HIE Management and Operational Considerations

Save to myBoK

Editor's note: This update supplants the November-December 2006 practice brief "Privacy and Security in Health Information Exchange".

The primary function of a health information exchange (HIE) is to permit access to clinical information on demand at the point of care. HIEs enable health information to be exchanged electronically between disparate healthcare information systems while ensuring information integrity. HIEs may also provide a structure for purposes like public health reporting, clinical quality measurements, biomedical surveillance, and consumer health informatics research.[1]

A successful HIE depends on trust between the patient, the healthcare provider, and the HIE. In order to build trust, HIEs must develop and implement policies and procedures guiding their operations, including how they will maintain and secure protected health information (PHI).

This practice brief identifies the policies, procedures, and best practices essential for successful HIE management and operations. It serves as a resource and reference guide for HIM professionals and subject matter experts involved with HIEs. (Appendix A provides a glossary of terms commonly used in HIEs.)

Federal Rules and Regulations That Affect HIE

Many federal laws and regulations govern the exchange of PHI. The Privacy Act of 1974, HIPAA, and the HITECH Act all include provisions to safeguard the confidentiality and integrity of PHI. HIEs must review every federal law and regulation that affects their operations to ensure compliance.

The HITECH Act expands the current federal protections for the privacy and security of PHI under HIPAA.[2] It requires business associates comply with HIPAA, an obligation that originally was restricted to covered entities. It also extends business associate status to HIEs and authorizes state attorneys general to enforce HIPAA by initiating lawsuits on behalf of victims of security breaches.

Other federal laws and regulations that affect the exchange of health information include the Medicare Conditions of Participation, the federal regulations regarding Confidentiality of Alcohol and Drug Abuse Patient Records, the Family Educational Rights and Privacy Act, the Gramm-Leach-Bliley Act, and the Food, Drug, and Cosmetic Act.

There should be few conflicts among these laws; however, when state laws do conflict with federal laws, pre-emption applies. HIEs must consult with legal counsel to ensure appropriate compliance is met.

Resolving State Laws That Affect HIE

Many states have enacted their own, more stringent laws to govern and manage the privacy and security of PHI. As with the federal rules and regulations, HIEs must review state laws to ensure compliance across networks and states (when applicable) for compliant HIE operations.

HIEs must take into account state laws pre-empting federal laws when two similar state and federal laws coincide. They should consult legal counsel for guidance on these matters. Resolving these differences will ensure information and data sharing, especially in times of public health emergencies.

The federal government is also working with state governments to help enable efficient HIE management and operations. For example, the Office of the National Coordinator for Health IT (ONC) has launched the State Health Information Exchange Cooperative Agreement Program to work with states to advance interoperability and health information exchange through a variety of activities, including:

- Collaborating with states and state-designated entities to promote, monitor, and share efficient, scalable, and sustainable mechanisms for HIE within and across states
- Helping coordinate and share information regarding federal health IT investments and programs across agencies (e.g., Centers for Disease Control and Prevention, Centers for Medicare and Medicaid Services, Agency for Healthcare Research and Quality, and non-HHS federal agencies)
- Conducting a national program evaluation and offering technical assistance for state-level evaluations
- Adopting standards and certification criteria to enable interoperability and HIE
- Providing technical assistance to states and state-designated entities
- Coordinating information sharing across states
- Advancing standards-based HIEs through Nationwide Health Information Network standards, services, and policies[3]

HIE Operations across Different States

In a multistate exchange, the technology available may not easily support variations in state laws and may require manual intervention. For example, an HIE operating in state A may need to respond differently to requests for information than an HIE operating in state B, depending on the laws of the two states. More specifically, HIV or mental health data may need to be suppressed to comply with the law of state A, but in the case of state B, full disclosure may be provided.

In states that require suppression of specific clinical information, HIEs must decide if or when to include a notice to clinicians that certain types of data have been redacted and that the information provided may be incomplete.[†]

HIE Guidance for Patient Rights

The HIPAA privacy rule affords patients specific individual rights to the uses and disclosures of their PHI. HIEs must clearly communicate these rights and their significance to patients participating in the HIE. Successful communication of patient rights is essential and demonstrates strong organizational commitment to build trust and gain consumer confidence.

ONC's "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information" outlines principles that, when taken together, constitute good data stewardship and form a foundation of public trust in the collection, access, use, and disclosure of personal information by HIEs. To complement the framework, the Office for Civil Rights (OCR) published a series of fact sheets that clarify how the HIPAA privacy rule applies to and can be used to help structure privacy policies behind electronic HIE.

ONC's framework and OCR's fact sheets call for the following principles in an HIE:

Individual Access: HIEs should provide consumers with a "simple and timely means to access and obtain their individually identifiable health information in a readable form and format," according to ONC's framework.[4] OCR's guidance further states, "An individual's right to access his or her PHI is a critical aspect of the Privacy Rule, the application of which naturally extends to an electronic environment. The Privacy Rule's specific standards address individuals' requests for access and timely action by the covered entity, including the provision of access, denial of access, and documentation."

