parents of minors, or when such may either be required or prohibited by a certain statute, and may be subject to differing legal opinions. The introduction of a state-wide information exchange system could present the opportunity to educate and increase awareness and understanding of the law, and to create more uniform practices within a given state. (For further discussion of some of the special laws impacting the respective rights of parents and minors and impacting release of information in Illinois, see discussion included in Appendix 7.)

Appropriate law enforcement agencies can request information, but hospitals may require a formal submission of a subpoena, which might include a copy of the traffic ticket with such a written request. If a subpoena were provided, patient authorization would not be required. Only the information specific to the subpoena would be released. The one provider that indicated that documentation of what was released to law enforcement would be kept in the back of the medical records indicates the degree to which information is siloed in Illinois, and therefore relatively inaccessible for exchange in the paper-culture environment.

Legal drivers for these practices include both HIPAA as well as the Illinois Motor Vehicle Act. In connection with this particular scenario, HIPAA permits release of information for payment purposes and to persons involved in the patient's treatment or payment for such treatment. The Illinois Motor Vehicle Act further defines when information can and cannot be released in an accident, and requires disclosure of blood or urine tests performed for individuals receiving medical treatment in a hospital emergency room for injuries resulting from motor vehicle accidents upon police request [*Illinois Vehicle Code*, 625 ILCS 5/11-501.4-1].

One law enforcement stakeholder participant noted that "DUI packages" are often carried by police officers. These packages contain the appropriate paperwork law enforcement needs to request from providers for the release of test results for a patient involved in an accident when alcohol or drug use is suspected.

Therefore, applying applicable Illinois laws, since this scenario involved ER treatment of a motor vehicle accident, law enforcement would be able to obtain patient test results without a subpoena to determine if the patient were under the influence of drugs or alcohol. Under HIPAA and Illinois law, however, the parents would not be entitled to obtain the test results due to their parental status because the patient is over 18 years old. There is no indication that the parents are seeking the information for "payment" purposes, or that the adult child has consented (verbally or otherwise) to the disclosure of the drug test results to the parents, or that the adult child is unconscious or unable to consent (or not) to the disclosure, or that such disclosure is necessary for treatment purposes or to the parents involvement in the care. Thus, consistent with the stakeholders' responses, it would be most appropriate to refrain from disclosing the son's test result information without his agreement or assent.

2.8 Prescription Drug Use/Benefit (Scenarios 9 and 10)

Scenarios 9 and 10 discussed Prescription Benefits Manager's (PBM) business practices and policies associated with the exchange of health information with providers. Scenario 9 discussed the interaction between a PBM and an outpatient clinic. In order for the patient to receive the physician-prescribed medication that is not on the PBM, list of preferred antipsychotic the physician is required to complete a prior authorization. Scenario 9 addressed the business associate agreements that would need to be in place between the PBM and the provider.

Scenario 10 discussed the interaction of PBM1 with Company A who is considering switching services from PBM2 to PBM1 for costs savings purposes. PBM1 required access to employee's prescription drug use and associated drug costs to review and effectively assess the situation to provide a cost savings comparison to Company A. Scenario 10 addressed the business associate agreement that would need to be in place between Company A and the PBMs.

2.8.a. Stakeholders

The stakeholders that were solicited for input to this scenario included pharmacies.

2.8.b. Domains

The domain addressed in this scenario includes:

- Information Use and Disclosure
    - The PBM would only have access to de-identified patient data. The PBM would be required to have a business associate agreement with the provider in order to obtain this information. The information shared would be limited by the minimum necessary guidelines under HIPAA.
- User and Entity Authentication
    - The pharmacy system is set-up with limited access by job function. User ID and passwords are randomly generated and assigned.
    - Suspicion of fraudulent access will warrant physician verification. Pharmacies typically are able to authenticate physician identities by referring to a linked database, which includes physicians across the country.
- Administrative or Physical Security Safeguards
    - One pharmacy participant indicated that the physical access to pharmacy data is secured "between four walls and a locked door."
- Information Transmission Security or Exchange Protocols
    - Transmission of data between pharmacy and physician offices is often sent via a secure FTP website and is encrypted.

2.8.c. Critical Observations

HIPAA does not allow for any HIE between companies that do not have business associate agreements. Scenario 9 involved a hospital employee covered under the hospital's self-insured group health plan. The group health plan would be subject to the HIPAA Privacy Rule requirements. As such, it would presumably have a business associate agreement in place with the Pharmacy Benefit Manager that provided for the use of PHI for specified purposes. The prescribing physician was asked by the group health plan's business associate to complete an authorization form in order for the prescription to be filled and paid for. The prescription appeared to have been made in connection with the provision of mental health services. The purpose of the request for information was related to the provision of treatment and the group health plan's payment for the prescription. If the information requested on the authorization form requested by the PBM included the type of information that the applicable state's law requires a certain form of patient authorization to release for this purpose, the provider would have to have obtained that form of authorization from the patient. Again, obtaining such forms at the point of service would be consistent with what seems to be a growing practice in Illinois. Under HIPAA, only the minimum necessary information should then be released, unless the patient had authorized otherwise. With the prospect of national HIE involving differing state laws, the concept of incorporating a process that permits providers to obtain necessary authorizations from the patient at the point of service would facilitate appropriate HIE.

Scenario 10 involved a business relationship between Company A (presumably a covered entity or a business associate of a covered entity) and two different PBMs. PBM 1 was asked to provide services involving data analysis of claims information for cost-savings purposes. PBM provided electronic claims processing services for Company A. HIPAA requires business associate agreements requiring the business associates to appropriately safeguard PHI received and used in order to provide covered services to the covered entity. In the scenario, it appeared that PBM 1 requested Company A to forward the same claims information that PBM 2 used in connection with its claims processing functions. Questions raised by this scenario included whether a more limited scope of patient information (perhaps redacted or de-identified) would suffice for PBM 2 to perform its data analysis services, and whether such could be technologically accomplished and/or economically feasible.

2.9 Healthcare Operations/Marketing (Scenarios 11 and 12)

Scenarios 11 and 12 discussed health care providers' policies on marketing services to targeted subsets of patients. Scenario 11 identified an integrated health delivery system (IHDS) consisting of critical access hospitals and a large tertiary hospital. The IHDS wanted to use patient identifiable data from the critical access hospitals to target market patients in need of the new rehab services available in the tertiary hospital. Scenario 11 addressed the possible business practices that would be required if a healthcare provider conducted marketing using PHI with their consumers.

Similarly, Scenario 12 discussed the interaction of a hospital obstetrics department with the marketing department. The marketing department requested patient identifiable data (including patient outcome) for the following purposes: to be able to market new pediatric services; to solicit for parenting classes; to raise funds for a neonatal intensive care unit; and to sell to a local diaper company so they can market their products. Scenario 12 addressed the use and sale of identifiable patient data for marketing and fundraising purposes.

2.9.a. Stakeholders

The stakeholders solicited for input to this scenario included representatives from urban and rural hospitals. The hospital job functions represented included: compliance, safety and privacy, risk management, health information, and medical records.

2.9.b. Domains

The domains addressed in this scenario include:

- Information Use and Disclosure Policies
    - Stakeholders reported that HIPAA allows providers to market or initiate fundraising efforts using only de-identified patient data (or only patient demographics) as long as patients receive a notice of privacy and are given an opportunity to sign an "opt-out clause."
    - Health care providers do not sell patient data under any circumstances.
- Information Transmission Security or Exchange Protocols
    - If an outside marketing service is used, a business associate agreement must be in place between the provider and the marketing organization.
    - When an outside marketing service is used, only de-identified or patient demographic data is exchanged. The data would be sent using a secure FTP server or through U.S. mail on an encrypted CD.

2.9.c. Critical Observations

Responses given by the stakeholders indicated that there are varying interpretations on HIPAA guidelines for operations and marketing purposes even though providers often referred to HIPAA guidelines as the basis for their marketing practices and policies.

Under HIPAA, providers must obtain patient authorization for "marketing" (other than face-to-face communications or promotional gifts of nominal value), and the authorization must state if the marketing is expected to result in remuneration from a third party. The Privacy Rule requires patient authorization even if the "marketing" disclosure is made to a business associate. However, under HIPAA, the definition of "marketing" does *not* include communications that describe a health-related product or service provided by the entity making the communication or communications for the individual's treatment, case management or coordination of care, such as to direct or recommend alternative treatments, therapies, health care providers, or settings of care.

HIPAA's "fundraising" provisions permit uses and disclosures of only limited information (demographics and dates of care provided) without patient authorization if the provider has included a statement in its Privacy Notice stating that it may contact the individual to raise funds, and then provides the opportunity to opt out of future fundraising communications with any fundraising materials.

Therefore, applying HIPAA principles to Scenario 11, the integrated health care delivery system would be able to distribute brochures describing its new rehab center and enhanced services to its patients without patient authorization because communications concerning its own products and services are not considered "marketing." Under Scenario 12, the hospital's marketing department would be able to use patient information to provide information on hospital services and parenting classes without patient authorization, but it would need the patient's authorization to use PHI (other than the limited demographic and dates of care) to request donations as well as to sell information to a local diaper company.

Of course, if any of the information was afforded extraordinary protections under other state or federal law (e.g., mental health, substance abuse treatment, HIV or genetic testing information), those more stringent laws requiring patient consent/authorization would need to be complied with, even if HIPAA would otherwise permit the marketing or fundraising use or disclosure.

Stakeholders identified further business practices associated with Scenario 12. If an outside organization were used for marketing, that organization would be required to be in a business associate agreement with the provider and adhere to HIPAA compliance issues. An outside marketing service would only be provided non-identifiable patient data, and the data would be sent either using a secure FTP server or via U.S. mail on an encrypted CD. The requirement for the development of business associate agreements presents a barrier for the implementation of HIE initially, but once executed, should facilitate the standardization of HIE.

If a patient indicates he/she would not like their contact information used for marketing purposes, that is brought to the corporate compliance officer's attention who will inform the marketing department. The steps taken to inform the marketing department would most likely differ from organization to organization.

The providers contacted stated that they do not sell patient data to outside entities for marketing purposes.

2.10 Bioterrorism Event (Scenario 13)

Scenario 13 discussed the reporting of and response to a laboratory-confirmed case of anthrax.

2.10.a. Stakeholders

The stakeholders that were solicited for input to this scenario included representatives from hospitals, public health agencies, and emergency medical services.

2.10.b. Domains

The domains addressed in this scenario included:

- User and Entity Authentication
    - Initial reports by providers to local health departments of immediately notifiable conditions such as a case of anthrax are most often handled by telephone and fax.
    - Reporting of notifiable conditions is a routine part of providers' business practices, and telephone and fax numbers, as well as personnel involved on both the private and public side, are well known to those responsible for providing and receiving reports.
    - Telephone contacts between parties are used to notify intent and confirm receipt of fax.
- Information Authorization and Access Controls
    - State laboratory provides complete patient information results for patients with anthrax confirmation only internally to IDPH Communicable Diseases Section.
- Information Transmission Security or Exchange Protocols
    - Routine practices for assuring telephone numbers and fax machine security would be used. Use of e-mail would be restricted to information without patient identifiers included.
    - Encrypted messaging from the Illinois National Disease Surveillance System to CDC is in development, but not currently available.

- State Law Restrictions/Considerations
    - In Illinois, the Communicable Disease Report Act, [745 ILCS 45], and the Control of Communicable Disease Code, [77 Ill. Adm. Code 690], require that reporting entities report certain diseases and conditions to IDPH, including suspected and/or confirmed acts of bioterrorism.
- Information Use and Disclosure Policy
    - Standard patient authorizations allow use and disclosure of all patient information for public health purposes.
    - State statutes for response to public health emergencies such as incidents of bioterrorism allow the disclosure of patient information to law enforcement.

