The Privacy and Security Gaps in Health Information Exchanges

A White Paper by the AHIMA/HIMSS HIE Privacy & Security Joint Work Group

April 2011

Table of Contents

EXECUTIVE SUMMARY

There are many mutual and overlapping interests around the issues of privacy and security in the context of Health Information Exchange (HIE). The Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA) formed a collaborative work group (The Workgroup) to address the issues surrounding privacy and security in Health Information Organization (HIO)/HIE initiatives, an effort to leverage the work of the State Level HIE (SLHIE) projects, the work coming out of the Health Information Security and Privacy Collaboration (HISPC) project, and the recommendations of the HIT Policy Committee Privacy and Security Tiger Team. The intent is not to produce a privacy and security "bible" but to highlight the privacy and security issues in the various domains within the HIE environment that need to be considered when forming an HIO or implementing an HIE.

For clarity, the HIE provides the mechanism for sharing health-related information in a secure manner, protecting the confidentiality of the information among diverse stakeholders. The HIO is an organization providing governance and oversight. In many instances, HIE has been used to describe both the process of health information exchange and the entity overseeing and governing the exchange. Consequently, HIE and HIO have been often used interchangeably. "To provide greater clarity, these terms are defined to achieve separation of meaning."[1]

Best practices in privacy and security surrounding protected health information (PHI) are the cornerstones to the trust relationships necessary when exchanging health data across the continuum of care. As HIO/HIE initiatives are deployed, the healthcare industry will continue to be faced with new challenges to the age-old issue of privacy and security of personal health information. Industry leadership needs guidance in security practices based upon a clear understanding of the legal framework, information content and context, and technical solutions including technical standards, architectures, and frameworks necessary to achieve secure and effective interoperable HIE. Many of these issues and solutions are not unique to healthcare and much can be learned from other information-intensive industries such as banking, payment cards, insurance, and finance.

This white paper has broken down privacy and security into several subparts discussed below. It is important to understand that all of the components discussed below, when taken together, provide the single most effective way to protect personal health information. An organization with robust privacy and security policies and practices will be at significantly less risk for inappropriate disclosures than one that is not.

The Workgroup recognizes there are significant privacy and security issues yet to be resolved with the introduction and integration of personal health records (PHR). The decision was taken to exclude detailed consideration of PHR privacy and security in this paper, in part because the objectives and use of the PHR are different from many of the other types of clinical and patient-related data

[1]Defining Key Health Information Technology Terms; The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology; April 28, 2008.

exchange in an HIE network or HIO. PHRs are used and controlled by patients; HIEs are used and controlled by other stakeholders for whose primary purpose is data exchange on behalf of patients. Furthermore, the model for how PHRs should operate, co-exist, and be managed within an HIE network or HIO has not been fully developed. At this time, the advice to readers is to monitor the development of PHRs and apply the same privacy and security principles to the access and use of PHR data as would be applied to exchange any other information within a provider organization, between a provider and other providers or business partners or within an HIO.

REGULATORY ISSUES

Much has already been written on the legal implications of sharing PHI. Suffice it to say an HIO and its stakeholders need to seek appropriate legal counsel and advice when considering the consequences of sharing PHI. In establishing a relationship with an HIO or managing an HIO for data exchange, provisions need to be made for sharing information within an organization, between organizations in the same state, between organizations in different states, and even among different countries.

Policies for PHI

The Health Insurance Portability and Accountability Act (HIPAA) aligns with state expectations in the definition and control of access that will protect health information while at the same time enabling authorized users to access the minimum necessary information for continuity of care. Policies, guidelines, and agreements should be developed to ensure that access to information is granted only to those users (and roles) that have a specific need to access the information. An organization considering HIE implementation must consider the wider impact and needs to seek separate legal counsel.

The Need for Consistent Data Sharing Agreements and Standards

Entities engaged in sharing/exchanging PHI should enter into a mutual data-sharing agreement. Common data access standards need to underpin these agreements. Through application of the National Data Use and Reciprocal Support Agreement (DURSA),[2] data disclosers are expected to make data-sharing decisions based on their own organization's policies, consistent with minimum necessary legal requirements (*45 CFR 164.502(b), 164.514(d)*). This could lead to some data requestors being denied access to data because their authentication level or minimum data requirements differ from that of their data trading partners.

Interstate Exchange of Health Information

The sharing of patient information across state boundaries through either state-level, regional or local HIO as well as through the national health information network is a major concern. Specific state requirements regarding access to medical records and breach of such data are primary concerns for HIEs as privacy, disclosure, and breach laws may differ widely from state to state. For example, some states have implied participation with the promulgation of "opt-out"[3] rules – where patients have the option of not including their information in an HIE. The "opt-in" rules require a patient to specifically affirm the inclusion of their records in the HIE. In the 2010 eHealth Initiative survey of HIEs, 18 percent of HIEs surveyed confirmed that they have a policy requiring patients to "opt-in" and give formal consent before any of their records are shared via the networks. Opt-in/Opt-out is further discussed later in this paper.

---

[2] Data Use and Reciprocal Support Agreement (DURSA) Retrieved from http://healthit.hhs.gov/portal/server.pt/document/909240/dursaversionforproductionpilotsfinal_pdf on January 30, 2011.

[3] choosing not to participate

To be effective, exchange of clinical health information across state boundaries needs national regulatory guidance and harmonization of privacy and security regulations. Prior state assessments under the Health Information Security and Privacy Collaboration (HISPC)[4] project contributed a great deal of knowledge regarding the disparities among states in their approach to privacy and security and the need for harmonizing laws among states relating to the exchange of health information data. Another issue for interstate exchange of health information is the need to develop national standards[5,6,7] for locating and matching patient information across HIE entities and networks as well as across healthcare facilities and organizations in the different states.[8] Patient identity/matching is discussed later in this document. Also, see HIMSS Patient Identity Integrity White Paper.[9]

The HITECH portion of the American Recovery and Reinvestment Act (ARRA) expanded the privacy protections required for PHI. These new protections must be translated into consistent policies and practices across healthcare entities involved in the movement of health information through HIEs and across state borders.

Compliance with Meaningful Use

Stage 1 of Meaningful Use can be satisfied with relatively minimal and benign data sharing, likely to be achieved through "push messaging" (data being exchanged are "pushed" from the data supplier to a specified recipient). The Health IT Privacy and Security Tiger Team recently coined the term "directed exchange" in which healthcare providers send data on patients to other providers in a point-to-point communication. This type of exchange comes into play in many of the use cases intended to be satisfied by the Nationwide Health Information Network (NwHIN) Direct pilot project.[10]

Regulators and policy makers should use "directed exchange" to help analyze the likely scenarios for later Meaningful Use stages where more complex data sharing requirements will need to be considered. While an HIE or HIO is not required to achieve the Meaningful Use Stage 1 criteria

---

[4]The Health Information Security and Privacy Collaboration (HISPC) Project; June 30, 2007. Retrieved from http://healthit.hhs.gov/portal/server.pt?open=512&objID=1240&parentname=CommunityPage&parentid=2&mode=2.
[5]Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions, June 30, 2007. Retrieved from www.rti.org/pubs/avas.pdf on January 30, 2011.
[6]Privacy and Security Solutions for Interoperable Health Information Exchange: Nationwide Summary, July 20, 2007. Retrieved from www.rti.org/pubs/nationwide_summary.pdf on January 30, 2011.
[7]Harmonizing State Privacy Law. Retrieved from http://healthit.hhs.gov/portal/server.pt?open=512&objID=1280&PageID=16053&mode=2&cached=true on January 30, 2011.
[8]Perspectives on Patient Matching: Approaches, Findings, and Challenges. Retrieved from http://healthit.hhs.gov/portal/server.pt?open=512&objID=1240&parentname=CommunityPage&parentid=25&mode=2&in_hi_userid=11673&cached=true#reports on January 30, 2011.
[9]Patient Identity Integrity A White Paper by the HIMSS Patient Identity Integrity Work Group, December 2009. Retrieved from www.himss.org/content/files/PrivacySecurity/PIIWhitePaper.pdf on January 30, 2011.
[10]Department of Health and Human Services Centers for Medicare & Medicaid Services, 42 CFR Parts 412, 413, 422 et al. Medicare and Medicaid Programs. Electronic Health Record Incentive Program. Final Rule. Federal Register /Vol. 75, No. 144. Wednesday, July 28, 2010. Page 44319. Retrieved from edocket.access.gpo.gov/2010/pdf/2010-17207.pdf on January 30, 2011.

exchange requirements, the industry is anticipating that future criteria requirements will require the establishment of an HIO and use of an HIE.