Correction: HIEs should provide patients "a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied."[6] OCR notes the privacy rule provides individuals with the "right to have their protected health information (PHI) amended in a manner that is fully consistent" with the framework.[7]

Openness and Transparency: Policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information should be open and transparent, according to ONC and OCR. Entities that participate in HIEs should provide "clear notice of their policies and procedures regarding how an individual's identifiable health information" is protected, used, and disclosed.[8]

Individual Choice: HIEs should provide individuals with "a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information."[9] (This is commonly referred to as

the individual's right to consent to identifiable health information exchange.) OCR further notes the framework "emphasizes the opportunity and ability of an individual to make choices with respect to the electronic exchange of their individually identifiable health information."[10]

Collection, Use, and Disclosure Limitation: "Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose."[11] OCR notes that the framework "emphasized that appropriate limits should be set on the type and amount of information collected, used, and disclosed, and that authorized persons and entities should only collect, use, and disclose information necessary to accomplish a specified purpose."[12]

Safeguards: "Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards (HIPAA security rule) to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure."[13] OCR notes that the HIPAA privacy rule "supports the Safeguards Principle by requiring covered entities to implement appropriate safeguards to protect the privacy of protected health information (PHI)."[14]

HIE Governance Policies and Procedures

Policies and procedures govern the operations of the HIE, and many factors must be taken into consideration during their development or revision. For example, the HIPAA privacy and security rules require PHI be accessible to patients; maintained in a manner that secures patient privacy, security, and data integrity; and released in accordance with state and federal laws. Appendix B outlines the areas that must be taken into account when establishing policies and procedures for HIE operations.

The policies and procedures also set expectations for the workforce. Training and accountability for the workforce members must be clearly delineated. Access to all available resources (including policies and procedures) must be part of an ongoing education and compliance program, which must be enforced by management.

HIE Contracts

HIEs typically contract with vendors for the technology they use to exchange health information. According to Randall E. Sermons, an attorney with HIE experience, when contracting with technology vendors, HIEs must consider how the technology is delivered, the licensing required to use the technology, and the technology's ability to protect data. Unique liability concerns within HIEs, such as liability for technology malfunctions and vicarious liability for acts of a data participant, must also be taken into consideration.

Contracts are complex in single-vendor solutions or software as a service (SaaS); in-house and custom solutions also require tight coordination and alignment of contractual provisions.[15] The complexity comes from a combination of the number of issues that must be addressed (e.g., privacy and security concerns, technology issues, legal issues, and the interplay of oversight committees and the reliance upon policies that may be amended outside the traditional contracting amendment process), coupled with coordinating all of these issues across multiple contractual relationships.

HIEs must also contract with each of the data participants in the HIE. Data participant agreements pose unusual challenges, according to Sermons. "For many regions of the country the concept of health information exchange is still new and the legal issues are not always clear or well defined," he says. He recommends HIEs develop educational processes for provider attorneys and privacy and security officers to ensure they learn the basic concepts and are able to identify liability and privacy and security concerns.

"Data participant agreements should address currently planned exchange operations and be flexible enough to accommodate changes or additional services," Sermons says. HIEs should also consider state-level models, cross-border exchanges, and the Nationwide Health Information Network when developing data participant agreements.[16]

Sermons recommends HIEs employ well-educated legal counsel to help develop a contracting plan for both vendors and data participants to ensure a cohesive approach to meeting the needs of both the HIE and its contracting partners.

Role of the HIM Professional in HIEs

HIM professionals play a key role in managing many of the legal and operational issues in the electronic, paper, and hybrid health record environments. As local, regional, and national HIE networks develop and as state and federal laws evolve, it is important that HIM professionals keep abreast of related privacy and security issues and of ever-changing regulatory, policy, and information standards for patient records. HIM professionals must remain vigilant in ensuring that HIEs have strong confidentiality and security foundations as electronic information is exchanged across communities.

HIM professionals possess the knowledge and skills that add value to the effective planning and implementation of an HIE while ensuring compliance with the HIPAA privacy and security rules. HIM professionals bring the following skill set to HIEs:

- An understanding of federal and state law and accreditation standards as they relate to confidentiality and privacy of PHI in all formats
- Expertise in determining permissible and impermissible electronic disclosures
- Expertise in defining appropriate access to PHI based on the needs of the patient, providers, and other members of the workforce and on federal and state laws and regulations
- Knowledge of the status of the organization's compliance with the privacy rule
- Expertise and experience in developing policies, procedures, standards, and guidelines
- Expertise and experience in the design of audit processes and programs
- Expertise in local, state, and federal public health disease reporting and surveillance requirements
- Expertise in the management of health information and disclosures during disaster and public health emergencies

In order to achieve successful implementation and sustainability, HIEs must establish and maintain a collaborative relationship between clinical and administrative stakeholders, including subject matter experts from areas such as privacy, security, HIM, information technology, compliance, and legal counsel.

Keys to Success

The success of an HIE is made up of multiple components. Once policies and procedures are in place, laws and regulations are understood, contracts are developed, and expectations are set, HIEs must address other factors that come into play to help ensure success. The participant's keys to a successful HIE operation include building trust, establishing responsibility, monitoring and managing operations for compliance, and enforcing privacy and security protections.

The relationship between the patient and his or her healthcare provider is the foundation for trust in health information exchange. Building trust also requires the HIE:

- Meet patients' needs and consider all reasonable expectations regarding the accurate, appropriate, secure, and confidential exchange of their health information.
- Educate patients on the purposes for the use and disclosure of their health information and allow patients to control use and disclosure wherever possible. Patients should not be surprised about or harmed by collections, uses, or disclosures of their data. A patient must feel his or her information is safeguarded from misuse and disclosed only when appropriate.[†]
- Provide accurate, pertinent information that is accessible and available when needed. Otherwise, providers will find the HIE unreliable and distrust the accuracy and integrity of the information maintained within the HIE.