2.10.c. Critical Observations

Actual bioterrorism events are unprecedented in Illinois, and as such, no routine business practices existed for critical analysis. As a proxy for such a public health emergency event, routine practices for interacting with public health in time-sensitive situations were discussed for this scenario. One of the tenets of bioterrorism preparedness is that development of routine person-to-person contacts and relationships between providers and public health personnel will aid in the rapid dissemination of information in the event of a public health emergency precisely because those involved will know "who to call." This relationship-building for emergency preparedness is neutral with respect to the implementation of electronic HIE.

Illinois has implemented an electronic disease reporting system (Illinois National Electronic Disease Surveillance System, or INEDSS) that is currently deployed to all local health departments, as well as to a significant proportion of large hospitals. It was developed to Public Health Information Network (PHIN) standards, and as such should be an aid to the implementation of electronic HIE due to its compatibility to such standards. However, the module specific for the reporting of bioterrorism events in INEDSS is still under development. Providers stated that despite the availability of an electronic reporting medium such as INEDSS, an extreme public health emergency event such as possible bioterrorism would necessitate the use of telephone contact until time was available to perform data entry into the system. Rather than the business practices of telephone contact, it is this current state of disjointed information systems which require separate data entry which comprises a significant technological barrier for electronic HIE.

The Illinois Department of Public Health (IDPH) is required to investigate the causes of and take measures to restrict and suppress diseases [20 ILCS 2305/2]. In order to prevent the spread of a dangerously contagious or infectious disease, IDPH, local boards of health and local public health authorities have emergency access to medical or health information or records or data upon the condition that the privacy and confidentiality of the information or records or data obtained shall protected. Any information, records or data accessed during an emergency is exempt from disclosure under the Freedom of Information Act and is neither admissible as evidence nor discoverable in any court proceeding, except for court proceeding held pursuant to the Department of Public Health Act. Further, the privileged quality of communication between an individual and any health care professional or facility does not constitute grounds for failure to provide emergency access to an individual's health information or records [20 ILCS 2305/2(h)].

IDPH has adopted the Communicable Diseases Code (Code) (77 Ill. Adm. Code 690) which requires health care providers, laboratories and other reporting entities to report the existence of any of the diseases, illnesses or conditions listed in the Code, including bioterrorism events, to local health authorities who, in turn, report the same to IDPH. The Code provides, among other things, that such reports shall be confidential and not subject to disclosure.

The HIPAA Privacy Rule provides exceptions to the consent and authorization requirements for uses and disclosures required by law, uses and disclosures for public health activities and for health oversight. Thus, the Privacy Rule supports IDPH's continued ability to receive health information related to the mandated reporting of diseases, injury, and vital events as well as the IDPH's collection of data related to preventing or controlling injury, disease, vital events, public health surveillance, investigation and intervention. In addition, the Privacy Rule allows covered entities to provide to a public health authority, such as IDPH, information about an individual exposed to a communicable disease or who may otherwise be at risk of contracting or spreading a disease or condition. In Illinois, the Communicable Disease Report Act, [745 ILCS 45], and the Control of Communicable Disease Code, [77 Ill. Adm. Code 690], require that reporting entities report diseases and conditions to IDPH. Accordingly, the mandated reporting and the related provisions in the Privacy Rule clearly require all reporting entities to continue their practice without restrictions, and does not require further contractual agreements. As noted above, the Control of Communicable Diseases Code requires the reporting of bioterrorist threats or events. It follows, therefore, that mandatory reporting during a bioterrorism event or other public health emergency would be permitted if certain privacy rule requirements are met under the HIPAA and the Privacy Rule.

Recent guidance issued by the U.S. Department of Health and Human Services indicates that the Privacy Rule does permit covered entities to disclose PHI, without individuals' authorization, to public officials responding to a bioterrorism threat or other public health emergency. The guidance indicates that the Privacy Rule permits covered entities to disclose needed information to public officials in a variety of ways. Covered entities may disclose PHI, without the individual's authorization, to a public health authority acting as authorized by law in response to a bioterrorism threat or public health emergency. The Privacy Rule also permits a covered entity to disclose PHI to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism. In addition, disclosure of PHI, without the individual's authorization, is permitted where the circumstances of the emergency implicates law enforcement activities, national security and intelligence activities, or judicial and administrative proceedings.

2.11 Employee Health (Scenario 14)

Scenario 14 discussed an employee's request for a return-to-work document after presenting at a local emergency department for treatment of a chronic condition and the mode of information transmission to the employer.

2.11.a. Stakeholders

The stakeholders that were solicited for input to this scenario included representatives from hospitals in both urban and rural settings, public health, clinicians and community and health centers.

2.11.b. Domains

The domains addressed in this scenario included:

- User and Entity Authentication
    - Stakeholders stated that identification of a patient who requests the return-to-work documentation via the telephone is authenticated by the patient providing their treatment date and social security number.
    - Employer stakeholders stated that they authenticate the source of the return-to-work document by the letterhead on which the document is printed.
- Information Authorization and Access Control
    - Employee personnel records are maintained in an information management system distinct from employee health records, and human resources managers do not have access to employee health records.
- Information Protections (from improperly modifications)
    - Stakeholders do not take any specific steps to protect return-to-work documents from being improperly modified by employee.
- Information Transmission Security or Exchange Protocols
    - Stakeholders stated that return-to-work documentation is given directly to patient in person or faxed to number given by the patient. No stakeholder had transmitted a document via email.
    - Stakeholders with EHRs do not cut and paste clinical information, either a software-generated form is created, or a hand written form is given to the patient.
- Information Use and Disclosure
    - Stakeholders stated that only the patient can initiate a return-to-work request, employers couldn't request the documentation without the employees consent.

- Stakeholders will list only actual diagnosis on return-to-work statement if explicitly requested by the patient. Otherwise, the "minimum necessary" information for one organization included the dates of treatment, date allowed to return to work, and any physical limitations.

2.11.c. Critical Observations

Hospital stakeholders with an EHR stated that they would not cut and paste any information from the EHR; however, some EHRs have a software-generated letter on the hospital's letterhead that contains the minimum necessary information that includes treatment date(s), return-to-work date and any physical limitations. Stakeholders without an EHR stated that they use standard forms with hospital logo that contain the minimum necessary information, treatment dates(s), return-to-work dates and any physical limitations.

All stakeholders stated that they use only one of two modes of transmission for the return-to-work document: handed to the patient, or faxed to a number provided by the patient. E-mail transmission has not been utilized by any of the stakeholders interviewed.

All stakeholders interviewed stated that a patient has to initiate the request for return-to-work documentation; employers are not able to directly request the information, as the patient's authorization would be required by HIPAA.

2.12 Public Health (Scenarios 15-17)

Scenario 15 discussed the public health response to an active tuberculosis carrier that has taken a bus trip across state lines. Scenario 16 discussed the public health response to a positive laboratory result in state-mandated newborn screening tests for genetic/metabolic or endocrine disorders. Scenario 17 discussed issues concerning the transfer of a homeless person from a county shelter to a hospital-affiliated drug treatment clinic.

2.12.a. Stakeholders

The stakeholders that were solicited for input to these scenarios included representatives from hospitals, a homeless shelter, public health agencies, and behavioral health services.

2.12.b. Domains

The domains addressed in this scenario include:

- User and Entity Authentication
    - Public health personnel have established working relationships and corporate contact information for telephone, e-mail and fax machines is readily available.
    - Business practices for the reporting of newborn screening tests include only public health personnel, the hospital where the baby was born, and the attending physician. No Interactive Voice Response (IVR) system exists in Illinois.
- Information Authorization and Access Controls
    - Patient authorization is required for release of any PHI that would be transmitted between homeless shelters and drug treatment facilities
- Information Transmission Security or Exchange Protocols
    - Facsimile transmissions are secured via telephone notice of intent to send and follow up call to assure receipt.
    - E-mail encryption is not used, so patient identifiers are excluded from e-mailed communications.
    - State laboratory results for newborn screening tests are maintained in a mainframe database and therefore can be transmitted only by extraction into another format or hard copy.
    - Commercial laboratory results for newborn screening tests can be supplied to hospital information systems via secured electronic laboratory reporting, which are then accessed by attending physicians.
- Information Audits and Record and Monitor Activity

- Communications from a health department to another entity that occur by facsimile transmission are confirmed by a follow-up telephone contact to assure transmission to the correct entity.

- Administrative or Physical Security Safeguards

  - Caseworkers who perform intake interviews of homeless persons entering shelters collect some PHI required for the management of the cases. Such information is paper-based and secured in physically locked cabinets within a locked room to keep separate from facility and access by any others besides the caseworkers.

- State Law Restrictions/Considerations

  - In Illinois, the Communicable Disease Report Act, [745 ILCS 45], and the Control of Communicable Disease Code, [77 Ill. Adm. Code 690], require that reporting entities report certain diseases and conditions to IDPH, including tuberculosis and laboratory-confirmed genetic/metabolic disorders in newborns.

- Information Use and Disclosure

  - State statutes for disease control include procedures for the transmission of information to enforcement agencies outside of public health, such as the State's Attorney's Office.

  - Both state and local health departments stated they would not communicate with a private business entity, such as the bus company involved in the transport of the TB carrier, if obtaining any information helpful to the disease investigation was improbable. Information exchange could and would take place if such an entity could assist in the disease control investigation, e.g., an airline.

  - All disclosures of PHI to relatives occur only with express written consent of patient.

  - Release of PHI for payment of treatment services follows minimally necessary information guidelines.

2.12.c. Critical Observations

HIPAA permits uses and disclosures without patient authorization for public health and health oversight activities, to avert serious health or safety threats, and for national security activities. Disclosures to public health authorities are made for the purpose of preventing or controlling disease, and include reporting diseases and public health surveillance and interventions. In Illinois, the Communicable Disease Report Act, [745 ILCS 45], and the Control of Communicable Disease Code, [77 Ill. Adm. Code 690], require that reporting entities report diseases and conditions to IDPH. The minimum necessary standard applies to public health disclosures. Permitted uses and disclosures for health oversight include government benefit programs for which health information is relevant to beneficiary eligibility and government regulatory programs in determining compliance with program standards, and de-identified information may be sufficient for the purpose of the use or disclosure

under these provisions. Disclosures made to prevent or lessen serious and imminent health or safety threats may involve a small number of people or a public health or national emergency.

To the extent that the subject information being requested or released in these scenarios may trigger the special protections of certain state or federal laws (e.g., the federal and state laws protecting federal and state funded substance abuse treatment programs in Scenario 17), such particular laws would have to be taken into account in determining whether a particular disclosure could be made without the patient's consent (e.g., redisclosure of program treatment services information by the homeless shelter to someone claiming to be a homeless man's relative would presumably require the individual's consent, as would disclosures by treatment programs for payment purposes, with an exception for inter-program disclosures and disclosures to entities having administrative control over the program).

Stakeholders reported variability in interpretation of "minimum necessary" information for release between entities. Authorizations, when deemed necessary, are carefully sought, but not so carefully explained. Entities requesting information can be given wide latitude in what is being requested, such as with "fill-in-the-blank" forms, with patient allowing or disallowing by simple check boxes. This approach to authorization is neutral with respect to electronic HIE.

Professional relationships were reported by the stakeholders to be key to public health and to disease control and response activities. These relationships provide the platform for information exchange during a public health response. However key these relationships are to the success of public health response, they are neutral with respect to electronic HIE. On the contrary, it is widely regarded that functional electronic HIE will facilitate public health response.

