## Appendix 8 - Barriers to the Implementation of e-HIE in Illinois

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

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

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

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

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

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

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

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

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

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

- Consumer Knowledge About Health Information Barriers

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

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

- Privacy and Security Leadership Development Barriers

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

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

➢ Global Market Barriers

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

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