ADMINISTRATIVE SECURITY

An HIE initiative presents a complex technical environment for the management of sensitive PHI. Consumers and stakeholders need assurance that the accuracy of data and access to data are controlled and managed effectively and in an auditable way.

HIPAA defines administrative safeguards as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."[11] In this section, we address administrative security considerations that are unique to HIOs.

Implement a Robust Governance Framework

Only those authorized to access and share patient data should be able to do so; the records that are shared should be kept confidential; any breach should be captured and reported according to the regulations and laws.

The ONC Policy Committee's Governance Workgroup has provided recommendations for governance criteria for the Nationwide Health Information Network. The Policy Committee plans to issue a Notice of Proposed Rulemaking in late 2011 that will formalize these requirements. This information, while binding only as a condition of participation in this specific exchange activity, may be useful to HIOs. Watch for more information at: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cached=true&objID=1142.

Define and Implement Clear Policies for Changing Demographic and Clinical Data

In an information-sharing environment, the ability to maintain consistent, accurate data requires not only good systems, but also effective control processes. Any changes to patient-related information must be tracked back to the individual making the change with a clear indication of the change that has been made. Policies must clearly define who can change data and under what circumstances. Additionally, the means by which changes are communicated to source systems need to be clearly defined. This in turn drives the actual clinical and health information that is accessed and used by clinicians in the patient care delivery process.

Defining the Roles and Responsibilities with Respect to Data Stewardship

As the use of electronic patient records and HIEs become more widespread, records may be both virtual and aggregated across multiple providers. A critical issue is how to protect the virtual part of the health record that does not maintain a physical presence. A view of data ownership is that healthcare providers "own" a patient's medical record maintained within their systems, and patients possess the right of access. (This may vary depending on the state in which the provider is based). However, the deployment of HIE networks and HIOs places health information in a trust capacity,

[11] **§** 164.304 Definitions

with the healthcare provider acting as trustee or "steward" for the patient's benefit to create, receive, protect, and disseminate patient-specific health information.

A white paper by the National Committee on Vital and Health Statistics[12] states, "the term *health data stewardship* refers to the responsibility of ensuring the appropriate use of personal health data. The purpose of stewardship is to realize the greatest possible benefit from the effective and appropriate use of data while minimizing the risk of harm."[13]

Providers - Data Stewardship

Providers are often the "source" of data they hold about a patient, in that they conduct initial intake and put the data in electronic form. But it is important to note that they also have an obligation to disclose data directly to the patient or to other authorized individuals or organizations on request. They are responsible for making that disclosure only to authorized individuals and to do so safely and securely, sending only the minimum data necessary. In this sense, they are acting as a data steward.

HIE/HIOs - Data Stewardship

At the highest level, data stewardship is a process for ensuring data integrity. For an HIE initiative, determining which party is responsible for providing protections in the data exchange process is an important issue to resolve. Most HIEs use the principle that the party who has administrative control of the data at any moment is responsible for protecting it. Entity-oriented HIE models generally treat the HIE/HIO entity itself as a HIPAA business associate for each subscribing Covered Entity. These are typically a consortium of healthcare providers, HIOs, State Level HIE organizations (SLHIEs, Regional Health Information Organizations (RHIOs) Integrated Delivery Networks (IDNs), and Hospital-based HIEs. Although each participating entity has its own policies, it is important to harmonize as many data exchange policies as possible. The policies by which the HIEs/HIOs govern and operate are often set by the participating entities

HIE initiatives often work with businesses and institutions that are subject to state and federal breach notification laws; HITECH requires HIEs to be subject to the breach notification rule as a business associate. This statutory obligation, along with their legal and contractual obligations, provides incentives to prevent and manage breach of data within the HIE initiative. The ability to share data is complicated when data from one provider obtained through an HIE initiative is incorporated into a second provider's record. Then the question becomes: "who is responsible for the integrity of that data once it has been added into the second data set?"

When HIE/HIO initiatives consider linking information systems and organizations that generate information, it is fundamental that they have in place appropriate agreements to govern the sharing of patient-related information. There should be clear and unequivocal policies stating that regardless of who originally created the record, any provider asked to exchange data must act as the steward

---

[12] "Health Data Stewardship: What, Why, Who, How, An NCVHS Primer." Retrieved from www.ncvhs.hhs.gov/090930lt.pdf on January 26, 2011).

[13] Health Data Stewardship: What, Why, Who, How, An NCVHS Primer." Available at www.ncvhs.hhs.gov/090930lt.pdf.

for that combined record – which includes both protection and sharing according to the policies of the entity where the combined record resides. Once the data have been taken into a provider's record, that provider must be able to use it and disclose it in just the same way as if the data had been originally obtained through their own efforts within their own organization. Any attempt to segregate data obtained from others and apply unique consent or other authorization rules will result in making HIE exchange activities unworkable.

Requirement for Unique User Identification

HIPAA, in Section 164.312(a)(2)(i), requires that each user be uniquely identifiable and that the user's activities be identifiable while logged on to the system. No two users may share the same identity and all users must be distinguishable in the usage logs. These rules are even more important when considering that an HIE will employ a user's personal attributes and role, in part, to make determinations on how to share data. A physician who has given his or her login credentials to a colleague would be accountable for any actions that that other person takes – creating a liability situation for either the individual physician or user and also for the entity he or she works for. It is very important that any entity considering participation in an HIE has rigid policies and procedures in place to avoid shared identities and shared credentials.