Electronic, as opposed to paper, health information is developing in Illinois in a fragmented manner, with an apparent lack of planning for an overall strategic, statewide health information network. This fragmentation is a major barrier for implementation of information exchange, as significant resources are being brought to bear at isolated institutions, creating more and more systems that may or may not be interoperable with respect to information exchange.

2.13 State Government Oversight (Scenario 18)

Scenario 18 discussed a request by a state governor for PHI about immunization and lead screening of children to be supplied to researchers at a state university for analysis. In the scenario, there existed neither a legislated mandate for the consolidation of this data, nor a contract with the university to provide analytical services.

2.13.a. Stakeholders

The stakeholders that were solicited for input to this scenario included representatives from public health agencies and hospitals.

2.13.b. Domains

The domains addressed in this scenario included:

- Information Authorization and Access Controls
    - Information from the statewide immunization registry can be supplied to researchers, but only in aggregate form without patient identifiers.
    - Without statutory requirement for the provision of the data, collection and consolidation of such information would then be defined as a research protocol and subject to legal and IRB review and approval prior to participation.
- Information transmission security or exchange protocols
    - Blood lead screening laboratory test result information is provided currently by the state public health laboratory to other involved state agencies only by transfer to disk format and courier delivery.
- Information Use and Disclosure
    - All HIPAA guidelines on patient authorization for information use and disclosure would apply to the research protocols established to execute this scenario.

2.13.c. Critical Observations

This scenario was interpreted by working group participants as a theoretical research proposal, rather than legitimate governmental oversight function. This interpretation is due to the lack of a statutory requirement for the consolidation of data that would then be supplied to an agency external to the agencies that collected the data. (HIPAA permits disclosures without patient authorization for activities that are authorized by law or other oversight activities necessary for appropriate oversight of the health care system (e.g., government benefit or compliance programs. Disclosures are generally limited to that which is authorized or required by the applicable law.) Policies developed for business practices related to research which utilizes PHI are generally neutral with respect to the implementation of electronic HIE, as the federal and state statutory requirements for the protection of

research participants and their health information do not change with respect to format of the information.

2.14 Summary of Critical Observations and Key Issues

The assurance of security and privacy are critical to the successful proliferation of HIE in Illinois and throughout the country. If the public does not feel its health information is safe and kept confidential, the movement towards HIE will be hampered at best and most likely impeded completely, no matter how great the possibilities are to improve quality of health care in the state. Currently, Illinois is at the infancy of HIE development among its health care organizations. Major privacy and security-related barriers currently exist. For example, the wide range of interpretation of HIPAA's "minimum necessary" clause for the same scenarios among organizations is a barrier to HIE as it will be difficult to exchange information if parties cannot agree on what is appropriate to exchange. Inconsistent application of legal principles are not unique to Illinois, and the future institution of either a state or national information exchange mechanism will provide an opportunity to educate health care providers and others on legal requirements and good clinical practices associated with maintaining and appropriately releasing patient information for appropriate purposes. Education and awareness should be viewed as a means to encourage universal HIE. It is an encouraging finding of this report that there is a high level of existing awareness and adherence to strict confidentiality standards by health care providers and other stakeholders in Illinois. In analyzing potential legal "barriers" to HIE, the various state (and federal) laws that provide protections and extraordinary protections for health information should not be viewed as "barriers," but rather the existence of, appropriate application of and education in such laws need to be addressed in creating the framework for national information exchange. Using technology to further existing privacy and confidentiality protections should be viewed as a means of promoting confidence and participation in national electronic HIE, and also not viewed as a barrier. Also, because of the competitive nature of the health care market in Illinois, the culture has not been conducive to data sharing. Silos of technology have formed, but there has been no real driving force promoting the sharing of data among organizations. As such, policies and procedures surrounding inter-organizational HIE are greatly lacking. By identifying issues like these and subsequently providing practical solutions, HISPC and efforts like it will have a positive impact on increasing HIE and ultimately improving the quality of health care in Illinois.

3.0 Analysis of Solutions

The VWG, along with over twenty (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 appeared regardless of the level of technology available to an organization. The varying array of interpretation and sometimes misinterpretation of HIPAA was 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.

3.1 Summary of Key Findings from the Assessment of Variation

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 they relate to electronic HIE. In comparing organization to organization, this study found significant variations in practice due to varying interpretations of privacy and security protections. In addition, silos of technology utilization are found throughout Illinois. Many health care organizations have been able to incorporate significant technological resources to maintain and protect patient data within their organizations. This is particularly true of the major urban health care facilities in the Chicago area. However, very little effort has gone into enabling organizations, through either technical or procedural standardization, to share data electronically with one another. The most salient reason 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 will need to come together before the policies and procedures necessary to facilitate HIE begin to become more commonplace.

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.

In identifying organizational-level practices, there were 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 identified was 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 indicated that they provide 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.

3.2 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 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 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 8: 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 9: 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 SWG, 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
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, MPA, RHIA, CSL, CPHQ	Professional Dynamic Network	HIM Expert/IHEMA
Rachelle Stewart, DrPH, RHIA	University of Illinois at Chicago	Academic HIM
Vernel Johnson, MD	St. James Hospital	Emergency Medicine

Committee Members	Organization	Area/Industry of Expertise
Neal Zeigler, MD	Baylor Medical Center	Emergency Medicine

Charge of SWG: The SWG is responsible for developing a detailed report on the proposed solutions to privacy and security issues that impact the widespread 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, LWG, and HSC. The lists of all solutions generated can be found in Appendix 10: 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 11: Prioritization of Solutions for the Implementation of HIE in Illinois.

The EHRTF served as the reviewing body for the proposed solutions. The solutions were vetted and evaluated by EHRTF prior to implementation planning. Taskforce membership included 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 ensured the solution reviewing process was 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 11: Prioritization of Solutions for the Implementation of HIE in Illinois, under Weighted Criteria Column B, Maximize Feasibility.

3.3 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. A comprehensive approach will be absolutely necessary in order to overcome the silos of technological development currently present in Illinois, as well as capitalize on the ongoing, but sporadic, initiatives taking place in HIE development. 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 or given incentives 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, the 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 HIE, the SWG focused its efforts on analysis of root causes of barriers. This facilitated the development of cross-cutting solutions across barrier groups, domains, stakeholders, feasibility barriers, and solution types. The degree to which the solutions cross-cut these various aspects is seen in the Matrices following. Solutions with the greatest potential for cross-cutting impact would be for the development of professional standards for privacy and security officers, inclusion of privacy and security legal expertise in the lead agency for HIE development, and the development of core competencies for staff education. 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

Most of the solutions prioritized for consideration of implementation addressed more than one barrier to effective HIE. The following matrix illustrates the various barriers addressed by each proposed solution.

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		
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

In addition to cross-cutting activity to address barriers to HIE, the proposed solutions had over-arching impact in regards to the domains of security and privacy as defined by RTI. The following matrix illustrates the various domains addressed by each proposed solution.

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

	Domains								
Solution	**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	X	X	X	X	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

A direct result of the effort of the SWG to find solutions for root causes to barriers of HIE led to the creation of solutions which impacted a wide variety of stakeholders. The following matrix illustrates the various stakeholders impacted by each proposed solution.

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

Barriers to the feasibility of implementation of the proposed solutions were defined by the SWG, LWG and HSC. Due to the over-arching nature of the proposed solutions, all had multiple barriers to their feasibility which will need to be addressed in any implementation plan developed for them. The following matrix illustrates the various feasibility barriers for each proposed solution.

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

RTI defined various solution types for any solution developed nationwide in the HISPC project. The following matrix summarizes the cross-cutting relationships between the proposed solutions and RTI's solution types, and each is discussed in detail in the following sections.

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							
Solution Type	**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: Business agreements, and uniform patient consent/authorization forms								
6: Solutions that would require changes in existing state law/regulations						X		
7: Solutions that would require new state laws/regulations								X
8: Solutions that would address issues of non-compliance with state laws/regulations			X	X				X
9: Education solutions to address misinterpretations of state laws/regulations			X	X				
10: Solutions applicable to general privacy/security federal laws and regulations (e.g. HIPAA Privacy, HIPAA Security)								X
11: Solutions applicable to state programs (e.g., Medicaid)								
12: Solutions that would address issues of non-compliance with federal laws/regulations (such as non-compliance with HIPAA Privacy, HIPAA Security)			X	X		X		X
13: Education solutions to address misinterpretations of federal laws/regulations			X	X				
14: Solutions affecting Interstate Health Information Exchanges								X

3.3.1 Solutions to variations in organization business practices and policies

Solution types as defined by RTI to address variations in organization business practices and policies include:

- Governance-related solutions
- Business arrangement solutions
- Technical solutions
- Guidance/education solutions that address misinterpretation issues
- Business agreements and uniform patient consent/authorization forms

The solutions proposed by the SWG which fit these solution types included all solutions except for Solution 6. Governance for HIE has yet to be defined comprehensively for Illinois; however, three solutions make specific recommendations for that governance once it becomes defined: to benchmark regional exchange criteria (Solution 1), to provide recommendations for multidisciplinary teams for the acquisition of HIT (Solution 7), and for legal expertise in privacy and security to guide integrated statewide efforts for HIE implementation (Solution 8). The recommendation for multidisciplinary teams for HIT acquisition also falls within the business arrangement solution type, as it speaks to the need for organizations to address directly the multi-stakeholder impact of HIE implementation, and meet the needs of those stakeholders through representation that may require review of existing organization infrastructure and/or out-sourcing of functionality. Solution 2 speaks directly to the technical solution of the development of a universal standard for patient identification, and Solution 7 has a technical component in that the ultimate result of the implementation of HIT acquired with the use of a multidisciplinary team will have better defined technical solutions to any barriers to HIE identified by the team. Solutions 3, 4 and 5 all relate directly to guidance or education solutions aimed at standardizing procedures and increasing the competencies in privacy and security protection for those who provide the organizational infrastructure for protection (the privacy and security officers), those who enact the policies and procedures for protection (the staff), and those who have health information to protect (all consumers).

3.3.2 Solutions to issues derived from state privacy and security laws/regulations

Solution types as defined by RTI to address variations in practices related to state laws and/or regulations include:

- Solutions that would require changes in existing state laws/regulations, e.g., draft model legislation
- Solutions that would require new state laws/regulations
- Solutions that would address issues of non-compliance with state laws/regulations
- Education solutions to address misinterpretations of state laws/regulations

The over-arching goal for solutions considered by the SWG to overcome legal barriers to HIE was to create a desired end-state of state legislation and enforcement that is clear, complete and timely (see Appendix 10 for the complete list of solutions considered). After review of business practice variations and legal drivers, the SWG concluded the foremost legal issue concerning privacy and security protection in HIE was not the current state of state laws and regulations, but rather non-compliance and/or misinterpretation of existing laws. Therefore, the solutions proposed by the SWG which fit these solution types which target state laws and/or regulations primarily focused on the need

for education for both professional staff and consumers in privacy and security practices and protections currently in place (Solutions 3 and 4). In addition, it was determined to be of high priority to include legal expertise in privacy and security in whatever governance was put in place to guide integrated statewide efforts for HIE implementation Illinois (Solution 8).