In addition providers must be able to trust that all entities utilizing and accessing data are doing so in accordance with purposes outlined in the participation agreement.

HIEs must also establish responsibility within the HIE network. Establishing responsibility within the HIE requires providers be responsible for maintaining the privacy and security of their patients' records. Patients also must be fully informed about and accept the terms and policies of the HIE.

Monitoring and managing operations for compliance is another key to HIE sustainability. In order to monitor and manage operations for compliance, HIEs must:

- Develop a strong process to monitor performance. Key processes requiring ongoing review include compliance with regulations such as reporting and mitigating breaches.
- Establish well-documented policies and procedures and enforce a compliance program to promote confidence and trust between the patient, the healthcare provider, and the overall HIE process.

In order for HIEs to be effective, they must enforce privacy and security protections within the network. Enforcing these protections requires the HIE and covered entities agree on the policies and procedures that govern the privacy and security of all individually identifiable health information, regardless of the medium used to capture, store, transmit, and dispose of the information.

Notes

1. AHIMA. "Understanding the HIE Landscape." *Journal of AHIMA* 81, no. 9 (Sept. 2010): 60?65. Available online in the AHIMA Body of Knowledge at www.ahima.org.
2. US Department of Health and Human Services. "HHS Strengthens Health Information Privacy and Security through New Rules." Press release. July 8, 2010. www.hhs.gov/news/press/2010pres/07/20100708c.html.
3. US Department of Health and Human Services (HHS), Office of the National Coordinator for Health IT (ONC), State Health Information Exchange Program. "Program Information Notice." Document Number: ONC-HIE-PIN-001. July 6, 2010. http://statehieresources.org/grantee-3/pin.
4. HHS, ONC. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information." December 15, 2008. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173
5. OCR. "The HIPAA Privacy Rule's Right of Access and Health Information Technology." www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf.
6. HHS, ONC. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information."
7. OCR. "Correction." www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/correction.pdf.
8. OCR. "Openness and Transparency." www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/opennesstransparency.pdf.
9. HHS, ONC. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information."
10. OCR. "Individual Choice." www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf.
11. HHS, ONC. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information."
12. OCR. "Collection, Use, and Disclosure Limitation." www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/collectionusedisclosure.pdf.
13. HHS, ONC. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information."
14. OCR. "Safeguards." www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf.
15. Randall E. Sermons, attorney at law. Personal communication. February 7, 2011.
16. Ibid.

References and Resources

AHIMA. "Health Information Exchange." www.ahima.org/resources/hie.aspx.

AHIMA. HIPAA in Practice: *The Health Information Manager's Perspective*. Chicago, IL: AHIMA, 2004.

AHIMA and the American Medical Informatics Association. "Statement on Health Information Confidentiality." *Journal of AHIMA* 77, no. 10 (Nov.-Dec. 2006): 22. Available online in the AHIMA Body of Knowledge at www.ahima.org.

AHIMA e-HIM Workgroup on HIM in Health Information Exchange. "HIM Principles in Health Information Exchange." *Journal of AHIMA* 78, no. 8 (Sept. 2007): online version. Available online in the AHIMA Body of Knowledge at www.ahima.org.

AHIMA e-HIM Work Group on EHR Data Content. "Guidelines for Developing a Data Dictionary." *Journal of AHIMA* 77, no. 2 (Feb. 2006): 64A?D. Available online in the AHIMA Body of Knowledge at www.ahima.org.

AHIMA e-HIM Work Group on Patient Identification in RHIOs. "Surveying the RHIO Landscape: A Description of Current RHIO Models with a Focus on Patient Identification." *Journal of AHIMA* 77, no. 1 (Jan. 2006): 64A?D. Available online in the AHIMA Body of Knowledge at www.ahima.org.

Carter, Patricia, et al. "Privacy and Security in Health Information Exchange." *Journal of AHIMA* 77, no. 10 (Nov.-Dec. 2006): 64A?C. Available online in the AHIMA Body of Knowledge at www.ahima.org.

Connecting for Health. "Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy." February 2005. www.markle.org/sites/default/files/linking_report_2_2005.pdf.

Electronic Healthcare Network Accreditation Commission. "Health Information Exchange Accreditation Program." www.ehnac.org/accreditation-programs/hieap-accreditation.html.

Gallagher, Lisa. "Tiger Team Provides Its Initial Privacy Policy Recommendations." August 23, 2010. HIMSS Blog. http://blog.himss.org/2010/08/23/tiger-team-provides-its-initial-privacy-policy-recommendations.

Healthcare Information Technology Standards Panel. "HITSP Glossary." Version 1.2. September 26, 2008. http://publicaa.ansi.org/sites/apdl/hitspadmin/Reference%20Documents/HITSP%20Glossary.pdf.

Johns, Merida L. *Information Management of Health Professions*. Albany, NY: Delmar Publishers, 1997.

Latour, Kathleen M., and Shirley Eichenwald. *Health Information Management: Concepts, Principles, and Practices*. Chicago: AHIMA, 2002.

NHIN Cooperative DURSA Workgroup. "Draft Data Use and Reciprocal Support Agreement (DURSA)." January 23, 2009. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_849891_0_0_18/DRAFT%20NHIN%20Trial%20Implementations%20Production%20DURSA-3.pdf.

Office of the National Coordinator for Health Information Technology (ONC). http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__onc/1200.

ONC. "Nationwide Health Information Network (NHIN): Overview." December 17, 2010. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__nhin/1142.

ONC. "ONC Commissioned Medical Identity Theft Assessment." September 11, 2009. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__medical_identity_theft/1177.