Restricting Access to Data by Role and Other User Attributes

Users have many associated attributes – some associated with them as a person or professional, and others associated with their job function(s), role(s), or location(s). Some consumers have expressed the concern that beyond physicians and nurses, there are many other people representing various organizations who may have access or have need to access their records; and to some extent that is true. HIPAA has provided for TPO[14] – that is, access is acceptable without getting specific consent for reasons of Treatment, Payment and/or Operations.[15]

However, HIPAA and several states' laws have more restrictive language when it comes to the type of data that can be accessed. As a general rule of thumb, for authorization, access to data is restricted to only that data necessary to accomplish the reason for access. This is called the "minimum necessary"[16] requirement. This is a function that is typically controlled by the application system; however, there are no generally available methods that are applied across the industry to make the "minimum necessary" access determination. HHS' Office for Civil Rights (OCR), the group responsible for enforcing the HIPAA privacy and security rules, is due to publish a guidance document on minimum necessary, to comply with the ARRA statutory requirement that they do so.[17]

Access to data through HIE initiatives may also be restricted based on the type of entity making the request. For example, while providers working in a patient care setting (e.g., hospital, physician

[14] § 164.520; (ii)a Notice of privacy practices for protected health information.
[15] U.S. Department of Health and Human Services Office for Civil Rights. HIPAA Administrative Simplification. Regulation Text. 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through February 16, 2006). Page 45. Retrieved from www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf on January 30, 2011.
[16] §164.506; (iii)b Standard: Minimum necessary
[17] American Recovery and Reinvestment Act of 2009. Page 151. Retrieved from http://thomas.loc.gov/cgi-bin/query/z?c111:h1 on January 30, 2011.

office) would be expected to request data, and would be granted access to data, the same provider who works part time as a case reviewer for a health plan would either have significantly restricted access, or no access at all when working in that capacity.[18]

Unique Patient Identifier

The HIPAA statute actually requires that there be a Unique Patient Identifier (UPI) for each patient. That provision still stands today in the statute. However, due to concerns of privacy advocates, implementation of that requirement has been effectively placed on hold through a ban on the use of funds to implement it, which is contained in the annual congressional appropriation bill that makes funding available to HHS.

There has long been discussion around the viability and acceptability of a UPI and its potential for uniquely identifying patient data on a single patient, and as a potential identifier that can be used for access to patient data. A recent RAND Report[19]concluded that the U.S. healthcare industry could benefit immensely from creation and use of a UPI. But the ink had not dried on the published study before many privacy-advocacy groups uniformly rejected its content and conclusions. HIMSS also published a White Paper on Patient Identity Integrity that discusses the benefits of a UPI.

While there is clearly an advantage to be gained in having one uniform identifier to authenticate and authorize consumers (patients) who wish to access their healthcare records held in EHRs, HIEs, or PHRs, nothing nationally available exists at this time. There are some promising experiments in this area, such as the Kantara eCitizen Foundation project.[20] This project creates a working portal that will provide identity functions necessary to conduct healthcare-related interactions and transactions. The intent is to use existing business, legal, and technical components where available and to identity gaps to demonstrate the viability of existing identity solutions for the facilitation of healthcare through electronic means in an open, public integrated architecture.

Identity Management

Identity Management is a framework of policies, procedures, processes, and technologies that enable an organization to manage the identities and privileges of its users during their entire association with the organization and access the data it holds. The process begins with Identity Proofing, also known as Personal Identity Verification, which is the process of verifying that the individual is who he or she claims to be, and has the certifications and credentials sufficient to prove their claim. Identity Proofing can be as simple for some employees who have no special access privileges as verification of a driver's license or other state-issued identification, or as complicated as requiring a birth certificate or passport coupled with a certified document from a state agency, such as a medical licensing board. Typically, as a user's access privileges to a computer system become

---

[18]HIPAA Administrative Simplification Regulation Text. § 164.312 Technical safeguards. March 2006. Retrieved from www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf on January 30, 2011.
[19] www.rand.org/pubs/papers/P6628.html.
[20]eCitizen-Kantara Patient ID Service Projecthttp://www.ecitizenfoundation.org/.

broader and more functionally rich, the Identity Proofing requirements grow more stringent accordingly.

Once an individual's identity is verified, he or she is registered as a user on an entity's network and access is subsequently granted for the job-required applications (also called user provisioning). Unfortunately, although many provider entities do a reasonable job of verification and registration, once a user is granted access, management of that access results in use privileges becoming lax. It is just as important for an entity to provide ongoing management of its user identities throughout their employment, as they change roles and application access is added or removed, especially when their employment terminates. If users are not removed from active registration or deactivated, the entity runs significant risk of having unauthorized access by such terminated parties. Identity Management is comprised of this end-to-end process.

Authentication

The second step in the process of managing access to computer applications occurs when the user logs into the network to access the applications for which he or she has been granted privileges. This step is the electronic authentication of the user – in other words, it is the process of verifying the user's credentials to establish confidence that the user is who he or she claims to be. Authentication can simply be described as a process of the user providing to the computer system a unique identification, such as "user identification," after which (or in addition to the ID) the system will also request a secret password, known only to that user and to the system. Once the user responds appropriately with the correct password, there is a degree of confidence established that the person trying to gain access is actually that person known to the system. This is very often termed "one-factor" authentication, in that the user provides one piece of information only he or she "knows" in order to complete the process. In this example, it is clearly important for the user to keep the password confidential so that some other individual cannot "pretend" to be that person by using the password.

Authentication is a well-defined process which can make use of one or more of three different types of attributes or "factors" to establish an assurance that the user is as claimed – these attributes are:

- Something you know – such as a password, or a shared secret (many systems now use one or more secret questions, the answer to which is only known by the user);
- Something you have – such as an identity token, a badge with an internal identification chip or bar code;
- Something you are that makes you unique – such as a fingerprint, voiceprint, or retinal image.

The more attributes that are used, the more secure the authenticated identity, but the more expensive the technology may be to administer the authentication process.

The National Institute of Standards and Technology (NIST) defined four different levels of authentication strength – each level providing an increasing assurance of confidence in confirmation

of the user's identity (see Table 1).[21] These levels utilize different combinations of identity proofing and authentication attributes to establish identity confidence as shown in the simplified table below:

Table 1. NIST Levels of Authentication

Assurance Level	Confidence	Identity Proofing	Factors Required	Authentication threats addressed by this level
Level 1	Ok	Not Required	One	Online guessing; replay
Level 2	Good	Basic – one form of verifiable ID	One - Specific protocol	Online guessing; replay; session hijack, eavesdropping
Level 3	Better	May require two forms of ID	One - Specific protocol	Online guessing; replay; session hijack, eavesdropping; phishing / verifier impersonation; man-in-the-middle (weak)
Level 4	Best	Must be in-person verified by certifier	Two or more - One is a hard token for external verification.	Online guessing; replay; session hijack, eavesdropping; phishing / verifier impersonation; man-in-the-middle (strong)

Today authentication in most healthcare entities is accomplished through simple Level One authentication – mostly using a unique user-ID and a secret password. While this method has been considered "good enough" in the past, and it meets the HIPAA requirements, it has been typically used in a controlled environment – that is, it is used within one entity's walls. HIE, and specifically the need for authentication beyond a single entity's walls, has increased the vulnerabilities to different types of threats not typically found inside an organization's firewalls. Hence, we are seeing higher level requirements being specified by the Federal Government for functions such as e-prescribing of restricted medications and by the states as they address security concerns relative to HIE.

Industry Adoption

As discussed in the authentication section above, two-factor authentication is a much better method for authenticating a user, with higher confidence than single-factor authentication. A federated identity model provides users safe access to applications across the Internet without the need for multiple login credentials. It allows organizations to share credentials and attributes for

[21]NIST Special Publication 800-63. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf on January 26, 2011. [21]HITSP Access Control Service Collaboration 108; 07.08.2009. Retrieved from www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=12&PrefixNumeric=108 on January 26, 2011.

authentication and authorization, reducing the need to maintain user profiles in multiple systems. Federation's most visible aspect, Secure Internet Single sign-on, reduces security gaps by using a trusted connection between the enterprise, also known as the identity provider (IdP), and the service provider.

In the case of a federated identity model, many entities are requiring two-factor authentication.[22] The healthcare industry should set, as a minimum level, the use of two-factor authentication for all HIE users in the country, which would improve public confidence in HIE access management. As more HIE initiatives adopt and use two-factor authentication, those still using Level One or Level Two authentication will rapidly become isolated in their ability to exchange data outside their own jurisdictions. However, it should be noted that some organizations are moving to a minimum requirement of multi-factor authentication. This will require HIE initiatives to consider how to incorporate these organizations into their HIE Security Framework.