3.3.3 Solutions to issues driven by intersection between federal and state laws/regulations

Solution types as defined by RTI to address variations in practices related to the intersection of state and federal laws and/or regulations include:

- Solutions applicable to general privacy/security federal laws and regulations (e.g., HIPAA Privacy, HIPAA Security)
- Solutions applicable to state programs (e.g., Medicaid)
- Solutions that would address issues of non-compliance with federal laws/regulations (such as non-compliance with HIPAA Privacy, HIPAA Security)
- Education solutions to address misinterpretations of federal laws/regulations

Solution 6 proposes that the Stark and Anti-kick back relief regulations that currently allow for the donation of software and in some cases, hardware and training by hospitals to physician practices, be extended and promoted such that hospitals are allowed and possibly induced and/or provided incentives 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 would require changes to federal legislation and coordination with State's Attorneys for implementation. The SWG considered such a "Robin Hood" approach to resource re-distribution capable of significant impact on the implementation of EHR and HIE for historically underserved populations. Solutions 3 and 4 propose educational initiatives to address all aspects of security and privacy protection, and thus would address issues of misinterpretation and non-compliance with federal laws and/or regulations just as they would for state laws and regulations. The inclusion of legal expertise in privacy and security in whatever governance that will be put in place to guide integrated statewide efforts for HIE implementation Illinois (Solution 8) would also facilitate the compliance with existing or implementation of new federal regulations.

3.3.4 Solutions to Enable Interstate e-Health Information Exchanges

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. The inclusion of legal expertise in privacy and security in whatever governance that will be put in place to guide integrated statewide efforts for HIE implementation Illinois (Solution 8) has the potential to have the most significant impact on interstate e-HIE, in that this expertise will also be applied in the alignment of statewide legal initiatives with national legal initiatives, thus facilitating interstate exchange.

3.4 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. Whereas it is possible that states might come to interoperability standards without recourse to federal intervention, the likelihood of this is slim considering the diversity of HIT and HIE implementation nationwide. 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. Again, it is possible that states could achieve this type of standardization without recourse to federal intervention. However, again, this is unlikely to occur in a timely fashion.

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 or given incentives 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.

3.5 Conclusions and Next Steps

Analysis by the VWG revealed few specific barriers to electronic HIE, primarily because so little electronic exchange is occurring currently in Illinois. What assessment of the variations in business practices and legal drivers in Illinois for HIE did reveal was a strong culture for the protection of the privacy and security of health information: a culture, in fact, that has not been not conducive to data sharing. Information has been often deemed as proprietary and a business asset as opposed to an opportunity to improve quality of care and patient safety. Furthermore, the development of an over-protective culture based on misinterpretation or over-application of legal drivers contributes further to this paucity of information exchange. Although there is evidence that this culture is shifting, as indicated by the various EHR and HIT initiatives occurring in the state, the shift is currently slow and sporadic. The cultural change and technical infrastructure necessary for sharing information will need to come together before the policies and procedures necessary to facilitate HIE begin to become more commonplace.

The solutions developed by the SWG for this project, based on the real-world practices revealed by the VWG, reviewed for legal drivers by the LWG, and thoroughly vetted by the stakeholder and HIT communities, have the capacity to provide a multi-pronged leverage for the instigation of the needed culture change towards widespread electronic HIE in Illinois that will still continue to protect the privacy and security of health information. The Implementation Planning Working Group (IPWG) will be responsible for developing a detailed report on the implementation of the proposed solutions to the privacy and security issues discussed in this report that impact the widespread electronic exchange of health information among organizations in and around the state of Illinois. Please note, the SWG and the IPWG are actually the same team serving dual functions as it was deemed more practical to have the same people who derived the solutions be the ones to specify how they should best be implemented. The implementation plans developed by the IPWG will be prioritized and discussed in order according to the hierarchy of influence for the eight solutions as determined by the SWG. This hierarchy was determined by inter-relationship analysis of all the solution areas by the SWG, and this analysis revealed 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 will define the structure for the discussion of the implementation plans, as focus for action will be put upon those driving activities most likely to leverage development, and major outcomes will become key indicators of successful development.

4. Appendices

1. HISPC Steering Committee Roster and Charter
2. HISPC Variations Working Group Roster and Charter
3. HISPC Legal Working Group Roster and Charter
4. HISPC Solutions and Implementation Planning Roster and Charter
4. Health Information Exchange Scenarios
5. Confidentiality Protections in Illinois
6. Illinois Special Records Protections
7. Barriers to the Implementation of e-HIE in Illinois
8. Root Causes of Barriers to the Implementation of e-HIE in Illinois
9. Solutions for Root Causes of Barriers to the Implementation of e-HIE in Illinois
10. Prioritization of Solutions for the Implementation of e-HIE in Illinois

ILLINOIS FOUNDATION FOR QUALITY HEALTH CARE

Appendix 1 – HSC Charter

HISPC Steering Committee (HSC) Charter

Team Focus/Purpose

The HISPC Steering Committee (HSC) will provide oversight and direction for Illinois' HISPC project. The HSC will set direction, monitor progress, solicit work group members, provide updates to the Illinois EHR Taskforce, and approve deliverables to ensure success of the project.

RTI Contact	Phone/Email
Stephanie Rizk	(312) 456-5276 srizk@rti.org

Project Manager	Organization	Phone/Email
Shannon Smith-Ross	Illinois Foundation for Quality Health Care	(630) 928-5814 SSmithross@ilqio.sdps.org

Committee Members	Organization	Phone/Email
Jonathan Dopkeen, Ph.D.	Illinois Department of Public Health	312-814-5278 jonathan.dopkeen@illinois.gov
Maria I. Ferrera	CCA Strategies LLC	312-454-9326 maria.ferrera@ccastrategies.com
Laura K. Feste, RHIA	Illinois Health Information Management Association (formerly)	630-852-8370 lfeste@comcast.net
Steven Glass	Access Community Health Network	773-257-5099 glas@sinai.org
Beth Hackman	Illinois Foundation for Quality Health Care	630-928-5823 bhackman@ilqio.sdps.org
William Kempiners	Illinois Health Care Association	217-689-9615 bkempiners@ihca.com
Pat Merryweather	Illinois Hospital Association	630-276-5590 PMerryweather@ihastaff.org
Randy Mound	SUPERVALU	847-916-4237 randy.mound@albertsons.com
Kirk Riva	Life Services Network	217-789-1677 kriva@lsni.org
Nancy Semerdjian	Evanston Northwestern Healthcare	847-570-5236 nsemerdjian@enh.org

Key Stakeholders

- IFQHC
- IDPH

- EHR Taskforce

Goals of Committee

The HISPC Steering Committee (HSC) will strive to:

- Review, evaluate and analyze and approve contract deliverables produced by the working groups to ensure they are of the highest possible quality and truly reflects Illinois' current state and future needs relative to privacy and security of health information
- Provide organizational resources to help staff the working groups that will develop the contract deliverables
- Seek input and/or representation from as many stakeholder areas as possible in the creation and review of work resulting from HISPC's activities
- Communicate current HIPSC status to the Illinois EHR Taskforce
- Review progress and results of the project plan
- Identify opportunities for improvement
- Have members serve as a liaison between HSC and its organization/area of expertise, communicating HISPC activities to individual members constituencies and soliciting their feedback

Time Frames

The committee will continue its function until the completion of the HIPSC contract. It is anticipated that all activities will be completed by May 2007.

Ground Rules

The HSC will operate in the following manner:

- Every committee member will participate.
- Organizational representation is required. If a committee member cannot make a meeting, every effort will be made to find a replacement from your organization. The Project Manager must be notified if a replacement cannot be found.
- A three-fourths (3/4) quorum of the committee is required to have an official meeting.
- Consensus is the goal for approval of deliverables and committee recommendations.
- Each team member is expected to keep its constituent organization(s) updated on HISPC activities.
- Phones/Pagers should be put on vibrate
- If attending via conference call, the phones should be on mute unless the member is speaking.
- Only one committee member should be talking at a time (Don't talk over

each other).

- Committee members will respect each other's time.
- The agenda will be adhered to.
- A chairperson will be elected at the first meeting
- The facilitator/project manager will monitor time.
- Minute taking will taken by committee staff.
- Meetings will be held at a set time each month and more frequently when required. A standing meeting time will be determined at the first meeting.
- Any agenda items should be presented to the project manager no later than the two business days prior to the scheduled meeting date.
- Meeting times will be no longer than 2 hours unless special circumstances require extended time.
- Given the time commitment and cost of face-to-face meetings, conference calls will be offered for all meetings.

ILLINOIS FOUNDATION FOR QUALITY HEALTH CARE

Appendix 2 – VWG Charter

Business Practice Variations Working Group (VWG) Charter

Team Focus/Purpose

The Business Practice Variations Working Group (VWG) will develop a detailed report on the variation of privacy and security practices at the organizational level in Illinois for the HISPC project.

HSPC Steering Committee Chairperson	Phone/Email
Jonathan Dopkeen, Ph.D.	(312) 814-5278 jonathan.dopkeen@illinois.gov

RTI Contact	Phone/Email
Stephanie Rizk	(312) 456-5276 srizk@rti.org

Project Manager	Organization	Phone/Email
Shannon Smith-Ross	Illinois Foundation for Quality Health Care	(630) 928-5814 SSmithross@ilqio.sdps.org

Staff	Organization	Phone/Email
Virginia Headley, Ph.D.	Headley Associates	(217) 725-9687
Donna Travis	Illinois Foundation for Quality Health Care	(630) 928-5832 DTravis@ilqio.sdps.org

Committee Members	Organization	Phone/Email
Claire Dobbins	Kane County Health Dept.	(630) 208-3801 DobbinsClaire@co.kane.il.us
Carol Gibson Finley	IDPH	(217) 785-0121 Carol.Findley@illinois.gov
Valerie Holden	Cook County Bureau of Health Services	(312) 864-8166 mailto:VHolden@ccbhs.org
Bernie Ijimakin	Chicago Fire Dept.	(312) 746-4634 bijimakin@cityofchicago.org
Ron Isbell	Children's Memorial Hospital	(773) 880-4626
Paul Kuehnert	Kane County Health Dept.	(630) 208-3801 KuehnertPaul@co.kane.il.us
Pat Merryweather	Illinois Hospital Association	630-276-5590 PMerryweather@ihastaff.org
Debra McElroy, MPH., R.N.	Kane County Health Dept.	(630) 208-3801 McElroyDebra@co.kane.il.us

Committee Members	Organization	Phone/Email
Robert G Nadolski	The Alden Group	(773) 286-6622 rnadolski@aldengroup.org
Mary Ring	Illinois Hospital Association	630-276-5590 mailto:MRing@ihastaff.org
Pam Rudell	Humana	(502) 580-3850 PRudell@Humana.com
David Schanding, M.A., M.M.	Lake County Health Dept.	(847) 377-8297 dschanding@co.lake.il.us
Nadine Zabierek	Blue Cross Blue Shield	(312) 653-6305 zabierekn@bcbsil.com

Key Stakeholders

• CMS • AHRQ • RTI	• IDPH • EHR Taskforce • IFQHC	• Illinois businesses involved in health information exchange

Goals of Work Group

The Business Practice Variations Working Group (VWG) is responsible for developing a detailed report on the variation of privacy and security practices at the organization-level focusing at a minimum on the following key domain areas:

- User and entity authentication for accessing electronic personal health information
- Information authorization and access controls to allow access to only people or software programs that have been granted access rights to electronic personal health information
- Patient and provider identification matching across multiple information systems and organizations
- Information exchange protocols for information that is being exchanged over an electronic communication network
- Safeguards to ensure electronic personal health information cannot be improperly modified
- Information audits that record and monitor activity of health information systems
- Administrative or physical security safeguards required to implement a comprehensive security platform for health IT
- State law restrictions regarding information types and classes and the solutions by which electronic personal health information can be viewed and exchanged
- Information and disclosure policies that arise as health care entities share clinical health information electronically

Time Frames

The working group will remain intact until completion of the HISPC project in April 2007. However, this working group will serve as an advisory group after the submission of its assigned deliverable in October 2006.