ONC. "Privacy and Security." January 19, 2011. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147.

Sinay, Sandy. "Managing Information Privacy & Security in Healthcare Accounting of Disclosures of Protected Health Information." HIMSS Privacy and Security Toolkit. www.himss.org/content/files/CPRIToolkit/version6/v7/D25_Accounting_of_Disclosures.pdf.

State Alliance for eHealth. www.nga.org/portal/site/nga/menuitem.1f41d49be2d3d33eacdcbeeb501010a0/?vgnextoid=5066b5bd2b991110VgnVCM1000001a01010aRCRD.

US Department of Health and Human Services (HHS). "Health Information Technology." www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit.

HHS. "Summary of the HIPAA Privacy Rule." www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.

HHS, Office of the National Coordinator for Health IT. "Consumer Preferences Draft Requirements Document." October 5, 2009. http://healthit.hhs.gov/portal/server.pt?open=512&objID=1202&PageID=16769&mode=2.

Appendix A: Glossary of Terms

Authorized testing and certification bodies (ATCBs): six organizations authorized by the Office of the National Coordinator for Health IT to test and certify complete EHRs and/or EHR modules to the certification criteria in the EHR standards and certification criteria final rule.[1] These organizations have been selected to verify that an EHR meets minimum requirements including those for security. Certification by an ATCB will signify to eligible professionals, hospitals, and critical access hospitals that an EHR technology has the capabilities necessary to support their efforts to meet the goals and objectives of the meaningful use program.

Consent model: the method the HIE uses to enlist and enroll patients into a health information exchange. Several consent models are available for use by HIEs:

- **No consent**—patient health information is automatically included?patients cannot opt out
- **Opt-out**—patient health information is included automatically, but patients can opt out completely
- **Opt-out with exceptions**—patient health information is included, but patients can opt out completely or allow only select data to be included
- **Opt-in**—no patient health information is included; patients must actively express consent to be included, but if they do so then their information must be all in or all out
- **Opt-in with restrictions**—no patient health information is made available, but patients may allow a subset of select data to be included

Data use and reciprocal support agreement (DURSA): a comprehensive, multiparty trust agreement that signed by all HIEs, both public and private, wishing to participate in the Nationwide Health Information Network (NHIN). The DURSA provides the legal framework governing participation in the NHIN and requires the signatories abide by a common set of terms and conditions. These common terms and conditions support the secure, interoperable exchange of health data between and among numerous HIEs across the country.

Electronic Healthcare Network Accreditation Commission (EHNAC): a federally-recognized standards development organization accrediting body. EHNAC offers the Health Information Exchange Accreditation Program (HIEAP), which assesses readiness for meeting privacy and security criteria.[2]

Health information exchange (HIE): a plan in which health information is shared among providers. HIE refers to the process of reliable and interoperable electronic health-related information sharing conducted in a manner that protects the confidentiality, privacy, and security of the information.[3] The electronic mobilization of healthcare information across organizations, communities, or regions.[4]

A multitude of terms are currently used to describe a networked community of healthcare entities using interoperable electronic health record systems to exchange health information. These include health information exchange (HIE), the Nationwide Health Information Network (NHIN), and at one time, community health information network (CHIN). For this practice brief, the term *HIE* is used.

Health information exchange models: the infrastructure for the exchange of information among various organizations. There are several different HIE models available:

Federated Models

- **Shared repositories**—This model uses a seriesof networks connected through the Internet. Participants submit data to a regional repository responsible for patient identification, storage, system management, security, and privacy. The regional repositories are interconnected.
- **Peer-to-peer network**—This model employs a peer-to-peer network of participant networks connected through the Internet. Participants maintain their own health information network with no centralized repositories. A national or regional entity maintains a master patient index for the HIE. Using this index, participants can obtain patient data from the other individual participant networks. This can be done peer to peer by direct communication to the participant holding the data or through a national or regional entity that manages the index as an intermediary.

Nonfederated Models

- **Peer-to-peer network (co-op model)**—This approach uses a peer-to-peer network of participant networks connected through the Internet. The network may be smaller and more community based (e.g., a hospital system and affiliated clinics with point-to-point communication). Participants maintain their own health information network, and there is no centralized repository. All communications are direct from participant to participant.
- **Centralized database or data warehouse**—This approach employs a regional centralized repository of health information accessed through the Internet. A database or data warehouse may be a component or building block of other models. Storage, system management, patient identification, security, and privacy are all managed and controlled at a central HIE site. Participants submit data to and request data from this central site.

Hybrid: any variation or combination of the above.

Health Record Bank: an electronic repository developed to collect,store, and distribute a patient's health record.[5]

Health information organization (HIO): "an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards."[6].

National Institute of Standards and Technology: a government agency that develops information security tools and standards to improve information security. The standards and practice tools created by its Computer Security Division are available at http://csrc.nist.gov.

Nationwide Health Information Network: the building blocks or foundation for interoperability; the physical and national network components that make EHRs interoperable.