HIE initiatives and HIOs need a roadmap to achieve the proposed level and approach to authentication and the management of risk along the way. Basic requirements must be defined that include user name and password, with two-factor authentication as the goal. The roadmap requirements should cover the strength of the password and the necessity of changing the password every 90 or 180 days. Many organizations lack a transition plan or the resources needed to connect to the HIE using any more than a single factor authentication.

TECHNICAL AND PHYSICAL SECURITY

Technical and physical security encompasses, and is a part of, all the other essential elements for a strong security foundation that enforces and protects the confidentiality, integrity, and availability of health information. The technological knowledge, standards, and equipment provide the environment crucial to ensuring the privacy of the exchange participants while enhancing the trust of users.

The 2010 HIMSS Analytics Report *Security of Patient Data* reported that breaches of PHI increased by six percent in 2010 to 19 percent of total respondents, even though 87% of respondents indicated that they have policies in place to monitor access and sharing of electronic health information.[23] Other research shows that 84% of healthcare breaches since 2003 were due to "low tech" incidents such as lost or stolen laptops, improper disposal of documents, stolen backup tapes, etc.[24]According to the Ponemon Institute, the average cost to the organization to correct a record is $202, with total costs to organizations ranging from $341,000 to over $5 million.[25]

---

[22]HITSP Access Control Service Collaboration 108; 07.08.2009 , Accessed January 26, 2011; www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=12&PrefixNumeric=108.

[23] 2010 HIMSS Analytics Report: Security of Patient Data Commissioned by Kroll Fraud Solutions. April 2010. Retrieved from www.krollfraudsolutions.com/about-kroll/HIMSS-Security-Patient-Data-return.aspx on January 30, 2011.

[24] HIMSS Analytics. Healthcare Industry Continues to Overlook Critical Gaps in Data Security, According to New Bi-Annual Report. Retrieved from www.himssanalytics.org/general/pr_20100421.asp on January 30, 2011.

[25]Ponemon Institute, LLC. Fourth Annual US Cost of Data Breach Study Benchmark Study of Companies Sponsored by PGP Corporation. January 2009. . Retrieved from www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf on January 30, 2011.

Risk Assessment – HIOs and HIE Participants Accountability

The American Recovery and Reinvestment Act of 2009 stimulated the development and implementation of HIO/HIE initiatives nationwide. The Workgroup recognizes the necessity to discuss the HIO's compliance with the Privacy and Security Rule and its responsibility for oversight and ensuring accountability of its participants. The organization should undertake a Risk Assessment to understand the risks associated with confidentiality, integrity, and availability of e-PHI. This assessment provides the basis on which to implement reasonable and appropriate safeguards commensurate with the criticality of the data. Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications not only for the HIO but also for participants of the HIO. The Risk Assessment will drive the process to identify and mitigate any potential opportunity for cyber crime and serious security breaches while balancing the cost of proposed measures versus the threat of the breach and potential notification.

As part of the HIO's application process for participating organizations, an applicant should complete a compliance questionnaire.[26] The Participation/Data Sharing Agreement should state that there will be a review of the organization's Annual Risk Assessment and all supporting policies and procedures at the time of the Readiness Assessment.

HHS' OCR was made responsible for enforcing the HIPAA Security Rule[27] (45 C.F.R. §§ 164.302 – 318.) on July 27, 2009. OCR's enforcement activities have strived to improve the privacy practices of covered entities, improving the privacy protection of health information for all individuals. Through a series of guidance documents, OCR assists organizations[28] to identify and implement the most effective and appropriate administrative, physical, and technical safeguards to secure e-PHI.

The Security Management Process standard in the Security Rule requires organizations to:

"[I]implement policies and procedures to prevent, detect, contain, and correct security violations." (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

> RISK ANALYSIS (Required).
>
> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].[29]

---

[26] See NIST SP 800-66, Section #4 "Considerations When Applying the HIPAA Security Rule." Available at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf.

[27] Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.

[28] As used in this guidance the term "organizations" refers to covered entities and business associates. The Guidance will be updated following implementation of the final HITECH regulations.

[29] Security Rule Guidance Material on Risk Analysis Requirements under the HIPAA Security Rule.

All e-PHI created, received, maintained, or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI.

Lack of Technical/Physical Standards for HIPAA Covered Entities

According to HIPAA, the contractual agreement between business associates (BAs) should be concrete and enforceable to ensure that all security and privacy requirements are met by all parties. ARRA amends HIPAA to cover BAs directly by the requirements of the privacy and security rule. Additionally, in the case of any loss or breach of health information at or under the control of a BA, it must be reported by the BA to the Covered Entity (CE) and then subsequently by the CE to HHS and/or the Federal Trade Commission (FTC).

Both CEs and BAs are legally responsible and potentially liable for any loss and/or breach that occurs. The HIO may be considered a BA and, therefore, must provide appropriate security for health records. There is no requirement under HIPAA or HITECH for a CE to perform an audit of its business associates to verify adherence to HIPAA. However, it is implied that the CE is legally just as liable for security of the health information as its BA under the binding agreement.

ACCESS MANAGEMENT

The discussion above focused on Authentication as a key part of Administrative Security. The ability to accurately identify and confirm that a person, user, or patient is who they say they are, when considering controlling access to an HIE, the other part of the equation – Authorization – is just as important. The key is that a person is only given access to those applications and data for which he or she has approval. This section explores these issues in more detail below.

Authorization

Authorization is the main mechanisms for ensuring users have access to only those applications and the protected health information that they are allowed to use or review. Just because a user is identity proofed and subsequently authenticates properly does not automatically give the user rights to access just any set of information. While an emergency physician working in an emergency room on a trauma case may be granted a wide range of access privileges (his or her authorization would allow access to many different data sets and functional capabilities), that same physician, working in the capacity of a health plan reviewer, may have very limited privileges, if any. Access privileges are assigned to individuals typically based on their professional position, the role that they play in the organization, and their need for access to various applications and data. Access privileges may vary further by type of organization and sensitivity of data. This is generally called Attribute-Based Authorization Control (ABAC), and is becoming a common method for authorization as HIE initiatives becomes more widespread.

D. Richard Kuhn, National Institute of Standards and Technology recently provided this explanation of ABAC.[30]

> Role Based Access Control (RBAC) has frequently been criticized for the difficulty of setting up an initial role structure and for inflexibility in rapidly changing domains. A pure RBAC solution may provide inadequate support for dynamic attributes such as time of day, which might need to be considered when determining user permissions. To support dynamic attributes, particularly in large organizations, a "role explosion" can result in thousands of separate roles being fashioned for different collections of permissions. Recent interest in attribute-based access control (ABAC) suggests that attributes and rules could either replace RBAC or make it more simple and flexible.

All users, no matter who they are and what roles they play in an organization, possess a set of attributes. There are identity attributes such as the person's name, perhaps a pseudonym or User ID, their work hours, address, phone number, Social Security Number, and other such items gathered about the individual during the hiring process or on-boarding. There are also professional attributes which are indicative of the individual's skills and professional capabilities such as degrees, licenses, certified skills, and so forth. All of these are descriptive of the user, and while most often are not part of authorization, are none-the-less personal attributes which could be made available to determine access to systems. Additional attributes which are typically used to determine access are type of organization, role in the organization, and staff position (e.g., a nurse would be further classified as LPN, RN, or LVN for determinations in medication management, or physicians may be further classified by their specialty when it comes to access to sensitive data).