Ground Rules

The VWG will operate in the following manner:

- Every working group member will participate.
- Organizational representation is required. If a working group member cannot make a meeting, every effort will be made to find a replacement from your organization. The Project Manager must be notified if a replacement cannot be found.
- A three-fourths (3/4) quorum of the working group is required to have an official meeting.
- Each group member is expected to keep its constituent organization(s) updated on HISPC activities.
- Phones/Pagers should be put on vibrate
- If attending via conference call, the phones should be on mute unless the member is speaking.
- Only one working group member should be talking at a time (Don't talk over each other).
- Working group members will respect each other's time.
- The agenda will be adhered to.
- The facilitator/project manager will monitor time.
- Working group staff will take minutes.
- Working group will be held at a set time each month and more frequently when required. A standing meeting time will be determined at the first meeting.
- Any agenda items should be presented to the project manager no later than the two business days prior to the scheduled meeting date.
- Meeting times will be no longer than 2 hours unless special circumstances require extended time.
- Given the interactive nature of the task, your onsite participation is highly encouraged. However, the ability to participate via conference calls will be offered for all meetings.

ILLINOIS FOUNDATION FOR QUALITY HEALTH CARE

Appendix 3 – LWG Charter

Legal Working Group (LWG) Charter

Team Focus/Purpose

The Legal Working Group (VWG) will develop a detailed report on the legal drivers for the variation of privacy and security practices at the organizational level in Illinois for the HISPC project.

HISPC Steering Committee Chairperson	Phone/Email
Jonathan Dopkeen, Ph.D.	(312) 814-5278 jonathan.dopkeen@illinois.gov

RTI Contact	Phone/Email
Stephanie Rizk	(312) 456-5276 srizk@rti.org

Project Manager	Organization	Phone/Email
Shannon Smith-Ross	Illinois Foundation for Quality Health Care	(630) 928-5814 SSmithross@ilqio.sdps.org

Staff	Organization	Phone/Email
Virginia Headley, Ph.D.	Headley Associates	(217)725 -9687 headleyassociates@gmail.com
Donna Travis	Illinois Foundation for Quality Health Care	(630) 928-5832 DTravis@ilqio.sdps.org

Committee Members	Organization	Phone/Email
Amy Shappert	Lanpher, Shappert & Associates	(815)398-1545 ashappert@lanphershappert.com
Judy Mondello	Mayer, Brown, Rowe and Maw	JAMondello@mayerbrownrowe.com
Leatrice Berman Sandler	McDermott Will & Emery	(312)984.7769 lbermansandler@mwe.com
Marilyn Thomas	IDPH	MARILYN.THOMAS@illinois.gov
Mark Novak	Methodist Medical Center of Illinois	(309)672-4865 mnovak@mmci.org
Rob Kane	Illinois State Medical Society	kane@ismie.com
Ted Nodzenski	Illinois Hospital Association	tnodzenski@ihastaff.org

Key Stakeholders

• CMS • AHRQ • RTI	• IDPH • EHR Taskforce • IFQHC	• Illinois businesses involved in health information exchange

Goals of Work Group

The Legal Working Group (LWG) is responsible for developing a detailed report on the legal drivers for variation of privacy and security practices at the organization-level focusing at a minimum on the following key domain areas:

- User and entity authentication for accessing electronic personal health information
- Information authorization and access controls to allow access to only people or software programs that have been granted access rights to electronic personal health information
- Patient and provider identification matching across multiple information systems and organizations
- Information exchange protocols for information that is being exchanged over an electronic communication network
- Safeguards to ensure electronic personal health information cannot be improperly modified
- Information audits that record and monitor activity of health information systems
- Administrative or physical security safeguards required to implement a comprehensive security platform for health IT
- State law restrictions regarding information types and classes and the solutions by which electronic personal health information can be viewed and exchanged
- Information and disclosure policies that arise as health care entities share clinical health information electronically

Time Frames

The working group will remain intact until completion of the HISPC project in April 2007. However, this working group will serve as an advisory group after the submission of its assigned deliverable in October 2006.

Ground Rules

The LWG will operate in the following manner:

- Every working group member will participate.
- Organizational representation is required. If a working group member cannot make a meeting, every effort will be made to find a replacement from your organization. The Project Manager must be notified if a replacement cannot be found.
- A three-fourths (3/4) quorum of the working group is required to have an official meeting.
- Each group member is expected to keep its constituent organization(s) updated on HISPC activities.
- Phones/Pagers should be put on vibrate
- If attending via conference call, the phones should be on mute unless the member is speaking.
- Only one working group member should be talking at a time (Don't talk over each other).
- Working group members will respect each other's time.
- The agenda will be adhered to.
- The facilitator/project manager will monitor time.
- Working group staff will take minutes.
- Working group will be held at a set time each month and more frequently when required. A standing meeting time will be determined at the first meeting.
- Any agenda items should be presented to the project manager no later than the two business days prior to the scheduled meeting date.
- Meeting times will be no longer than 2 hours unless special circumstances require extended time.
- Given the interactive nature of the task, your onsite participation is highly encouraged. However, the ability to participate via conference calls will be offered for all meetings.

ILLINOIS FOUNDATION FOR QUALITY HEALTH CARE

Appendix 4 – SWG and IWPG Charter

Solutions and Implementation Planning Working Group Charter

Team Focus/Purpose

As part of the Illinois HISPC project, the Solutions Working Group (SWG) and Implementation Planning (IWPG) will develop a detailed report outlining proposed solutions for the addressing privacy and security barriers to the electronic exchange of health information in Illinois as well as a high-level plan for implementing these solutions.

HSPC Steering Committee Chairperson	Phone/Email
Jonathan Dopkeen, Ph.D.	(312) 814-5278 jonathan.dopkeen@illinois.gov

RTI Contact	Phone/Email
Stephanie Rizk	(312) 456-5276 srizk@rti.org

Project Manager	Organization	Phone/Email
Shannon Smith-Ross	Illinois Foundation for Quality Health Care	(630) 928-5814 SSmithross@ilqio.sdps.org

Staff	Organization	Phone/Email
Virginia Headley, Ph.D.	Headley Associates	(217) 725-9687 headleyassociates@gmail.com
Donna Travis	Illinois Foundation for Quality Health Care	(630) 928-5832 DTravis@ilqio.sdps.org

Committee Members	Organization	Phone/Email
Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS	Margret\A Consulting, LLC	(847) 895-3386 MargretCPR@aol.com
Maria I. Ferrera	CCA Strategies LLC	(312) 454-9326 maria.ferrera@ccastrategies.com
Steven Glass	Access Community Health Network	(773) 257-5099 glas@sinai.org
Joe Granneman	Rockford Memorial Hospital	(815) /971-5250 JGranneman@rhsnet.org
Merida Johns, PhD, RHIA.	Bundling Board	(815) 338.7054 innkeeper@bundlingboard.com
Gary Nalley	University of Illinois Medical Center at Chicago	(312) 996-4675 gnalley@uic.edu

Committee Members	Organization	Phone/Email
Maria Pekar	Loyola University Health System	(708) 216-8686 mpekar@lumc.edu
Lou Ann Schraffenberger,MBA, RHIA, CCS, CCS-P	Advocate Health Care	(630) 990-5659 Louann.Schraffenberger@advocatehealth.com
Donna Schnepp, MHA, RHIA	Moraine Valley College	(708) 974.5315 Schnepp@morainevalley.edu
Geraldine Smothers, MPA, RHIA, CSL, CPHQ	Professional Dynamic Network	(708) 747-4361 info@pdnseek.com
Rachelle Steward, DrPH, RHIA	University of Illinois at Chicago	(312) 996-9177 stewartr@uic.edu

Key Stakeholders

• CMS • AHRQ • RTI • IHIMA	• IDPH • EHR Taskforce • IFQHC	• Illinois businesses involved in health information exchange

Goals of Work Group

The Solutions Working Group (SWG) and Implementation Planning Working Group (IPWG) are responsible for developing a detailed report outlining proposed solutions and a plan of action 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 following key domain areas:

- User and entity authentication for accessing electronic personal health information
- Information authorization and access controls to allow access to only people or software programs that have been granted access rights to electronic personal health information
- Patient and provider identification matching across multiple information systems and organizations
- Information exchange protocols for information that is being exchanged over an electronic communication network
- Safeguards to ensure electronic personal health information cannot be improperly modified
- Information audits that record and monitor activity of health information systems
- Administrative or physical security safeguards required to implement a comprehensive security platform for health IT
- State law restrictions regarding information types and classes and the solutions by which electronic personal health information can be viewed and

exchanged
- Information and disclosure policies that arise as health care entities share clinical health information electronically

Time Frames

The working group will remain intact until completion of the HISPC project in April 2007.

Ground Rules

The SWG will operate in the following manner:

- Every working group member will participate.
- Organizational representation is required. If a working group member cannot make a meeting, every effort will be made to find a replacement from your organization. The Project Manager must be notified if a replacement cannot be found.
- A three-fourths (3/4) quorum of the working group is required to have an official meeting.
- Each group member is expected to keep its constituent organization(s) updated on HISPC activities.
- Phones/Pagers should be put on vibrate
- If attending via conference call, the phones should be on mute unless the member is speaking.
- Only one working group member should be talking at a time (Don't talk over each other).
- Working group members will respect each other's time.
- The agenda will be adhered to.
- The facilitator/project manager will monitor time.
- Working group staff will take minutes.
- Working group will be held at a set time each month and more frequently when required. A standing meeting time will be determined at the first meeting.
- Any agenda items should be presented to the project manager no later than the two business days prior to the scheduled meeting date.
- Meeting times will be no longer than 2 hours unless special circumstances require extended time.
- Given the interactive nature of the task, your onsite participation is highly encouraged. However, the ability to participate via conference calls will be offered for all meetings.

Appendix 5 – HIE Exchange Scenarios Guide

Privacy and Security
Health Information Exchange Scenarios Guide

The following 18 scenarios were developed specifically for the privacy and security project to provide a standardized context for discussing organization-level business practices across all states and territories. The scenarios represent a wide range of purposes for the exchange of health information (e.g., treatment, public health, biosurveillance, payment, research, marketing, etc) across a broad array of organizations involved in health information exchange and actors within those organizations. The product of the "guided or focused" discussions will be a database of organization-level business practices that will form the basis for the assessment of variation upon which all other work will be based.

Each scenario describes a health information exchange within a given context to ensure that we cover a most of the areas we expect to find barriers. Clearly, we have not covered the universe of exchanges—which would be impossible given the timeframe for the project. However, the purposes and conditions represented should be more than adequate to get the discussions of privacy and security policy moving forward.

Exhibit 1 below shows a mapping of stakeholder organizations identified in the HIE scenarios. A shaded box containing an "X" with some additional text indicates stakeholders that are explicitly identified in the scenario. A lightly shaded box with no text indicates a stakeholder group that could conceivably weigh in on a scenario. For example, Scenario 1—Patient Care Scenario A, involves an exchange between the ER in Hospital A and the out-of-state Hospital B. Both the requesting and releasing organizations are hospitals, regardless of the actors that may be representing those organizations in the work group meetings which may include physicians, nurses, HIM professionals, etc. We have also identified the relevant organizations and exchanges at the beginning of each scenario. This should help to guide decisions about creating the right mix of stakeholders for each work group based on the selected scenarios.