Appendix A Notes

1. Office of the National Coordinator for Health IT. "ONC-Authorized Testing and Certification Bodies." December 28, 2010. http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3120.
2. Electronic Healthcare Network Accreditation Commission. "Health Information Exchange Accreditation Program." www.ehnac.org/accreditation-programs/hieap-accreditation.html.
3. AHIMA. "Health Information Exchange." www.ahima.org/resources/hie.aspx.
4. Centers for Medicare and Medicaid Services, Office for Civil Rights. "Collection Use and Disclosure Limitation." The HIPAA Privacy Rule in Electronic Health Information Exchange in a Networked Environment. www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/collectionusedisclosure.pdf.
5. Dimick, Chris. "Taking Medical Records to the Bank." *Journal of AHIMA* 79, no. 5 (May 2008): 24?29. Available online in the AHIMA Body of Knowledge at www.ahima.org.
6. National Alliance for Health Information Technology. "Defining Key Health Information Technology Terms." April 28, 2008. www.hhs.gov/healthit/documents/m20080603/10_2_hit_terms.pdf.

Appendix B: HIE Policy and Procedure Considerations

HIEs should consider the following subject areas and issues when developing and implementing their policies and procedures.

Access Control

Organizations must determine who requires access to the information shared within the HIE and establish policies and procedures for managing authentication and auditing use.[†] Healthcare decisions may be made based on information from the exchange, so organizations in the HIE may need to review and redefine their designated record sets accordingly.

HIEs should address the following access management issues in their policies and procedures:

- Identify who is responsible for overall access management (e.g., who approves authentication, assigns access, adds/deletes staff, tracks access)
- Define patient access procedures
- Identify authorized users, including the process for user authorization and the types and levels of access (e.g., read-only, role-based) in keeping with minimum necessary standards
- Implement a formal user agreement and policy regarding user IDs and password management
- Define the criteria (if any) for termination of access or sanctions for improper use or data violations

Access audit considerations for HIE policies and procedures include:

- Identify oversight for review and management of audit results
- Determine how often audits will be performed and by what method(s)
- Identify to whom and what method audit results will be communicated and how
- Review audit reports for content and evaluating reports for a human-readable format and potential integration with a report writer system
- Design process to detect alterations of audit logs
- Create an audit trail retention schedule

HIEs should also review their business associate agreements, including language and signatories, when developing and implementing their policies and procedures for access control. In addition, they should outline the procedures for handling sensitive patients, records, and information (e.g., mental health, drug and alcohol, HIV, high profile/celebrity status, genetic information, etc.). Access controls and functionality (e.g., granular or "break-the-glass") should also be reviewed.

Accounting of Disclosures

Under HIPAA's accounting of disclosures requirements, a patient may request a record of the entities to which their PHI has been disclosed. ARRA further contains specific requirements pertaining to accounting of disclosures.

HIEs must define and outline policies and processes for the appropriate disclosure of health information. The policy should address under what circumstances information can be released, by whom, and who will maintain the accounting of disclosures report. It is important to determine if there will be one consolidated report or a report provided from each participating organization. Is the HIE simply a broker of the information with the expectation that the patient will go to each of their participating healthcare providers to obtain an accounting of disclosures?

HIEs should consider the following steps when developing their accounting of disclosures policies and procedures:[†]

- Outline the processes for accounting of disclosures, including who will manage requests
- Identify who will maintain the accounting of disclosure (e.g., individual provider organizations or HIE)
- Determine the report format for requests (e.g., whether one consolidated report or individual reports from each provider organization)
- Establish acceptable time frames to complete accountings of disclosures

Breach Notification

HIEs must develop policies that ensure high levels of privacy and security of personal health information and outline responsibilities for breach notification. These policies should address the breach notification process, who shall conduct such notifications and by what means, the role of the HIE versus the individual participating partners in breach notifications, and the penalties for breaches.[†] HIEs must ensure compliance with HIPAA privacy and security rules as well as all applicable state and federal laws.

An HIE's policy regarding the standard for breach notifications should:

- Establish the HIE's and participating organization's responsibilities
- Outline indemnification provisions
- Establish a timeline for breach notifications
- Include state and federal requirements for breach notifications
- Delineate the content for breach notifications
- Define the method for individual notification
- Outline the response time to potential breach investigations
- Define the process for breach notification when the HIE is subject to laws from multiple states

An HIE's sanctions for breach notifications should:

- Distinguish between reasonable cause, reasonable diligence, and willful neglect
- Establish criteria for data breaches, inappropriate access, and/or use and disclosure of information by authorized users
- Define what sanctions apply and when
- Outline how the sanctions will be applied consistently across the HIE
- Determine the conditions under which participants will be expelled from the HIE

Consent/Authorization Process

The patient consent model the HIE chooses is not a simple decision and can be made at various points in the process. The HIE's HIPAA state pre-emption analysis, particularly as it relates to authorization, may determine whether it implements an opt-in or opt-out approach.

Consumer education is a critical piece regardless of which consent model is adopted. Patients must understand their rights and responsibilities and clearly understand the potential ramifications of including or excluding all or portions of their health information.

HIEs must consider the following consent/authorization issues:

- Determine opt-in or opt-out model, hybrid model, or combination of both opt-in and opt-out
- Define the role of the state, if any, in approving the consent model
- Decide what restriction requests will be approved, including technical considerations and restriction management at the HIE versus the individual provider level
- Determine if and what types of authorization form(s) are required, if any (e.g., whether one form will be developed by the HIE for providers to give to patients or whether each participating partner will develop its own)
- Determine where authorizations are going to be stored and relevant retention periods
- Establish validation processes for authorizations for disclosure
- Develop break-the-glass policy/scenarios, including whether break-the-glass functionality is permitted and whether these policies must be consistent across participants or whether such criteria may be locally defined, and the criteria and process for implementing, reviewing, and acting upon break-the-glass events

- Develop a process for handling revocation of authorization (e.g., how to proceed when a patient rescinds his/her previous authorization to disclose his/her health information), as well as who should receive, approve, and/or process such requests

Consumer Education

Consumer trust in the HIE's ability to protect the privacy and security of patient information will be key to the HIE's success, and consumer communication will play an important role in gaining that trust. HIM professionals may be instrumental in developing and executing public awareness campaigns that educate consumers on the quality of care benefits of using interoperable health IT and the benefits that can be realized without sacrificing the privacy and security of their information.