Federated Access Management

HIE by its very nature integrates multiple sources of data, where the patient's records from a particular physician's visit reside in one location, and the data are needed in a different location. Today some smaller HIOs maintain a centralized registry of all users of their services, but HIOs of reasonable size are finding that maintaining such registries is a significant effort as their user base grows. HIOs and HIE initiatives are now beginning to adopt federated user authentication, and cross-enterprise authorization as the preferred approach. Under these scenarios, the authentication process occurs locally within the data requestor's security domain, and the receiver of the data request, or the HIE initiative that brokers the request, has agreed to trust the results from the authentication process of the data requestor's domain. Authorization is accomplished much the same way, but with the important difference that while the attributes are asserted by the data requestor, determination of the requestor's ability to access data in the other entity's system is based on application of that entity's access policies – not those of the requestor.

---

[30] D.R. Kuhn, E.J. Coyne, T.R. Weil, "Adding Attributes to Role Based Access Control", IEEE Computer, vol. 43, no. 6 (June, 2010), http://csrc.nist.gov/groups/SNS/rbac/documents/kuhn-coyne-weil-10.pdf.

Access to PHI for Case or Disease Management by Health Plans

As discussed above, HIPAA provides for access to data for TPO. As Covered Entities, health plans are given access to patient records as part of their responsibility for managing the overall care of patients as they move through care settings. This type of access has the potential to become even more prevalent as health reform and structures such as Accountable Care Organizations become more common. Health plans see HIE initiatives as a good way for them to receive aggregate data on their insured patients in order to determine if their treatment meets the standards they require from their participating physicians.

Currently, health plans have limited access to information that is not directly supplied by the provider and not to data available through an HIO/HIE initiative as defined by their business associate agreements. While the plans do have access to their own claims data, they also have access to dispensing data for Medication Therapy Management (MTM) patients – even data for self-pay prescriptions. This is not thought to be a significant issue today (most MTM patients have many prescriptions and over the counter medications and are supportive of their pharmacy benefit managers having access to all data), but as HIE initiatives start carrying more of the load of supporting provider messaging and ePrescribing, care will need to be exercised to make sure that appropriate consents are in place when otherwise restricted data are made available through the HIO/HIE initiatives.

HIPAA Security Standard for Employee Health Plans

Under HIPAA, a health benefit plan is a HIPAA covered entity, but the employer who sponsors the plan is not. Because the employer sponsor of a health benefit plan is, under the Employee Retirement Income Security Act (ERISA), a separate legal entity from the plan, the transfer of health information to the employer or to the administrator of the plan is actually considered a disclosure. The HIPAA regulations, however, do not consider an employer sponsor to be a business associate of the plan. Rather, the regulations contain special rules for disclosures to a plan sponsor, in recognition of the fact that the employer is a separate legal entity from its plans even though the employer may administer the plan. Under HIPAA, group health plans may disclose PHI to a plan sponsor, or permit an insurance issuer or HMO to disclose PHI to a plan sponsor, only to carry out "plan administration functions," so long as the plan documents are amended in accordance with the regulations. HIPAA requires that a health plan's documents be amended to provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate certain provisions. This includes that the plan sponsor will inform the plan of any unauthorized use or disclosure of which it becomes aware.

Employer sponsors of health plans may receive identifiable health information from sources other than from the health plans it sponsors. This situation is not covered by HIPAA. In most states, the law does not require the employer to implement any particular security standard with respect to this information.

Third Party Use of PHI for Wellness Programs

HIPAA provides for business associates who perform work for a covered entity to enter into agreements when they must access and use PHI to accomplish the work required. An example would be a health plan that wishes to engage a third party to perform wellness and health assessments, and the third party would need access to health plan data. The health plan may contract with an educational institution to conduct the health assessments. Educational researchers are considered business associates for such wellness assessments. However, researchers at the same educational institution may not use the PHI received for other research purposes. If the educational institution wishes to use PHI for another research purpose, it must enter into a data use agreement and limit its research to a limited data set, obtain authorization from all patients involved, or de-identify the information prior to conducting the research. There is always the potential for a third party to misuse PHI. The business associate agreement is a very important document for protecting information and defining responsibilities and obligations for information received from the health exchange.

Access to PHI for Research Purposes

HIOs have not yet been used to accessing records for research purposes. The discussion has begun in many states that such access could not only be very useful to researchers, but could also be a revenue source for the HIO/HIE initiative. Consumer advocates and state laws around research have to date made using the HIE as a source of research data very difficult, as evidenced by the requirement for review/determinations by an Institutional Review Board (IRB) and the need for cross-population analysis to find suitable subjects.

Some HIEs have been successful in obtaining permission from their stakeholders to fully de-identify data and then use that data to perform population studies. While de-identified data is not PHI by definition, there is concern that sharing such data to use it in that way may present a risk, if it were possible to reconstruct the identity of the data. Additionally, and conversely, the HIPAA Privacy Rule permits disclosures of PHI that are required by law. This includes access for Public Health Agencies at local, national and international levels to data shared in the event that there is a public safety issue or threat.[31] More work is required to define how research can interoperate with and through HIE, but in the short term, it is safe to assume that most research data will be obtained through normal provider EHR channels.

Third-party Access

No legally mandated set of security standards applies to third parties gaining access to PHI pursuant to a HIPAA authorization, including researchers, employers, and marketing organizations.

An HIO may grant access to PHI in the form of a limited data set to researchers and public health organizations pursuant to a data use agreement. Under HIPAA, a data use agreement must (1) establish the permitted uses and disclosures of the limited data set, (2) establish who is permitted to use or receive the limited data set, and (3) provide that the limited data set recipient will (a) not use or disclose the information other than as permitted by the agreement or required by law, (b) use

[31] 45 CFR 164.512(b) Disclosures for Public Health Activities. Retrieved from www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html on January 26, 2011.

appropriate safeguards to prevent use or disclosure of the information other than as provided by the data use agreement, (c) report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which it becomes aware, (d) ensure that any agents to whom it provides the information agrees to the same restrictions, (e) not re-identify the information or contact the individuals, and (f) for only the prescribed term of the agreement.

While there is a general requirement in the data use agreement that recipients use appropriate safeguards to protect the limited data set, researchers and public health organizations that obtain PHI in the form of a limited data set are required to sign a business associates aagreement under the new ARRA/HITECH requirements and are now subject to enforcement for failure to comply with the HIPAA security standards or the data use agreement. In addition, under ARRA/HITECH, these third parties are required to report a security breach of such health information to the covered entity.

It is important to clearly outline such details as the term of the use of the data, the purpose for the use of the data, specific security and privacy safeguards, and data destruction requirement in the Data Sharing Agreement.

Health Plan User Access

The authentication and authorization processes discussed above will be in place and are functional deterrents against misuse of access privilege for any user of any entity. Each user of an exchange must be authenticated and authorized to access only specific information about specific patients, and activities such as patient browsing are generally not allowed by any user, but in particular users from Health Plans. Patient browsing or reporting functions could only be enabled by applications built for that purpose, and such capabilities are typically not available in HIE initiatives today.

PUBLIC HEALTH / POPULATION HEALTH

Multi-Stakeholder Considerations for Authorization

Although interoperability with public health is a criterion for Meaningful Use, policies to determine the use of that data for improvement of population health are still emerging. Use of HIOs and HIE initiatives in public health is still an area under development and privacy and security concerns in this area are still being determined. Patient consent issues and de-identification issues are well known as discussed elsewhere in this document and need to be addressed at the national level. Appropriate use of de-identified data and appropriate circumstances for re-identification are still being developed and will require direction from the states on the use of such data in the public health domain.