ILLINOIS FOUNDATION FOR QUALITY HEALTH CARE

Exhibit 1. Scenario by Stakeholder Map

Scenarios	1. Clinicians	2. Physician groups	3. Federal health facilities	4. Hospitals	5. Payers	6. Public Health agencies	7. Community clinics and health centers	8. Laboratories	9. Pharmacies	10. Long term care facilities and nursing homes	11. Homecare and Hospice	12. Law Enforcement/ Correctional facilities	13. Professional associations and socieities	14. Medical and Public health schools that undertake research	15. Quality improvement organizations	16. Consumers or consumer organizations	17. State government (Medicaid, public health departments)	18. Other, specify
1. Patient Care - Scenario A (Emergent Transfer)				X ER Staff (sending and receiving)														
2. Patient Care - Scenario B (Sub Abuse)	X Provider	X Primary Care Physician					X Substance Abuse Treatment									X Client/Patient		
3. Patient Care - Scenario C (Access Security)	X Provider	X Psychiatrist		X Hospital Psych Unit						X Nursing Facility								X Transcription Service
4. Patient Care - Scenario D (HIV and Genetic)				X Mamography Dept.			X Outpatient Clinic											
5. Payment Scenario	X Provider	X Provider	X Provider	X Provider	X Health Plan		X Provider			X Provider	X Provider					X Patient		
6. RHIO Scenario	X Provider	X Provider	X Provider	X Provider			X Provider	X Provider	X Provider	X Provider	X Provider							
7. Research Final Scenario	X Provider	X Provider												X IRB, Research Investigator		X Study Member		
8. Law Enforcement Final Scenario				X Provider								X Law Enforcement				X Patient Patient's family		
9. Pharmacy Benefit Final Scenario A							X Outpatient Clinic		X Pharmacy Benefit Manager							X Patient		
10. Pharmacy Benefit Final Scenario B									X Pharmacy Benefit Manager							X Employees		X Company
11. Operations and Marketing Final Scenario A				X Tertiary Hospital Marketing Dept			X Critical access clinics (sending)											
12. Operations and Marketing Final Scenario B				X Obstetrics department Marketing												X Patient		X Company
13. Bioterrorism Event Final Scenario	X Provider	X Provider		X Provider		X Public Health Staff						X Law Enforcement					X Emergency Govt agencies	
14. Employment Information Final Scenario				X ER Staff												X Employees		X Company HR Dept
15. Public Health Final Scenario A	X Provider	X PCP				X Public Health Staff						X Law Enforcement				X Patient		
16. Public Health Final Scenario B	X Provider	X Physician				X Public Health Staff	X Specialty Care Center	X Lab Staff									X Public Health	
17. Public Health Final Scenario C	X Provider	X PCP		X Drug Treatment Center			X Homeless shelter Community									X Patient Patient's family	X County Program	
18. Health Oversight Final Scenario						X Public Health Staff								X Faculty				
18. Health Oversight Final Scenario						X								X Faculty				

ILLINOIS FOUNDATION FOR QUALITY HEALTH CARE

Health Information Exchange Scenarios

1. Patient Care Scenario A

The emergent transfer of health information between two hospitals that represent the 2 stakeholder organizations (i.e., Hospital A and Hospital B) when the status of the patient is unsure. The actors are the staff involved in carrying out the request. The ER physician is requesting the information on behalf of the Hospital A.

Stakeholder organizations and exchanges:

- Hospital emergency room in Hospital A is the organization requesting information
- Hospital B is the organization releasing the information.

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89 year old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

Potential areas for discussion of BUSINESS PRACTICES based on this scenario:

1. Determining status of the patient and chain of responsibility
2. Practice and policy for obtaining information sufficient for treatment.
3. Practice and policy for handling mental health information.
4. Practice and Policy for securing the data exchange mechanism.
5. Practice and policy related to authentication of requesting facility by the releasing facility.
6. Practice and policy related to patient authorization for the release of information.

2. Patient Care Scenario B

The scenario involves the non-emergent transfer of records from a specialty substance treatment provider to a primary care facility for a referral to a specialist.

Stakeholder organizations and exchanges:

- Specialty substance abuse treatment facility (releasing sensitive clinical records)
- Primary care provider's organization (e.g., doctor's office, community health center, public health agency, etc) (requesting clinical records from the substance abuse facility; releasing information to specialist)

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The two organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol that is relevant for medical diagnosis. The primary care provider has requested that the substance abuse information be sent by the treatment facility. The primary care provider intends to refer the patient to a specialist and plans to send all of the patient's medical information, including the substance abuse information that was received from the substance abuse treatment facility, to the specialist.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. How does the releasing organization obtain authorization from the patient to allow release of medical records?
2. What is the process for handling substance abuse medical record data?
3. How does the releasing organization authenticate the healthcare provider requesting the information?
4. How is the data exchange secured?

3. Patient Care - Scenario C

Stakeholder organizations and exchanges:

- the hospital psychiatric unit (sending) and the skilled nursing facility (receiving)
- the physician (sending) and the transcription service (receiving)
- the transcription service (sending) and the physician (receiving)
- the physician (sending) and the skilled nursing facility (receiving)

:

At 5:30pm Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psychiatric unit to the skilled nursing facility. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

When Dr. X enters the facility, he seeks assistance locating his patient, gaining entrance to the locked psychiatric unit, and accessing the patient's electronic health record to review the discharge summary, I&O, MAR and progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the EHR. As it is Dr. X's first visit, he has no login or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure web portal.

The next morning, from his home computer, Dr. X checks his e-mail and receives notification that the assessment is available. Dr. X logs into his office web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr X's Office Manager downloads this assessment from the web portal, saves the document in the patient's record in his office and forwards the now encrypted document to the long-term care facility via e-mail.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Agreements for data sharing - business associate agreements.
2. Setting out access and role management policies and practices for temporary or new access
3. Determining appropriate access to mental health records.

4. Securing unstructured, possibly non-electronic patient data.
5. Reliability of other entity security and privacy infrastructure

4. Patient Care - Scenario D

The non-emergent transfer of health information

Stakeholder organizations and exchanges:

- Hospital mammography department (requesting health information)
- Outpatient Clinic (receiving request)

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the BrCa gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Authenticating entities and individuals.
2. Determining processes and laws for release of genetic and HIV information.

5. Payment Scenario

Stakeholder Organizations and Exchanges:

- Healthcare Provider (Hospital or Clinic)
- Health Plan (Payer)
- Patients

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the healthcare provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (e.g., emergency department records, clinic notes, etc.).

The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the healthcare provider's workforce members and medical staff members and their office staff.

X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Get patient authorization to allow payer access.
2. Facility needs to determine the minimum necessary and limit to pertinent timeframe.
3. If allowed, access and role management are issues.
4. Determine method for enabling secure remote access if allowed.

6. RHIO Scenario

Note: Each stakeholder should participate in this scenario keeping in mind the type of data their organization anticipates exchanging with a RHIO.

Stakeholder organizations and exchanges:

- Multiple provider organizations (providing data)
- Multiple RHIO's (receiving data)

The RHIO in your region wants to access patient identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to utilize medical record data to monitor disease management.
2. Authorization from patients to allow RHIO to monitor their PHI for disease management.
3. Determine mode of transferring information and type of information i.e. identifiable or de-identified information to the RHIO

7. Research Data Use Scenario

Stakeholder organizations and exchanges:

- Health care consumer (taking part in the study)
- Health care provider (distributing meds and collecting clinical data)
- Research investigator (receiving and analyzing clinical data)
- Institutional Review Board (IRB) (receiving reports on data collection)

A research project on children younger than age 13 is being conducted in a double blind study for a new drug for ADD/ADHD. The research is being sponsored by a major drug manufacturer conducting a double blind study approved by the medical center's IRB where the research investigators are located. The data being collected is all electronic and all responses from the subjects are completed electronically on the same centralized and shared data base file.

The principle investigator was asked by one of the investigators if they could use the raw data to extend the tracking of the patients over an additional six months and/or use the raw data collected for a white paper that is not part of the research protocols final document for his post doctoral fellow program.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. IRB approval of any significant changes to the research protocol
2. Research subjects have signed consents and authorization to participate in the research effort.

8. Scenario for access by law enforcement

Stakeholder organizations and exchanges:

- Healthcare provider (providing health information)
- Law enforcement
- Patient
- Patient's family

An injured nineteen (19) year old college student is brought to the ER following an automobile accident. It is standard to run blood alcohol and drug screens. The police officer investigating the accident arrives in the ER claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood alcohol test results and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

The patient is covered under their parent's health and auto insurance policy.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. County contracts with emergency department to perform Blood Alcohol test draws.
2. Printing of additional copies of medical record reports for parents, insurance companies, and police.
3. Asking patient if it's OK to talk to parents or give information to parents about their condition
4. Communication with primary care provider.

9. Pharmacy Benefit Scenario A

Stakeholder organizations and exchanges: :

- Pharmacy Benefit Manager (requesting information)
- Outpatient Clinic (receiving request)
- Patient X

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital which is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's Outpatient Clinic.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Patient authorization to share information with the pharmacy benefit manager.
2. Agreements for data sharing – business associate agreements.
3. Healthcare provider must determine minimum necessary access to PHI.
4. If allowed role and access management are issues.
5. Determine method for enabling secure remote access if allowed.

10. Pharmacy Benefit Scenario B

Stakeholder organizations and exchanges:

- Pharmacy Benefit Manager (requesting information)
- Company A (providing claims information)
- Employees

A Pharmacy Benefit Manager 1 (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if the PBM1 could save the company money on their prescription drug benefit. Company A is self insured and as part of their current benefits package, they have the prescription drug claims submitted through their current PBM (PBM2). PBM1 has requested that Company A send their electronic claims to them to complete the review.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Business associate agreements and formal contracts exist between Company A and the Pharmacy Benefit Managers.
2. The extent and amount of information shared between the various parties would be limited by the minimum necessary guidelines.

11. Healthcare Operations and Marketing - Scenario A

Note: This scenario could be modified to apply to any healthcare provider (physician group, home health care agency, etc.) wishing to market services to a targeted subset of patients.

Stakeholder organizations and exchanges:

- Tertiary hospital (requesting study data)
- Critical access hospital (being asked to provide health information)

ABC Health Care is an integrated health delivery system comprised of ten critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient identifiable data to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/ procedures:

- Cerebrovascular Accident (CVA)
- Hip Fracture
- Total Joint Replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to conduct marketing using PHI with their consumers.
2. Authorization from consumer to allow IHDS to market to themselves.
3. Determine mode of transferring information and type of information, i.e., identifiable or de-identified information to the marketing department

12. Healthcare Operations and Marketing - Scenario B

Stakeholder organizations and exchanges:

- Healthcare provider (Hospital obstetrics department sending data)
- Hospital marketing department (receiving data)
- Local company (purchasing data from marketing department)
- Patients/Consumers

ABC hospital has approximately 3,600 births/year. The hospital Marketing Department is requesting identifiable data on all deliveries including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries resulting in healthy live births).

The Marketing Department has explained that they will use the patient information for the following purposes:

1. To provide information on the hospital's new pediatric wing/services.
2. To solicit registration for the hospital's parenting classes.
3. To request donations for construction of the proposed neonatal intensive care unit
4. They will sell the data to a local diaper company to use in marketing diaper services directly to parents.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Requesting patient consent or permission to use and sell identifiable data for marketing purposes.
2. Decisions to conduct marketing using patient data.
3. Determining mode of transferring information and type of information, i.e., identifiable or de-identified information to the marketing department

13. Bioterrorism event

Stakeholder organizations and exchanges:

- Laboratory (collecting data)
- Healthcare provider (transmitting data to public health)
- Public health department (receiving data from provider, providing data to gov't agencies)
- Law enforcement (receiving data)
- Government agencies (receiving data)
- Patients

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the State declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well informing the regional media to alert the public to symptoms and seek treatment if feel affected. The State also notifies the Federal Government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as they arise to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient specific information related to specific symptoms to law enforcement, CDC, Homeland Security, and health department in a situation where a threat is being investigated.