HIEs must outline the following consumer education issues in their policies and procedures:

Develop community outreach efforts

- Design patient education that outlines what information is being shared, to whom, and for what purpose; the patient's rights, including access, restriction requests, and amendment requests; the implications on patient care; the purpose of use; the enrollment process; consumer preferences; and breach notification processes
- Outline notice of privacy practices (NPP) to ensure that the covered entities' relationships with other organizations to exchange information is reflected accurately, including participation and exchange of health data
- Develop a policy for distributing and tracking compliance with the NPP requirement

Data Integrity and Quality

HIEs must develop a policy to ensure high levels of data integrity for which the HIE and participating organizations are responsible.

It is imperative that organizations exchanging health data take responsibility for the quality of the data they make available to the HIE. The originating organizations or data participants must establish rules addressing data characteristics including data definition, timeliness, accuracy, relevancy, consistency, accessibility, granularity, precision, currency, and comprehensiveness.[†]

The HIE must adopt data content standards and definitions to maintain data integrity and quality. A key component of achieving this includes developing a data dictionary, a topic discussed in the practice brief "Guidelines for Developing a Data Dictionary." The integrity of the data in the HIE will be compromised if participating organizations do not consider data characteristics.

HIEs should consider the following data integrity issues when developing their policies and procedures:

- Define data sources and related management processes
- Define procedures to ensure accurate verification of the patient for mapping purposes
- Define processes to identify and manage duplicates, including breaking records apart that have been incorrectly linked
- Standardize data between participating partners
- Ensure common interpretation
- Determine who is responsible/liable for the accuracy of the data provided by participating partners
- Outline the method to detect alteration in content
- Establish procedures for handling data omissions (e.g., intentionally withheld due to patient preference or determined to be sensitive information)

- Define the error management protocol for data not accepted by the HIE system
- Determine the format in which the data will be viewable
- Evaluate the need for a data integrity workgroup

Data Loss Protection

HIEs must develop a policy to incorporate HIPAA administrative, physical, and technical safeguards. Security awareness and training, contingency planning with a focus on data back-up, disaster recovery, and an emergency mode operation plan should all be included in the policy.

HIEs should review the following data loss issues when developing their policies and procedures:

- Adopt technical standards
- Designate responsibility for security compliance
- Determine access points (e.g., Internet)
- Determine the method of communication (e.g,. point-to-point, intermediary)
- Identify the personnel responsibility for system maintenance
- Implement data back-up plan, restore, and archive procedures
- Provide security awareness and training
- Develop a contingency plan
- Design a disaster recovery/emergency management plan

Data Retention

HIEs must develop a policy to identify who owns what data and establishes record retention requirements.[†] A determination must be made regarding whether the HIE is simply providing access to a view into the health record maintained by the originating organization, or whether it will store key components of the record in some sort of repository or data warehouse.

The following data retention issues should be considered in the development of an HIE's policies and procedures:

- Establish data ownership
- Determine whether protected health information will be passed through or stored in the HIE
- Identify types of information to be stored on the HIE, including but not limited to PHI, patient correlation and demographics; authorized users, audit logs, and compliance documentation
- Set record retention schedule (where applicable)
- Outline purging and destruction processes and procedures
- Define variance in retention policies according to federal versus state regulations or organizational policy

Data Use/Disclosure

The privacy rule generally requires covered entities take reasonable steps to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. It also requires covered entities take reasonable steps to limit any requests for PHI to the minimum necessary when requesting such information from other covered entities.

Although the privacy rule does not require that the minimum necessary standard be applied to electronic health information exchanges for treatment purposes, covered entities engaging in electronic health information exchange can apply minimum necessary concepts to develop policies that limit the information they include and exchange, even for treatment purposes.

Doing so would be consistent with the Office for Civil Rights' collection, use, and disclosure limitation principle and may help foster increased trust in electronic health information exchange.

HIEs should consider the following data use and disclosure issues in their policies and procedures:[†]

- Develop data use agreements outlining responsibilities, obligations, and expectations of participating partners
- Define allowable purpose of use such as:

    - **Treatment:** The purpose of the HIE will determine what patient information needs to be collected, used, and disclosed. Purposes can vary, and the most commonly stated purposes, in alignment with the requirements of the Nationwide Health Information Network, are to improve the delivery of care to individual patients by increasing communication between patients and providers; coordinate multiple providers involved in an individual patient's care at the point of care; protect and recover a patient's critical health information in case of a disaster; and improve overall management of healthcare costs.[1] These goals are very patient centric. If the uses of the patient's PHI is restricted to only these uses, the decision on what information to collect and disclose is much easier, since a great deal of work has already been done to define the data needed for the purpose of continuing care. For example, the Healthcare Information Technology Standards Panel has defined the demographic and clinical information considered necessary for continuity of care, which summarize a patient's medical status for the purpose of information exchange. These elements include information regarding demographics, current problem lists, medications, and insurance status.[2]

