Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Variations Report

Subcontract No.
RTI Project No. 9825

Prepared by:

Shannon Smith-Ross, MPH, MS
Donna M. Travis
Virginia Headley, PhD (Headley and Associates)
Marybeth Sharp (Sharp Research)
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

November 6, 2006

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 is 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 may pose challenges to interoperability of health information exchange. 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 HISPC Privacy and Security Steering Committee (HSC) will be the reporting body for Illinois' contract with RTI. In addition, the Steering Committee will receive oversight from the Illinois Electronic Health Records (EHR) Task Force. As part of their charge, the HSC will provide RTI and the EHR Task Force with the following:

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

The HSC will have under its purview several working groups to support its objectives. These working groups include business variations working group (VWG), a legal working group (LWG), a solutions working group (SWG), an implementation plan working group (IPWG), and an ad hoc working group (AWG). HSC will determine membership of the working groups as well as review and approve all work products resulting from the groups. It is anticipated that the organization you represent will play an active role on at least one of these groups.

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

Silos of technology utilization are found throughout Illinois. Many health care organizations have been able to incorporate significant technological resources to maintain patient data. This is

particularly true of the major urban health care facilities in the Chicago area. However, very little effort has gone into enabling organizations to share data electronically with one another. Chief among the reasons for this is that the culture in Illinois is not conducive to data sharing. Information is often deemed as propriety 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, it has been a slow process. The cultural change and technical infrastructure necessary for sharing of information needs to come together before the policies and procedures necessary to facilitate health information exchange begin to become more commonplace.

Identifying viable solutions to these issues will be the next order of business for the HISPC project. Once identified and reviewed by the wider stakeholder community, a plan will be developed to implement these solutions in Illinois. Also, the business practice barriers, solutions and implementation plans will be shared on a national level.

1. Methodology Section

Upon award of the HISPC contract, the Illinois Foundation for Quality Healthcare, in conjunction with the Illinois Department of Public Health, determined the make-up of the HISPC Steering Committee (HSC). The HSC is comprised of several members of Illinois' Taskforce on Electronic Health Records (EHR). The primary goal of the Illinois EHR Taskforce is to promote and provide legislative guidance for statewide use of EHRs and improved health information exchange. The HISPC project will provide the Taskforce with needed information in the area of security and privacy to help achieve this goal. The HSC provides the leadership and oversight for the Illinois HISPC project. The HSC also provides recommendations of members for each of the working groups that make up the HISPC. The HSC has 12 members representing 11 organizations. The HSC roster and Committee Charter are included in the Appendix.

Meetings with the Variations Working Group (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 Variations Working Group (VWG) was formed from the recommendations of the HSC. The VWG consists of 13 members representing 11 organizations. The VWG met six (6) times to discuss each of the eighteen (18) scenarios provided by Research Triangle Institute (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 health information exchange (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 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 business practices are currently under review by the Legal Working Group to identify any legal drivers for the practices. Once determined, this document will be revised to include this information.

2. Summary of Relevant Findings Purposes for Information Exchange

2.1 Treatment (Scenario 1-4)

Scenarios 1 through 4 discuss the transfer of information in emergent and non-emergent situations, the amount of information that can 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 are 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 treaters.
- 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.

2.1.1 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.

2.1.2 Domains

The domains addressed in this scenario include:

- 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 US 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 US 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 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 A and C).

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

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

Patient Consent Generally Required. Under each of these Illinois laws, release of information is 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 treatment scenario requires further analysis under these special protection laws to determine whether the particular type of information requested could be released under the particular circumstances:

Mental health information. Applying Illinois law to the releasing facility in scenarios A and C, mental health information could be released if the patient is able to sign a valid "consent." Scenario A raises 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 is 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."

Substance abuse treatment information. 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 B involves 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.

Genetic test information. 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 D, the patient is requesting a deceased relative's genetic testing information that may be 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.)

HIV test information. 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 D contained such information, the releasing facility would need to have a "legally effective release" in order to comply with the Illinois law.

Form of Consent. Also impacting the timely and effective health information exchange 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 A) and for release of substance abuse records (scenario B) 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, Illinois law requiring a "legally effective release" for HIV and genetic testing information (scenario D) does not specify any particular elements or form for such a release to be valid.

Inter-state exchange. 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 D), 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 A and C, substance abuse treatment information under scenario B, or HIV or genetic testing results under scenario D), the law of the releasing facility's state would need to be addressed. We have applied Illinois law to the releasing facility, but presume that if the releasing facility was located in a different state that there would be similar restrictions and the need to comply with the particular laws of that state. We understand that, 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 we presume that the releasing facility's authorization form could be obtained.

Prohibitions against redisclosure. In each of the scenarios involving information afforded extraordinary protections under Illinois law (e.g., mental health information in scenario A, substance abuse treatment records in scenario B, and the HIV and genetic testing information in scenario D), 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.