14. Employee Health Information Scenario

Stakeholder organizations and exchanges:

- Hospital emergency room (releasing health information)
- Employer human resources department (requesting health information)
- Employee

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated which is not work-related. The employee's condition necessitates a four-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days leave. The hospital Emergency Department has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information via email to the Human Resources department of the patient's employer.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Determining employee agreement to release information.
2. Determining what are the minimum necessary elements which can be legally transmitted.
3. Ensuring the data is secured as it is transmitted.

15. Public Health - Scenario A - Active carrier, communicable disease notification

Stakeholder organizations and exchanges:

- Healthcare provider (primary care physician)
- Public health department
- Law enforcement
- Patient

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multi-drug resistant). The patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops across several states. State A is made aware of the patient's intent two hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient specific information related to a specific communicable disease to law enforcement, non-healthcare entities, and health department in a situation where a threat is being responded to.
2. Ensuring the data is secured as it is transmitted.

16. Public Health - Scenario B -Newborn screening

Stakeholder organizations and exchanges:

- Healthcare provider (sending initial data to public heath and lab, receiving data on follow up/eligibility)
- State laboratory (receiving data)
- State public health department (receiving data, sending data for program eligibility)

A newborn's screening test comes up positive for a state-mandated screening test and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response (IVR) system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient specific information related to specific symptoms of a disease to a health department in a situation where a targeted disease is being investigated.

17. Public Health Scenario C- Homeless shelters

Stakeholder organizations and exchanges:

- Primary care provider (sending) and hospital-affiliated drug treatment center (receiving)
- the hospital-affiliated drug treatment clinic (releasing) and the county program (requesting for purposes of reimbursement)
- the hospital-affiliated drug treatment clinic (releasing) and the shelter (requesting to verify the treatment)
- the family member (requesting) and the shelter

Stakeholder entities:

- Health care consumer/patient
- Primary care provider
- Hospital-affiliated drug treatment center
- Homeless shelter
- Patient relative/family member

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. The person does have a primary care provider, and he is sent there for medical care. Primary care provider refers patient to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement, and back to the shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter is working to connect the homeless man with his relative.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. The extent and amount of information shared between the various facilities would be limited by the minimum necessary guidelines.

18. Health Oversight: Legal compliance/government accountability

Stakeholder organizations and exchanges:

- State university faculty (requesting health information)
- State public health agencies (asked to provide health information)

The Governor's office has expressed concern about compliance with immunization and lead screening requirements among low income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient level health care data on an ongoing basis to determine if the children are getting the healthcare they need. This is not part of a legislative mandate. The Governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the Governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is not existing contract with the state university for services of this nature.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

What is the practice of the organization to provide appropriate information for healthcare oversight activities? These may include:

- determining minimum amount necessary
- how to release (electronically or paper - with existing claims data)

Appendix 6 - Confidentiality Protections in Illinois

There are extensive laws that apply to Illinois providers, payors, and others, establishing rights and obligations with respect to maintaining patient privacy, and confidentiality and security of patient health information. These laws drive health information exchange practices in Illinois and should be taken into account in discussing necessary information technology parameters and requirements for national electronic health information exchange.

The State of Illinois has obtained a thorough review and analysis of Illinois laws related to the use and disclosure of health information. This document, titled the State of Illinois Draft Preemption Analysis, was compiled in 2003 and contains an exhaustive list of state laws, some of which impact upon the analysis of the scenarios contained in the Illinois Interim Assessment of Variations Report. The document may be accessed on the State of Illinois Website at http://www.illinois.gov/hipaa/ .

The Legal Working Group compiled the following partial list of the state and federal laws addressing confidentiality, privacy, and security of health information that most impact stakeholders in Illinois.

(Confidentiality Laws)

AIDS Confidentiality Act, 410 ILCS 305/1 *et seq.*

Alcoholism and other Drug Abuse and Dependency Act, 20 ILCS 301/1 *et seq.*

Child Care Act of 1969, 225 ILCS 10/1 *et seq.* (applicable to childcare facilities).

Community Living Facilities Code, 77 Ill. Adm. Code 370.1230 (Confidentiality - adopting the Mental Health and Developmental Disabilities Confidentiality Act confidentiality provisions).

Confidentiality of Alcohol and Drug Abuse Records, 42 CFR Part 2.

Genetic Information Privacy Act, 410 ILCS 513/1 *et seq.*

Dental Care Patient Protection Act, 215 ILCS 109/1 *et seq.* (a patient has the right to privacy and confidentiality).

Early Intervention Services System Act, 325 ILCS 20/1 *et seq.*

Early Intervention Services System Act Regulations:

Rules Implementing the Early Intervention Services System Act, 89 Ill. Adm. Code 500.155 (written consent regarding use and exchange of information).

HIPAA Administrative Simplification Regulations, 45 CFR Parts 160, 162), and 164.

Hospital Licensing Act, 210 ILCS 85/6.17 (protection of and confidential access to medical records and information).

Hospital Licensing Regulations, , 77 Ill. Adm. Code 250.1510 (provisions for maintenance, storage, responsibility, content, authentication, verification, confidentiality and security safeguards, indexing and preservation of medical records, and special record requirements for psychiatric service). Note that this law recommends that the unique confidentiality requirements of a psychiatric record, and requires that the unique confidentiality requirements of the alcoholism patient's records, be recognized and safeguarded in any unitized system.

Illinois Constitution, Article I, Section 6 (right to privacy)

Illinois Public Aid Code, 305 ILCS 5/1-1 *et seq.* (confidentiality and protection of records)

Insurance Code, Article XL, Insurance Information and Privacy Protection, 215 ILCS 5/1001 *et seq.* (standards for collection, use and disclosure of information gathered by insurers in connection with life, health, disability, property and casualty insurance transactions), including Article XL (Insurance Information and Privacy Protection), 215 ILCS 5/1001 *et seq.* (standards for the collection, use and disclosure of information gathered in connection with insurance transactions, including medical record information, and restrictions on disclosures without patient authorization and required form of authorization).

Managed Care Reform and Illinois Patient's Rights Act, 215 ILCS 134/1 *et seq*. (Right to privacy and confidentiality in health care.)

Medical Patient Rights Act, 410 ILCS 50/0.01 *et seq.* (Patient's right to privacy and confidentiality of records, including restrictions on disclosures by physicians, health care providers, health services corporations and insurance companies.)

Medicare Conditions of Participation for Hospitals, 42 CFR 482.13 (Patient's right to personal privacy and confidentiality of clinical records).

Nursing Home Care Act, 210 ILCS 45/1-1-1 *et seq.* (privacy and confidentiality of records)

Nursing Home/Long Term Care Regulations:

Skilled Nursing and Intermediate Care Facilities Code, 77 Ill. Adm. Code 300.1810 (Resident Record Requirements), 300.1820 (Content of Medical Records), 300.1840, 300.3320 (Confidentiality).

Sheltered Care Facilities Code, 77 Ill. Adm. Code 330.1710 (Resident Record Requirements), 330.4320 (Confidentiality).

Illinois Veterans' Homes Code, 77 Ill. Adm. Code 340.1800 (Resident Record Requirements), 340.1840 (Confidentiality of Resident's Records).

Intermediate Care for the Developmentally Disabled Facilities Code, 77 Ill. Adm. Code 350.1610 (Resident Record Requirements), 350.1630 (Confidentiality of Resident's Records).

Long Term Care for Under Age 22 Facilities Code, 77 Ill. Adm. Code 390.1610 (Resident Record Requirements), 390.1630 (Confidentiality of Resident's Records), 390.3320 (Confidentiality).

Managed Care Reform and Patient Rights Act, 215 ILCS 134/1 *et seq.* (right to privacy and confidentiality of records).

Medical Patients Rights Act, 410 ILCS 50/.01 *et seq.* (right to privacy and confidentiality of records).

Medicare Conditions of Participation for Hospitals, 42 CFR 482.13 (Patients' Rights).

Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/1 et seq.

Physician and Patient Privilege, 735 ILCS 5/8-101. (We note that the courts have recently recognized the strong medical privacy law protections of this state law privilege. See, for example, the recent district and appellate decisions quashing an otherwise valid subpoena for sensitive non-party medical records in *Nat'l Abortion Fed'n v. Ashcroft*, 2004 U.S. Dist. LEXIS 1701 (N.D. Ill. Feb. 5, 2004) *aff'd Northwestern Memorial Hospital v. Ashcroft*, 362 F.2d 923 (7th Cir. 2004).

Rules Implementing the Community Services Act, 59 Ill. Adm. Code 132.20 (adopting Mental Health and Developmental Disabilities Confidentiality Act confidentiality provisions).

Rules Implementing the Respite Program Act, 89 Ill. Adm. Code 220.100

Standards and Licensure Requirements for Community Integrated Living Arrangements, 59 Ill. Adm. Code 115.250 (Individual rights and confidentiality - adopting Mental Health and Developmental Disabilities Confidentiality Act confidentiality provisions).

Workers' Compensation Act, 820 ILCS 305/1 *et seq.*

(State Licensure Laws)

In addition to the above laws, the State's licensure laws that govern the various categories of health care providers in Illinois generally provide that unprofessional or unethical conduct (such as breaching patient privacy or confidentiality) may be grounds for disciplinary action, and the following specifically reference the provider's duty to maintain the confidentiality of patient information:

Clinical Psychologist Licensing Act, 225 ILCS 15/1 *et seq.*

Clinical Social Work and Social Work Practice Act, 225 ILCS 20/1 *et seq.*

Illinois Physical Therapy Act, 225 ILCS 90/1 *et seq.*

Marriage and Family Therapy Licensing Act, 225 ILCS 55/1 *et seq.*

Professional Counselor and Clinical Professional Counselor Licensing Act, 225 ILCS 107/1 *et seq.*

Rules Implementing the Illinois Occupational Therapy Practice Act, 68 Ill. Adm. Code 1315.165.

Rules Implementing the Illinois Speech-Language, Pathology and Audiology Practice Act, 68 Ill. Adm. Code 1465.95.

Rules Implementing the Orthotics, Prosthetics and Pedorthis Practice Act, 68 Ill. Adm. Code 1325.65(a)(3).

Rules Implementing the Pharmacy Practice Act of 1987, 68 Ill. Adm. Code 1330.65.

(Reporting Obligations and Confidentiality of Reports and Information)

The laws addressing the mandatory and permissive reporting obligations of health care providers and others in Illinois contain confidentiality protections and limitations on the release of patient information, such as is provided in the following:

Abused and Neglected Child Reporting Act, 325 ILCS 5 *et seq.*

Child Sexual Abuse Prevention Act, 325 ILCS 15 *et seq.*

Communicable Disease Report Act, 745 ILCS 45/0.01 *et seq.*

Control of Sexually Transmissible Diseases Code, 77 Ill. Adm. Code 693.100.

Domestic Abuse of Disabled Adults Intervention Act, 20 ILCS 2435 *et seq.*

Elder Abuse and Neglect Act, 320 ILCS 20/1 *et seq.*

High Blood Pressure Control Act, 410 ILCS 425/1 *et seq.*

HIV/AIDS Confidentiality and Testing Code, 77 Ill. Adm. Code 684.220.