      It may be noted that the use and disclosure of PHI for the purpose of treatment is permitted by the HIPAA privacy rule without specific patient consent, unless otherwise required by law, or required by covered entity policy. However, there are federal laws that constrain the inclusion of certain types of treatment records unless patients authorize the information to be included, such as psychotherapy notes or drug and alcohol treatment records. There may also be state-specific laws that must be considered, as well, usually for a type of test or a certain diagnosis. For a summary of state specific laws, read ONC's "Report on State Medical Record Access Laws"

    - **Public health uses**. Many HIEs envision using information for uses other than patient care. The most common such use is public health reporting. The Health IT Policy Committee's Privacy and Security Tiger Team cautions that such reporting by the HIE on behalf of a healthcare organization should be limited to the least amount of identifiable data necessary to meet the requirements of the law.[3] HIEs must determine who has the responsibility for public health reporting, the HIE or the organization. If the decision is made that the HIE is responsible for reporting this data, the HIE must also have the capability to provide an accounting of disclosures upon request by each facility involved. It is also important to define who will be responsible for monitoring any changes in public health reporting laws and regulations to ensure compliance.
    - **Healthcare operations uses.** Healthcare operations is another proposed use of the HIE and includes continuous improvement, best practices, outcomes analysis, business continuity, and physician performance measurement.[4] Some envision the HIE as being the source of traditional release of information services, such as releasing health records to the Social Security Administration for disability determinations.[5] Clearly, if an HIE can perform these services by aggregating and de-identifying the data, it may do so if the service is defined in the business associate agreement (BAA). However, if a limited data set or a fully identified data set is needed for these purposes, the complexity for both the contributing facilities and the HIE increases. Each additional activity must be analyzed for compliance with the privacy rule and defined in the BAAs. In addition, the minimum necessary must be determined, and standard disclosure protocols developed. If an HIE routinely releases information for a CE based on authorizations or subpoenas, the possibility of breaches due to inadequate training or inadvertent error greatly increases. If an HIE is considered by a plaintiff's attorneys as an alternate source of a more complete legal health record than individual facilities or clinics, the amount of

work for the HIE will also significantly increase. Any BAA and service agreements between the HIE and contributing covered entities seeking these additional services need careful crafting by legal counsel.

A covered entity may also consider using a patient safety organization (PSO) for such activities as quality of care review and patient safety monitoring as these organizations have liability protections for providers under federal law.

- **Research**. It is imperative that PHI for research purposes have a strong institutional review board (IRB) oversight for uses and disclosures. Processes including the appropriate de-identification of PHI and proper auditing procedures must also be defined and implemented to ensure compliance is met.

- Define a standard set of identification data that should be included in an exchange
- Define what would be considered minimally necessary for the purpose of use
- State whether the HIE will be disclosing PHI for uses other than treatment. If yes, the Notice of Privacy Practices should include:
  - To whom it will be disclosed
  - Who will manage the process
  - What is the authorization process
  - Will there be a charge
- Define what information requires special protection under applicable laws prior to disclosing any information to or through the HIE
- Outline the process for collection of, access to, and disclosure of identifiable data (allowances for or constraints against)
- Outline the uses and disclosures of de-identified information (provisions for or constraints against)
- State whether copies of information received through the HIE will be stored in the health record maintained by the participating partner organization
- State whether or not information received through the HIE will be re-released as part of the health record
- State whether Information will be released only from the originating source or whether the HIE will be in the business of release of information. Myriad state and federal laws require a thorough pre-emption analysis be conducted to determine release of information requirements. Once these issues are clarified and processes are established, it is also necessary to develop and implement HIE participation agreements outlining terms of the relationship and requirements of each party.
- Outline disclosure to third parties

Governance Board

An overarching HIE policy should be developed defining the purpose of the HIE, type of HIE model, type of data to be exchanged, and what uses are allowed. The policy should be based on the mission, vision, and values of the HIE. The HIE must comply with all applicable state and federal privacy and security rules and regulations. A data use and reciprocal support agreement (DURSA) should be established. Finally, technical requirements should be outlined that identify standards and interoperability requirement, and explore various solutions.

Since no standard governance model exists, healthcare organizations and physicians will have to develop an HIE governance model that works for their particular environment. The "State HIE Toolkit" (http://statehieresources.org/) offers a useful resource. Sponsored by ONC, the State HIE Program developed the toolkit to assist in the implementation and development of HIEs. It includes resources such as governance structures, infrastructure requirements, and sample policies and procedures.

HIEs should consider the following governance issues when developing their policies and procedures:

- Outline membership
- Develop roles and responsibilities
- Develop a charter, including whether a privacy/security committee will be formed, how membership is determined, and the nature of their charge(s)
- Designate the type of exchange model (e.g., centralized, federated, or hybrid model)
- Implement appropriate processes for organizational withdrawal from the HIE

Providers or health plans contributing data to or receiving data from the exchange should enter into a written agreement specifying the terms of the relationship and the roles, rights, and responsibilities of each party. In addition to operational issues relating to the exchange of information, these agreements will need to address matters such as HIPAA business associate provisions, protecting each participant's proprietary information and intellectual property rights, software licensing, insurance, indemnification, audit rights, and dispute resolution.