Advance Consent. In considering the ability of providers to obtain advance consent for health information exchange (for example, authorizing release to subsequent treaters 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 A or participation in the treatment program in scenario B). 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.

Responsibility for the Health Record, Access, Transcription, and Related Security Issues. Patient Care Scenario C involves 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 proceeds to see the patient and dictate notes, which are then electronically transmitted for oversees transcription, then to his office, and then back to the facility. The facility is unable to incorporate the physician's report into the patient's record because it is encrypted. The Legal Working Group notes 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 B.) Therefore, this scenario raises 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 raises 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 impracticability 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.

2.1.3 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 is no longer private.

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.[1] 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 Legal Working Group does not believe that these type of inconsistent application of legal principles are unique to Illinois, and the future institution of either a state or national information exchange mechanism provides 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 health information exchange.

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 electronic health record 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, we note 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 seemingly unwillingness of providers to openly share information in non-emergent treatment or

[1] Illinois law requires health care practitioners and health care facilities to permit patients and persons authorized by patients to access and obtain copies of records kept in connection with the treatment of the patient. See *Code of Civil Procedure* 735 ILCS 5/8-2001 and 2003.

payment situations. We note, however, that 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 health information exchanges 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 health information exchange, the Legal Working Group does 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 health information exchange, and not a barrier.

The Legal Working Group has identified various privacy laws that impact the release and exchange of health information in Illinois. (See Appendices A and B.) 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 this analysis will need to be considered by the Solutions and Implementation Plan Working Groups.

Specifically, the following issues are 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.[2]

- 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

[2] 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.

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 A.) 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 A). 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.[3]

[3] 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 Legal Working Group 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 health information exchange.

2.2 Payment (Scenario 5)

Scenario 5 discusses 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 addresses the possible business practices that are required if a healthcare provider utilizes an EHR and provides access to the EHR to insurance company caseworkers.

2.2.1 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.

2.2.2 Domains

The domains addressed in this scenario include:

- 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.[4] [HIPAA also requires patient

[4] E.g., 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.

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 their insureds 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].

2.2.3 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 involves 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 state that they share only the "minimum necessary" data with other entities. However, the definition of "minimum necessary" can 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 PHI by employees and physicians of the hospital. However, typically electronic access is not granted to non-employees of the hospital. And although this is 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 lab 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 safequards (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 sum, 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.

2.3 RHIO (Scenario 6)

Scenario 6 discusses the participation of stakeholders in a Regional Health Information Organization (RHIO) with participation by multiple organizations in electronic health information exchange.

2.3.1 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.

2.3.2 Domains

The domains addressed in this scenario include:

- 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.

2.3.3 Critical Observations

Currently, there are no operational RHIOs in Illinois. Several RHIO initiatives are in various stages of 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 we interviewed, there are not currently any business practices surrounding RHIO activities. We would anticipate that, as the first Illinois RHIOs develop and regardless of the legal structure of the RHIO (e.g., separate corporate entity or contractual venture), the participants of the RHIO would enter into a participation agreement that sets forth the agreed upon terms for all of the foregoing.

All of the provider stakeholders state 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 state they would not share any of their proprietary data. Hospitals state 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 say 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 the others and the permitted purposes for which the particular category of information could be accessed by another stakeholder. These "rules of the road" 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 access may not be complete in all circumstances.

The statement that provider stakeholders will 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.

2.4 Research (Scenario 7)

Scenario 7 discusses 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 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.

2.4.1 Stakeholders

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

2.4.2 Domains

The domains addressed in this scenario include:

- 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.

2.4.3 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 protected health information 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 B.)

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.[5] 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 or 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 health information exchange, 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 health information exchange for any reason, not just research.

In applying these legal requirements to scenario 7, this situation involves a clinical research trial being conducted with the information of minor children with private funding from a pharmaceutical company pursuant to IRB review. Thus, 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 protected health information 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.

[5] 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.

2.5 Law Enforcement (Scenario 8)

Scenario 8 discusses the interaction of law enforcement and health care providers. Law enforcement requests a copy of a patient's blood alcohol test results to investigate an accident. It is believed that the patient may have been the cause of the accident so law enforcement would need this information to properly assess the situation. Scenario 8 addresses 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.

2.5.1 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.

2.5.2 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.

2.5.3 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 Legal Working Group 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 Exhibit A.)

One provider indicated that documentation of what was released to law enforcement would be kept in the back of the medical records.

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.

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.[6]

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 involves 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.

[6] *Illinois Vehicle Code*, 625 ILCS 5/11-501.4-1.

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

Scenarios 9 and 10 discuss Prescription Benefits Manager's (PBM) business practices and policies associated with the exchange of health information with providers. Scenario 9 discusses 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 addresses the business associate agreements that would need to be in place between the PBM and the provider.

Scenario 10 discusses the interaction of PBM1 with Company A who is considering switching services from PBM2 to PBM1 for costs savings purposes. PBM1 requires 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 tries to address the business associate agreement that would need to be in place between Company A and the PBMs.