HIV/AIDS Registry Act, 410 ILCS 310/1 *et seq.*

Illinois Adverse Health Care Events Reporting Law of 2005, 410 ILCS 522/10-1 *et seq.*

Illinois Sexually Transmissible Disease Control Act, 410 ILCS 325/1 *et seq.*

Lead Poisoning Prevention Code, 77 Ill. Adm. Code 845.20.

Reye's Syndrome Reporting Act, 410 ILCS 245/1 *et seq.*

(Special Protections for Research Uses and Disclosures)

Department of Health and Human Services, Public Welfare, "Common Rule" Regulations, 45 CFR Part 46 (regulations for research involving human subjects conducted, supported or otherwise subject to regulation by federal agencies).

Food and Drug Administration, Department of Health and Human Services "Protection of Human Subjects" Regulations, 21 CFR Part 50 (regulations applicable to all clinical investigations regulated by the FDA and clinical investigations supporting applications for research or marketing permits for products regulated by the FDA).

Food and Drug Administration, Department of Health and Human Services "Institutional Review Boards" Regulations, 21 CFR Part 56 (IRB standards for review of clinical investigations subject to FDA jurisdiction).

HIPAA Privacy Rule, 45 CFR 164.512(i) (Standard: Uses and disclosures for research purposes, establishing conditions for permitted uses and disclosures per IRB/Privacy Board waiver of authorization (including waiver criteria and Common Rule IRB review procedures) and for preparatory reviews and on decedent's information).

HIPAA Privacy Rule, 45 CFR 164.508 (Uses and disclosures for which an authorization is required).

HIPAA Privacy Rule, 45 CFR 164.502(d) (Standard: Uses and disclosures of de-identified protected health information).

HIPAA Privacy Rule, 45 CFR 164.514(e)(1) (Standard: Limited data set).

Appendix 7 - Illinois Special Record Protections

The following is a summary of the provisions of Illinois laws that provide extraordinary protections for certain categories of information considered in the Final Assessment of Variation and Analysis of Solutions Report.

Mental Health Information

Illinois law provides strict protections to mental health and developmental disabilities information. *Mental Health and Developmental Disabilities Confidentiality Act*, 740 ILCS 110/1 *et seq*. Under this law, and with limited exceptions, information relating to "mental health or developmental disabilities services" may not be released without the patient's specific written "consent." The definition of what constitutes "mental health services" includes examination, diagnosis, evaluation, treatment, and pharmaceuticals.

There are two exceptions that may be applied to the given scenarios. First, there is an "emergency exception" that permits disclosures "to the extent disclosure is, in the sole discretion o the therapist, necessary to the provision of emergency medical care to a recipient who is unable to assert or waive his or her rights hereunder." Thus, if the patient is unable to sign a consent at the time (and has not signed an advance consent), relevant information may be released without consent.

Second, there is a "therapist" exception that permits a health care provider providing "mental health services" to disclose information without consent to certain persons involved in the care, including a "consulting therapist." Thus information may be shared without consent if the health care provider receiving the information is a "consulting therapist."

The law has specific requirements as to what constitutes a valid "consent," which are similar to HIPAA's Authorization requirements but require some additional provisions (such as a witness signature). Also, the consent must contain an express calendar expiration date or the requested information may only be released on the day the consent is received. To be valid, the consent must specify "the person or agency" to which disclosure will be made, and "advance consent" is valid only if the information to be released is specified in detail and the duration of the consent is indicated.

Illinois law specifically prohibits redisclosures of released information unless the patient has consented to subsequent disclosures.

The Illinois law permits persons aggrieved by violation of the law to sue for damages and attorneys' fees, and provides that violation of the law constitutes a criminal misdemeanor.

Substance Abuse Information

Illinois has adopted the federal substance abuse regulations governing federally assisted treatment programs (42 CFR Part 2) as the standards that apply to state assisted treatment programs. *Alcoholism and Other Drug Abuse and Dependency Act*, 20 ILCS 301/1-1 *et seq*. The Illinois law protects: "Records of the identity, diagnosis, prognosis or treatment of any patient maintained in connection with the performance of any program or activity relating to alcohol or other drug abuse or dependency education, early intervention, intervention, training, treatment or rehabilitation which is regulated, authorized, or directly or indirectly assisted by any Department or agency of this State or under any provision of [the Illinois] Act"

Under the state law and the federal regulations, information may be disclosed only under certain circumstances, including "with patient consent" or for "medical emergencies."

These laws also specify the required form of a valid "consent", including the specific name or title of the individual or the name of the organization to which disclosure is to be made and a specific expiration date, event, or condition – which must insure the consent lasts no longer than reasonably necessary to serve its purpose.

There is also a specific prohibition against redisclosure (further disclosure is prohibited unless the written consent permits it), and a written statement describing the prohibition must be included with any disclosures made with the patient's consent.

The Illinois law provides that violation of the law constitutes a criminal misdemeanor.

HIV/AIDS Information

The Illinois AIDS Confidentiality Act, 410 ILCS 305/1 et seq., contains a general prohibition against disclosures of the identity of persons tested and against disclosures of test results in a manner that permits identification of the individual, which limited exceptions, such as to the individual or to persons designated in a "legally effective release," and other exceptions that do not apply to these scenarios.

The law also contains a prohibition against redisclosure.

The Illinois law permits persons aggrieved by violation of the law to sue for damages and attorneys' fees, and provides that violation of the law constitutes a criminal misdemeanor.

Genetic Testing Information

The Illinois law provides extraordinary protections to genetic testing information. *Genetic Information Privacy Act*, 410 ILCS 513/1 *et seq.* Under this law, genetic testing and information derived from such testing may only be released to the individual tested, to persons "specifically authorized" in a "specific written legally effective release" by the subject of the test or the subject's legally authorized representative, and other limited exceptions that are not relevant to the scenarios presented in this analysis.

This law also contains a specific prohibition against redisclosure, and recipients of genetic test information without the patient's signed release.

The Illinois law permits persons aggrieved by violation of the law to sue for damages and attorneys' fees, and provides that violation of the law constitutes a criminal misdemeanor.

Rights of Parents and Minors to Access and Control Release of the Minor's Health Information

(Treatment Under HIPAA)

The HIPAA Privacy Rule (45 CFR 164.502(g) requires covered entities to treat persons considered to be the patient's "personal representative" as the individual with respect to the individual's HIPAA privacy rights, including the rights to access and authorize release of information. Under HIPAA, a personal representative is a person legally authorized to make health care decisions on the individual's behalf. In the case of minors, parents are generally considered to be the personal representatives for their minor children, and thus are generally entitled to access and authorize release of the child's health information. However, in certain situations, the parent may not be considered the personal representative of the minor child (for example, if state law permits the minor to consent to a certain type of health care service without the parent's consent). In such cases, the Privacy Rule generally defers to State or other law that either permits, requires or prohibits providing parental access. If the underlying state law does not contain a specific provision addressing parental access, the Privacy Rule permits the health care professional to look to other law for guidance and exercise judgment as to what is in the minor's best interest in permitting or denying parental access to information.

In other words, state law will govern the rights of parents and minors when such law requires, permits, or prohibits disclosure or access to a parent of a minor child's health information, but the health care provider may exercise judgment if the underlying law is silent on the issue of parental access to the minor's health care information. *See* DHHS Summary of the HIPAA Privacy Rule at http://www.hhs.gov/ocr/privacysummary.rtf . *See also* American Medical Association Code of Ethics, E-5.055 (Confidential Care for Minors).

(Treatment Under Illinois Law)

Medical and Surgical Procedures - Consent

Illinois law permits certain minors to consent to the performance of medical or surgical procedures if the minor is:

- Married;
- A parent; or
- Pregnant.

Under this law, such minors and any person who is 18 years or older is deemed to have the same legal capacity to act as a person of legal age. Further, minor parents have legal capacity to consent to procedures performed on his or her child and parental consent is not required for emergency treatment or first aid given to a minor when obtaining such consent is not feasible. *Consent by Minors to Medical Procedures Act,* 410 ILCS 210/0.01 *et seq.*

Sexual Assault/Abuse - Consent

Illinois law also contains special consent provisions allowing for minor consent (without the need for parental consent) for certain types of health care services, namely:

- Medical care and counseling related to the diagnosis or treatment of any disease or injury arising from sexual assault or abuse of a minor victim.

STD and Alcohol/ Drug Abuse - Consent

In addition, there are specific provisions permitting minors age 12 and older may consent (and parental consent is not required) to medical care and counseling related to diagnosis or treatment relating to certain diseases, namely:

- Minors who may have come into contact with a sexually transmitted disease
- Minors who may be determined to be an addict, an alcoholic or intoxicated person or may have a family member who abuses drug or alcohol.

Consent by Minors to Medical Procedures Act, 410 ILCS 210/0.01 *et seq.*; *Consent by Minors to Medical Procedures Act*, 410 ILCS 210/0.01 *et seq.*

The federal regulations governing alcohol and drug abuse treatment (the “Part 2” regulations) similarly provide that minors age 12 through 18 may authorize release of their own information. 42 CFR 2.15

Mental Health Services – Consent and Parental Access/Notification:

Illinois law permits minors age 12 and older to receive a limited amount of counseling services or psychotherapy on an outpatient basis without parental consent, and providers are *prohibited* from notifying the minor's parents without the minor's consent "unless the facility director believes such disclosure is necessary," in which case the minor must be informed. *Mental Health and Developmental Disabilities Code*, 405 ILCS 5/3-301.

Minors age 16 and older may be admitted to a mental health facility and treated as an adult; however, in that case, parental consent *is required*. *Mental Health and Developmental Disabilities Code*, 405 ILCS 5/3-302.

Under Illinois law, minors age 12 through 17 have the right to access and authorize release of their own mental health and developmental disabilities records and information, and their parents have such rights only if the minor does not object or the therapist does not feel there are compelling reasons to deny parental access. (Nonetheless, parents may receive information regarding the minor's physical and mental condition, diagnosis, treatment needs, services provided/needed, and medication.). *Mental Health and Developmental Disabilities Confidentiality Act*, 740 ILCS 110/5.

Birth Control Services

Further, birth control services and information may be given by licensed physicians to any minor who is:

- Married;
- A parent;
- Pregnant;
- Has parental consent;
- Is referred by a physician, clergyman or planned parenthood agency;
- Or where the failure to provide such services would create a serious health hazard.

Birth Control Services to Minors Act, 325 ILCS at 10/1.

Parental Access/Notification Provisions

These laws are generally silent as to the issue of parental access to the minor's information, except, for example, in the case of:

- STD and Alcohol/Substance Abuse – Parental Involvement. In the provision of diagnosis or treatment relating to sexually transmitted disease and alcohol/substance abuse for a minor, reasonable efforts must be made *upon the minor's consent* to involve the minor's family in treatment, if not detrimental to the minor's care.

- STD – Parental Notification. In the diagnosis, treatment or counseling to a minor who has come into contact with any sexually transmitted disease, providers may but are not required to inform the parent or guardian concerning treatment.
- Alcohol/Drug Abuse – Parental Notification. Persons providing counseling to a minor who abuses, or has a family member who abuses drugs or alcohol *are prohibited* from informing the parent or guardian without the minor's consent unless necessary to protect the safety of the minor or another person.
- HIV Test Results. In the case of HIV test results, the encourages but does not require reasonable efforts to notify the parent if the provider believes such to be in the minor's best interest and the provider has been unsuccessful in persuading the minor to do so.
- Mental Health Services – Parental Access and Notification. (See above discussion.)

Consent by Minors to Medical Procedures Act, 410 ILCS 210/0.01 *et seq*; AIDS *Confidentiality Act*, 410 ILCS 305/9.

Appendix 8 - 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 9 - 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 10 - 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 technical 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 11 – 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 technical 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