Until further guidance is forthcoming from ONC and HHS, it is recommended that HIO/HIE initiatives enter into specific business associate and data-sharing agreements in addition to DURSAs, and that Public Health participation in HIEs be primarily limited to push messaging – both from and to HIE participants. There is limited need today for query-based messaging from public health (public health entities requesting data on specific patients), and there are established paths for that communication to take place when it is needed. That said, public health should be an equal participant in the HIE, and should eventually have the ability to gather data from HIO/HIE initiatives on a request basis, just the same as providers.

Health Oversight Agencies Not Required to Comply with HIPAA Security Standards

Public health laws require information sharing (e.g., the reporting of communicable diseases by providers) based on the long-recognized premise that the public's interest in stopping the spread of disease by human-to-human contact takes precedence over the privacy needs of the individual who is discovered to have a communicable disease. HIPAA permits covered entities to report PHI to health oversight agencies at the state and federal level with patient authorization, but unless the oversight agency itself is a covered entity, no set of security standards generally applies to such agencies in their handling of identifiable health information. A state agency has oversight of HIPAA issues because they are tied to state law, but the agency has no requirement to notify clients in case of breach under HIPAA, unless such a requirement exists at the state level.

CONSUMER PRIVACY

Consent

The expanded opportunity to share health data via the HIO/HIE initiative only highlights the need for additional authorization controls, such as patient consent. This is an attribute that can be associated with either the patient's data or with the user who is requesting access. Patient consent was not a particular issue before electronic records and HIE, because patients were typically asked to sign a "consent for treatment" before providers rendered services in their facilities, or such consent was implied by the patient accepting treatment, and, thereafter, all access to the paper and electronic records were covered by that treatment consent.[32]

With electronic records and the ability to exchange data comes the ability for providers to easily share a patient's records with another caregiver outside of that provider's facility. Additionally, outsiders can electronically request information from the provider's records. The concept of getting patient consent to share records electronically is now becoming an issue of national interest, and many states are requiring providers to get the patient's permission to share records before that patient's data are made available via HIE initiatives. The HIT Privacy and Security Tiger Team recently concluded its examination of patient consent and issued their recommendations as to when providers must get a patient's consent.[33]

As indicated above, the opt-in/opt-out consent emanates from the patient's agreement to allow his or her information to be shared. Consent may range from a very broad permission to either share or not share, to a very fine-grained capability to use other attributes such as the type of caregiver (or even particular caregiver by name) or the sensitivity of data for sharing determination. In most cases today, the share/don't share level of consent is all that HIE environments and EHR software

---

[32] Office of the National Coordinator for Health IT, HIT Policy Committee, Privacy & Security Tiger Team. Letter of Recommendation to Dr. David Blumenthal, MD, on patient consent and the electronic exchange of patient identifiable health information. http://healthit.hhs.gov/portal/server.pt/document/947492/tigerteamrecommendationletter8-17_2_pdf.

[33] HHS ONC Tiger Team http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19421information. Retrieved from http://healthit.hhs.gov/portal/server.pt/document/947492/tigerteamrecommendationletter8-17_2_pdf_%282%29 on January 26, 2011.

can accommodate, but in some regions of the United States, and in some other countries such as Canada, finer-grained consent directives are possible. This is commonly called "granular consent."

Consent is typically thought of as being associated with the patient's data, and from a practical perspective, consent is typically stored with the patient's attributes and applied to the access management process when data are requested. However; in the future, consent may also have to be associated with a particular physician, with the ability for a patient to override a previous decision not to share information when his or her data are needed for subsequent treatment. If a physician obtains a patient's permission for accessing records, that consent becomes associated with the physician for that encounter. We must also recognize that there are situations such as public health and safety, or the patient's immediate safety, where a previous no-consent decision should be overridden for the patient's or public's welfare (this is commonly called "emergency mode" access.) These situations are typically very rare, and must be accompanied with clear documentation of the reasons for overriding a patient's directive and the actual access obtained (an audit trail).

Restricting Access to "Sensitive" Portions of the Record

Consumers are concerned that there may be certain parts of their records which they do not want shared with others, whether the others are other caregivers, family members, or anybody else who may otherwise have a legitimate reason for accessing their records. The authorization attributes presently in use can accommodate some restrictions – for example, records associated with the diagnosis and treatment of behavioral health issues, drug abuse, sexually transmitted diseases, HIV, and other sensitive diagnoses can be marked as "sensitive" and potentially restricted. At the present time, this is technically challenging to implement.

There are three important issues, however, associated with restricting portions of a record, or redacting information from a record:

- **Embedded data:** Consider that while it might be possible to exclude a particular diagnosis from the list of active problems such as a diagnosis of AIDS – the list of laboratory results will still provide clues to the diagnosis, and the medications list will still show Zidovudine, or AZT, as an active medication. What is even more at issue is the binary large object, basic large object or blob-type[34] records where it is not possible to perform text searches and deletions, even if such were possible and desirable. The blob type represents a binary large object. For example, a blob could be an array of bytes. Properties of type blob can have an optional length attribute. The length attribute is not allowed on collections.
- **What constitutes "sensitive" parts of the record:** Some patients may consider pregnancy to be sensitive and not something they want disclosed, while others are very proud of it and publish their first ultrasound images on a variety of social media sites. A patient seeking employment as a fireman may consider their borderline chronic obstructive pulmonary disease (COPD) diagnosis as sensitive and not something they want disclosed. Patients who are changing health plans may consider a previous disease or diagnosis, or a history of smoking even though they do presently smoke, as being sensitive information.

[34] A Blob is a collection of binary data stored as a single entity in a database management system.

At the end of the day, sensitive information is in the judgment of the patient and therefore could always be beyond the technical ability of the HIO/HIE initiative to fully define and restrict.

- **Medical-legal implications:** In any of the cases cited above, there could be potentially life-threatening consequences of not supplying the suggested information. Supplying a medication list to a physician and deleting use of a psychotropic drug because a person is concerned about his or her diagnosis of mild depression could easily lead to harmful, if not fatal, complications when other interacting medications are prescribed. Passing a patient physical exam and not noting COPD could cause serious harm to the patient and other persons if that diagnosis is directly consequent to their inability to perform. In today's legally contentious environment, restricting access or worse, attempting to revise data, this could cause more issues than it ultimately protects.

Consumers should be made aware of the significant consequences of their consent/access decisions, and if they have an issue that they feel is that important to keep secret, perhaps they might consider opting-out of electronic data sharing completely.

HIT Privacy and Security Tiger Team Recommendations

The HIT Privacy and Security "Tiger Team" published a set of recommendations in August 2010 that covered a range of issues around privacy and security, including the ability of the patient to consent to participation in an identifiable HIE at a general level and how consent should be implemented.[35] Their focus was on what is required to comply with Stage One of Meaningful Use (note: This may not be sufficient for those organizations who choose to skip Meaningful Use Stage One and opt to implement Meaningful Use Stage Two and beyond). The main points from the Tiger Team recommendations with regard to consent were:

- In the context of Directed Exchange, i.e., in the context of an exchange of data directly from one entity to another for treatment, current law and customary practice is sufficient and requires no further consent.
- When patient identifiable information is to be passed out of the control of the provider's record or the provider's Organized Health Care Arrangement, then patient should be able to exercise "meaningful consent" to their participation. (Meaningful Consent is discussed in more detail below.) The examples that were given to support this included various architectures for an HIO (federated or centralized) and situations where this information may be combined with information from other sources such as a state's Department of Health Services that is responsible for the maintenance of surveillance databases.