2.6.1 Stakeholders

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

2.6.2 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.

2.6.3 Critical Observations

HIPAA does not allow for any health information exchange between companies that do not have business associate agreements. Scenario 9 involves a hospital employee covered under the hospital's self-insured group health plan. The group health plan is 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 protected health information for specified purposes. The prescribing physician is being 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 appears to have been made in connection with the provision of mental health services. The purpose of the request for information is 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 includes 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 health exchange 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 health information exchange.

Scenario 10 involves a business relationship between Company A (presumably a covered entity or a business associate of a covered entity) and two different PBMs. PBM 1 has been asked to provide services involving data analysis of claims information for cost-savings purposes. PBM provides 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. It appears that PBM 1 has requested Company A to forward the same claims information that PBM 2 uses in connection with its claims processing functions. Questions raised by this scenario include 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.

2.7 Healthcare Operations/Marketing (Scenarios 11 and 12)

Scenarios 11 and 12 discuss health care providers' policies on marketing services to targeted subsets of patients. Scenario 11 identifies an integrated health delivery system (IHDS) consisting of critical access hospitals and a large tertiary hospital. The IHDS would like 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 addresses the possible business practices that are required if a healthcare provider conducts marketing using protected health information (PHI) with their consumers.

Similarly, Scenario 12 discusses the interaction of a hospital obstetrics department with the marketing department. The marketing department requests 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 addresses the use and sale of identifiable patient data for marketing and fundraising purposes.

2.7.1 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.

2.7.2 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 US mail on an encrypted CD.

2.7.3 Critical Observations

There seems to be varying interpretations on HIPAA guidelines for operations and marketing purposes even though providers often refer 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 this scenario, including the following. If an outside organization were used for marketing, they 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 US mail on an encrypted CD. The requirement for the development of business associate agreements presents a barrier for the implementation of health information exchange initially, but once executed, should facilitate the standardization of health information exchange.

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 (these steps may differ by organization) who will inform the marketing department.

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

2.8 Bioterrorism Event (Scenario 13)

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

2.8.1 Stakeholders

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

2.8.2 Domains

The domains addressed in this scenario include:

- 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.
- 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.

2.8.3 Critical Observations

Actual bioterrorism events are unprecedented in Illinois, and as such, no routine business practices exist 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 exchange of health information.

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 exchange of health information 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 health information exchange.

The Illinois Department of Public Health (Department) 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, the Department, 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 FOIA 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).

The Department 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 the Department. The Code provides, among other things, that such reports shall be confidential and not subject to disclosure.

HIPAA Impact Upon Communicable Disease Reporting

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 the Department's continued ability to receive health information related to the mandated reporting of diseases, injury, and vital events as well as the Department'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 the Department, 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 the Department. 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 bioterroism 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 Department of Health and Human Services indicates that the Privacy Rule does permit covered entities to disclose protected health information, 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 protected health information, 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 protected health information 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 protected health information, 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.

2.9 Employee Health (Scenario 14)

Scenario 14 discusses 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.

2.9.1 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.

2.9.2 Domains

The domains addressed in this scenario include:

- 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 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.

2.9.3 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.

2.10 Public Health (Scenarios 15-17)

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

2.10.1 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.

2.10.2 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 protected health information 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 protected health information 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.

- 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 protected health information to relatives occur only with express written consent of patient.

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

2.10.3 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. 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 law 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 health information exchange.

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 health information exchange. On the contrary, it is widely regarded that functional electronic health information exchange 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 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.

2.11 State Government Oversight (Scenario 18)

Scenario 18 discusses a request by a state governor for protected health information about immunization and lead screening of children to be supplied to researchers at a state university for analysis. There exists neither a legislated mandate for the consolidation of this data, nor a contract with the university to provide analytical services.

2.11.1 Stakeholders

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

2.11.2 Domains

The domains addressed in this scenario include:

- 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.

2.11.3 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 protected health information are generally neutral with respect to the implementation of electronic health information exchange (see Section 2.4), 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.

3. Summary of Critical Observations and Key Issues

The assurance of security and privacy are critical to the successful proliferation of health information exchange 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. 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.

4. Appendices

HISPC Steering Committee Charter
HISPC Variations Working Group Charter

ILLINOIS FOUNDATION FOR QUALITY HEALTH CARE

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 Merriweather	Illinois Hospital Association	630-276-5590 Pmerriweather@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

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 Merriweather	Illinois Hospital Association	630-276-5590 Pmerriweather@ihastaff.org
Debra McElroy, MPH., R.N.	Kane County Health Dept.	(630) 208-3801 McElroyDebra@co.kane.il.us
Robert G Nadolski	The Alden Group	(773) 286-6622 rnadolski@aldengroup.org
Mary Ring	Illinois Hospital Association	630-276-5590

Committee Members	Organization	Phone/Email
		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.