Identity Management/Patient Correlation

The adopted exchange model should have robust patient identification capabilities. The patient identification process raises at least two privacy concerns. First, whether the correct patient has been identified. If not, detailed patient information about the incorrect patient may be disclosed. Second, even if the correct patient is ultimately identified, does the identification process itself require disclosure of inappropriate or excessive amounts of patient demographic or health information? The search process should be designed as narrowly as possible to ensure identification of the correct patient record while exposing only the minimum amount of information necessary about other patients.[†]

Identity management issues to consider in HIE policies and procedures include:

- Define which patient traits will be used, how many traits must correspond for a successful patient match and what algorithms will be used
- Identify how imperfect patient matches will be determined and resolved
- Determine the process for resolving duplicate record entries
- Determine the process for detecting medical identify theft and outline responsibilities for notifying other users if it is suspected
- Determine the process for detecting and resolving changes to patient identity traits, such as name changes, demographic updates, etc.
- Outline resources, staffing, and responsibilities for handling manual interventions
- Define the data provider's responsibility to provide clean data and meet standards regarding patient identification, data elements, and their accuracy
- Outline remediation processes for instances when the provider data has issues

Record Amendments

The privacy rule provides individuals the right to have their PHI amended in a manner fully consistent with the correction principle in ONC's privacy and security framework. Both the privacy rule and the correction principle recognize that individuals have a critical stake in the accuracy of their individually identifiable health information and play an important role in ensuring the integrity of that data. Under the privacy rule, individuals have the right to have a covered entity amend their PHI in a designated record set, as defined in § 164.501, for as long as the entity maintains the records.

For these reasons, HIEs require policies and procedures for accepting and managing amendments to the records they exchange, including rules on alerting partners to amended information. In establishing these policies and procedures, HIEs

should:

- Define processes for the management of all amendment requests including who will accept the requests from patients and providers, make amendments for a patient, and determine acceptance or denial of an amendment and under what conditions
- Define refusal processes
- Identify notification procedures (e.g., who must know, who will notify)
- Define amendment management, including how original entry will be retained, retrieved on demand, and linked to the amendment

Sanctions

Under HIPAA sanctions for breaches of the rules must be applied consistently throughout the organization regardless of user role.

The sanctions issues HIEs should consider in their policies and procedures include:

- Develop a policy to reconcile the varying breach sanction rules that may exist at different institutions
- Develop a dispute resolution process to be implemented in the event that the victim of the breach is dissatisfied with the sanctions applied

Sensitive Data

Individual states have their own laws addressing privacy of sensitive PHI. A pre-emption analysis comparing the HIPAA privacy rule with pertinent state laws is necessary. Some states have laws regarding highly sensitive information such as HIV/AIDS, behavioral health, and genetic test results. This pre-emption analysis becomes increasingly complex as the number of states involved in HIE increases. The current lack of consistency of laws between states can be a barrier to HIE adoption unless multistate HIE initiatives can find ways to accommodate varying state laws.

HIEs should consider the following sensitive data issues in their policies and procedures:

- Identify state versus federal policy and variance in state policies when HIE crosses over state lines
- Define actions necessary if treatment occurs when a patient resides in one state but seeks care in another state and the legal implications
- Outline technical constraints of the HIE and if they comply with the federal regulations
- Define what data if any are considered sensitive and determine whether additional patient authorization is required for the exchange of sensitive data
- Determine whether or not the system is capable of suppressing sensitive data

Appendix B Notes

1. Finn, Zach, et al. "Aligning HIE: A Model to Organize Networks for Core Principles, Collaborative Activities." *Journal of AHIMA* 81, no. 8 (Aug. 2010): 50. Available online in the AHIMA Body of Knowledge.
2. Healthcare Information Technology Standards Panel. "C 32—HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component."
3. Health IT Policy Committee. Letter to David Blumenthal. August 19, 2010.
4. Finn, Zach, et al. "Aligning HIE: A Model to Organize Networks for Core Principles, Collaborative Activities."
5. AHIMA. "Understanding the HIE Landscape." *Journal of AHIMA* 81, no. 9 (Sept. 2010): 60—65. Available online in the AHIMA Body of Knowledge.

Prepared by

Susan Carey, RHIT, PMP
Angela K. Dinh, MHA, RHIA, CHPS
Julie Dooling, RHIT
Aviva Halpert, RHIA, MA, CHPS
Judi Hofman, CAP, CHP, CHSS
Tanya Kuehnast, MA, RHIA, CHPS
Harry Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA
Jennifer Teal, MS, RHIA, CPC
Mary Thomason, RHIA, CHPS, CISSP
Susan Torzewski, RHIA
Traci Waugh, RHIA

Acknowledgments

Michael O. Bice
Jane DeSpiegelaere, MBA, RHIA, CCS, FAHIMA
Rose Dunn, MBA, RHIA, CPA, FACHE
Elisa Gorton, RHIA, MAHSM
Odia Godwin, MBA, MPA, NHA, RHIA
Barry S. Herrin
Laurie Lutz, MBA, RHIA, CHPS
Kelly McLendon, RHIA
Lori Nobles, RHIA
Brenda Olson, RHIA, CHP, M.Ed.
John C. Parmigiani
Daniel J. Pothen, MS, RHIA, CPHIMS
Jackie Raymond, RHIA
Mary Stanfill, RHIA, CCS, CCS-P
Diana Warner, MS, RHIA, CHPS, FAHIMA
Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Prepared by (original):

Rita Bowen, MA-HMT, RHIA, CHPS
Patricia Carter, JD
Beth Hjort, RHIA, CHPS
Chrisann Lemery, MS, RHIA
Debra Mikels

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

† Indicates an AHIMA best practice. Best practices are available in the AHIMA Compendium, http://compendium.ahima.org.

Article citation:
AHIMA. "HIE Management and Operational Considerations" *Journal of AHIMA* 82, no.5 (May 2011): 56-61.