---

[35]Office of the National Coordinator for Health IT, HIT Policy Committee, Privacy & Security Tiger Team. Letter of Recommendation to Dr. David Blumenthal, MD, on patient consent and the electronic exchange of patient identifiable health information. Retrieved from http://healthit.hhs.gov/portal/server.pt/document/947492/tigerteamrecommendationletter8-17_2_pdf_%282%29 on January 30, 2011.

Meaningful Consent

The explanation of Meaningful Consent in the Tiger Team report includes a key requirement that "patients be provided with an opportunity to give their consent before the provider releases control over exchange decisions to another authority, such as an HIO. Where patients do not consent to participate in an HIO model, then any required exchange would be through a directed exchange."

All of the Tiger Team recommendations are underpinned by a notion that providers will inform patients about how their information is being used and address any concerns they may have about privacy and security. On the basis of this information and guidance, individuals will be able to decide whether to participate in an exchange or not. What can vary is the process by which this decision will be implemented. Also, there is significant concern about whether all physicians are equipped to educate the patient to the point of the patient being considered "educated" and/or the consent "meaningful."

The Mechanics of Consent

The common discussion around consent in the context of an HIO or HIE revolves around whether the policy should be for the individual to decide to "opt in" or "opt out" of the opportunity to have his or her records shared in this way. Each approach brings with it a set of issues and problems that can impact the performance and efficiency of individual providers' practices. The decision prompts a range of questions that need to be answered in establishing an approach to consent including:

- What does the HIO intend to do with the information held in the HIE? What is the business model of the HIO, how does it support the HIO services of data exchange, and how does it impact data sharing?
- Who are the stakeholders and what are their intentions with regard to the shared information?
- Do the rules of the exchange apply to all of an individual's record or can the individual specify that sections of the record be excluded from the exchange?
- Does the technology being used by the exchange allow appropriate access and reporting controls, such as "sealed envelope," or "emergency mode access" where information can only be accessed in certain situations where it would be deemed in the patient's best interest to have that information accessed?

The Tiger Team does not attempt to make a recommendation about a preferred approach to opt-in/opt-out but does focus on the issues affecting each approach. We have not attempted to replicate the findings and recommendations of the Tiger Team except as they illustrate the points in this section of the White Paper. We would, however, strongly recommend that readers of this White Paper also read the Tiger Team recommendations. We have outlined below the key points of each approach.

Opt-In

Opt-in is a strategy based around patients "opting in" or opting to participate in the exchange. This requires that they be informed about the implications of their information being shared. Each

individual then needs to be asked to agree to and authorize their information to be exchanged. This approval must be revocable and should to the extent possible allow for the exclusion of certain sets of information that the individual wishes not to share.

A key question here is whether patients are required to approve having their information stored in a sealed vault but not generally accessible or not to have the information stored at all. The potential benefit of having it stored in a sealed vault is that it would then be available in a medical emergency using a "sealed envelope" or an "emergency mode access" concept. If the patient's information is not stored at all, then it would negate the possibility of employing a "sealed envelope" or "emergency mode access" approach.

Opt-Out

The underlying premise behind opt-out is the default position: patients' information will be collected and stored in the HIE initiative unless the patient specifically requests that all or part of their information be excluded. The patient will need to request the exclusion (opt-out) in writing. It is possible for patients to change their requests from time to time and the same discussion as for Opt-In applies with regard to whether the data should be made inaccessible or not stored at all.

Resources and Timing

Not withstanding the discussion about Meaningful Consent above, it is inevitable that both Opt In and Opt Out methods will require that providers make the time to educate their patients on the potential uses of their information when control is handed to another authority outside of the providers practice. HIOs and their stakeholders will need to make the determination of the level of detail and approach to educating their patients that will be most appropriate to their chosen mechanism.

It is possible that an Opt In approach will be more resource intensive and time consuming than an Opt Out approach, although this will ultimately depend on the agreed approach.

Technical Constraints

In deciding on a preferred approach, it is important to ensure that the HIE system/technical architecture is able to support the necessary data capture and workflow changes. This is particularly important where there are significant requirements for Information Governance and audit as a result of a "break the glass" or "sealed envelope" approach to information access.

This section on patient consent has raised some important issues that underpin discussions on privacy and security in the context of HIE. The remainder of this White Paper makes recommendations as to how HIOs may wish to proceed in closing these gaps.

RECOMMENDATIONS

The HIMSS/AHIMA Privacy and Security in HIE Workgroup explored the privacy and security challenges HIEs are facing under six themes: Regulatory, Administrative Security, Technical/Physical Security, Access Management, Public Health/Population Health, and Consumer Privacy. These themes provided the Workgroup the ability to concentrate on specific areas of concern and identify

gaps that need to be addressed when establishing an HIE. The gaps identified under the themes have associated recommendations that can be translated into action steps for the HIO/HIE initiative.

The Workgroup recommendations are applicable for federal, state, and local HIE initiatives wishing to exchange PHI. As the healthcare industry moves forward in establishing HIE capacity, there is a need for a holistic approach based on trust through the development and implementation of common policies, processes and education supported by the technology. Our recommendations, below, are divided into three categories – Policy, Process, and Education.

Policy

HIOs should:

- Develop a comprehensive data governance strategy and framework to meet the goals of the HIE initiative. This should include data quality and integrity as well as data management policies and procedures built around privacy and security considerations and requirements utilizing the principle that "individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately."[36]
- Translate new HIPAA privacy requirements into consistent policies across the continuum of care.
- Adopt policies ensuring consistency of responsibilities to consumers among participants in the HIE initiative.
- Clarify the desired coverage/applicability of HIPAA requirements to state agencies. State agencies that collect, distribute, or exchange PHI should voluntarily implement administrative, physical, and technical safeguards to protect identifiable health information consistent with the HIPAA security standards.
- Establish privacy and security policies for employers who have access to PHI.
- Establish a common agreement such as the uniform commercial code that will identify, define and limit each party's rights, responsibilities, and liabilities in health information transactions.
- Assess the impact of the ARRA privacy and security sections on population health data and create policies that enable the compliant sharing and use of health information for population health uses.
- Adopt Federal and State Breach Notification requirements and promulgate a policy applicable to Public Health Oversight Agencies that wish to participate in the HIE initiative.
- Establish policies addressing the appropriate secondary uses of healthcare data.

[36]The HIPAA Privacy Rule and Electronic Health Information in a Networked Environment, Health and Human Services, Office for Civil Rights, 2009.

- Implement policies on required audit trail functionality relating to their technical security processes.
- Enter into a contractual agreement with Health Plan participants binding them to the same or greater security requirements to which the plan is bound.
- Have a contractual agreement with participants for security monitoring and annual security audits of their BAs.
- Establish clear policies, procedures, guidelines, and approaches governing patient consent.
- Develop policies and procedures for reporting patient requests to amend or correct healthcare records for their provider participants' process
- Translate new ARRA/HIPAA privacy requirements into consistent processes and practices across healthcare stakeholders who are involved in the flow of health information through HIEs.
  - Identify and reconcile the disparities between applicable state requirements for privacy and security and use to create baseline policies and procedures.
  - Collect, analyze, and harmonize state regulations pertaining to the collection and use of data for population health to allow for cross-state collection, cooperation, and reporting. This effort could be designed similar to the multi-state work that has already taken place through the Health Information Security and Privacy Collaboration (HISPC) projects.
- Ensure that their policies, logging processes, and practices allow patients to receive an accounting of disclosures when requested.
- Work with Healthcare Information and Management Systems Society *(*HIMSS), American Health Information Management Association (AHIMA), and other related groups for assistance with interpreting requirements and drafting privacy policies.[37]

---

[37]Several interesting reports and commentaries on drafting privacy policies can be found online, for example:
Eric Goldman, Esq and Cooley Godward, LLP, NITA. *Drafting a Privacy Policy? Beware!* Retrieved from www.ntia.doc.gov/ntiahome/privacy/files/9PK02!.HTM on February 1, 2011.
Barbara Demster MS, RHIA, CHCQM and Gary L. Kurtz, CHPS, FHIMSS. HIMSS. *Managing Information Privacy & Security in Healthcare Business Associates.*Retrieved from www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D27_Business_Associates.pdf on February 1, 2011.
Thomas Grove and Barbara Demster, MS, RHIA, CHCQM. AHIMA. Managing Information Privacy & Security in Healthcare Administrative Requirements for Privacy. Retrieved from www.himss.org/content/files/CPRIToolkit/version6/v7/D73_Admin_Requirements.pdf on February 1, 2011.
HRSA. What are the policies and procedures that we need to have in place? Retrieved from www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/OpportunitiesCollaboration/policiesprocedures.html on February 1, 2011.
AHIMA. The State-Level Health Information Exchange Consensus Project *HIE Policies and Practices: Developing Options and Implementation Guidance To Foster Consistency,* Interim Report , Version 1.0, August 15, 2008. Retrieved from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045662.pdfon February 1, 2011.
Adele A. Waller, JD. AHIMA. Getting Information Rights Right: Identifying the Rights-related Issues in Health Information Exchange. retrieved from

- HIOs should take responsibility for establishing metrics and best practices regarding acceptable levels of data quality in the EMPI/MPI.
- Develop correction and amendment procedures for correcting/amending patient data that incorporate a cross-community chain of custody for revisions to records.
- Develop procedures that clearly describe how the confidentiality, integrity, and availability of records will be preserved.
- Implement a policy requiring that PHI be de-identified before being disclosed to third parties. Have a policy that clearly states that third parties accessing PHI from the HIE may only use the PHI for the purpose specified in the business associate agreement.
- Establish and enforce requirements for security standards compliance for participation in the HIE. This should include regular security risk assessments for providers and the HIO to monitor processes and assure ongoing compliance and/or remediation.
- Establish frequent auditing practices and mechanisms for identification of breaches and unauthorized access to data.
- Establish a process for breach notification that meets the ARRA requirement.
- HIOs should conduct a rigorous risk assessment and mitigate those items which are found to be out of compliance. Identified actionable items must be fixed utilizing best efforts in applying reasonable and appropriate safeguards to reduce the likelihood of a security incidence.
- Establish a risk assessment intake evaluation questionnaire to be included in the HIO/HIE initiative participants' application process. Include in the Participation/Data Sharing Agreement, as a term of participation, a requirement of review of documentation of the most recent risk assessment, and supporting policies and procedures.
- HIO/HIE initiative participants should also provide documentation of all resolved actionable items or a declaration that identified threats and/or vulnerabilities can be managed at a reasonable and appropriate level.
- Establish oversight responsibility for HIE technical and physical security.
- Include technology, interface protocols with version, and a data set inventory used by entities participating in an HIO/HIE initiative as part of the readiness assessment conducted during the implementation planning.
- Establish minimum physical and environmental security standards.

---

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_032269.hcsp?dDocName=bok1_032269 on February 1, 2011.

- Access Control roadmap should provide full guidance from start-up to multi-factor authentication.
  - The HIO/HIE initiative's technical standards should include technical specifications for all protocols and equipment. All testing requirements and expected results should be published with the specifications.
  - Agree to the appropriate level of authentication for the HIE (two-level or multi-factor). Develop a plan of action to achieve the proposed level of authentication. Build the requirement into the HIO/HIE initiative participant contracts as a participant obligation.

Education

HIOs should:

- Develop an HIE HIPAA Privacy policy for consumers to review, outlining the obligations with which HIO/HIE initiative participants and providers are required to comply.
- Develop consumer education relating to "Opt-in and "Opt-out" methods of specifying consent and data sharing preferences.
- Develop education for providers to familiarize them with the best technical practices regarding information exchange and relevant agreements.
- Design and implement appropriate and ongoing education programs to provide HIO/HIE initiative participants with knowledge about good security practices that include:
  - The regulatory landscape in which their use of HIE-based patient data resides (such as state sharing principles and protected data classes);
  - How to appropriately utilize deployed technologies (such as single sign-on and biometric or token-based identification and authorization); and
  - Expected appropriate behaviors and consequences of misfeasance or malfeasance as a consumer of HIE patient data.
- Training should meet the requirements of the HIO/HIE initiatives Administrative Security policies.

ACKNOWLEDGEMENTS

Work Group Co-Chairs

Stacie Durkin, RN-C, MBA, RHIA

Christopher Sullivan, PhD

White Paper Contributors

Barbara Demster, MS, RHIA, CHCQM

Shari Donley, MBA, CPHIMS

Stacie Durkin, RN-C, MBA, RHIA

Reginald Grady, RHIT

Judi Hofman

Dave Kirby

Laura Kolkman, RN, MS, BSN, FHIMSS

Kristopher Kusche, CISSP, CPHIMS, FHIMSS

Chrisann Lemery, MS, RHIA

Jon Melling

Dave Minch, BA, FHIMSS

Greer W. P. Stevenson, MPH, MBA, CISSP, PhD

Christopher Sullivan, PhD

Work Group Participants

Glen Allen

John Avedian

Bill Braithwaite

Kelli Bravo

Julie Burgoon, PMP, CPHIMS

Jonathan Coleman, CISSP, CISM, CBRP

Patrick Curley

Lois Dahl, CHS

Jennifer Daniels

Patricia Dodgen, CPHIMS

Solomon Eboigbodin, MBA, RHIA

Karen Fairchild

Cathy Flite, MEd, RHIA

Amy Gasbarro, BHA, MHA

Alan Goldberg, JD, LLM

Catherine Gorman-Klug, RN, MSN

Peter Grant, JD, PhD

Betsy Gross

Robert Harper, PMP

Steve Hufman

Jeff Kerber

Vik Kheterpal, MD

Becky Learn, RN

Vicki MacDonald, RHIA

Patricia MacTaggart

Montra May, MBA

Richard Moore

Feisal Nanji, CISSP

Alison Nicklas, RHIA

Michele O'Connor, RHIA, FAHIMA

Peter Paulli

Erik Pupo, MBA, CPHIMS

Renea Quinn

April Robertson, MPA, RHIA, FAHIMA

Erik Rolf, CISA, CISSP

Karen Salmon

Leslie Scarborough, RHIA

Peter Schmidt

Erik Thieme, JD

Andrea Thomas-Lloyd

Brad Tritle, CPHIT

MJ White, MS, RHIA, NHA, CPHQ

Mariann Yeager, MBA

Stephen Young, RHIA

AHIMA Staff

Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA, Director Practice Leadership

HIMSS Staff

Lisa A. Gallagher, BSEE, CISM, CPHIMS, Senior Director, Privacy and Security

Pam Matthews, RN, MBA, CPHIMS, FHIMSS, Senior Director, Regional Affairs

Mike Kroll, Associate Manager, Informatics