Privacy and Security in Health Information Exchange

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

HIM professionals play a key role in managing many of the legal and operational issues in the paper environment. As local and regional networks for the exchange of electronic health information develop, and as state and federal laws evolve, it is important that HIM professionals keep abreast of related privacy and security issues. The expertise that HIM professionals bring to regulatory, policy, and information standards in paper practice must be developed and translated to help build the foundation for the confidential and secure exchange of electronic information across communities.

This practice brief outlines privacy and security issues related to developing and implementing a health information exchange.

Definitions

There are a multitude of terms currently used to describe a networked community of healthcare entities using interoperable electronic health record systems to exchange health information. These include regional health information organization (RHIO), health information exchange (HIE), the nationwide health information network, and at one time, community health information network. For this practice brief, the term *HIE* will be used.

Health information exchange can occur in many ways. The following are examples of linking methods:

- **Federated model with shared repositories.** This model uses a network of 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.
- **Federated model with 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 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. There is no national or regional entity maintaining a master patient index for the HIE, so a mechanism to identify the location of records is required.
- **Centralized database or data warehouse.** This model 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 at a central site. Participants submit data to and request data from this central site.

Guiding Privacy Principles

In a February 2005 report Connecting for Health, a public-private collaborative of the Markle Foundation, outlined nine guiding principles that provide a multilayered approach to ensuring confidentiality of patient data in an information-sharing system or network. These principles are openness and transparency; purpose specification and minimization; collection limitation; use limitation; individual participation and control; data integrity and quality; security safeguards and controls; accountability and oversight; and remedies.

These privacy principles are critical to achieving a successful HIE, and several are addressed within the discussion of legal and operational issues that appear below.

Legal Issues

Myriad state and federal laws require that 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. These issues are further described below.

Variations in state law. Since individual states have their own laws addressing privacy of patient health information, a pre-emption analysis comparing the HIPAA privacy rule with these state laws is necessary. Some of these state laws relate to 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 from state to state can be a barrier to HIE adoption, and multistate HIE initiatives must find ways to accommodate varying state laws.

Other federal laws. Other federal laws regarding privacy of health information generally still apply. Some federal laws and regulations that affect the exchange of health information are Medicare Conditions of Participation, Confidentiality of Alcohol and Drug Abuse Patient Records Regulation, Family Educational Rights and Privacy Act, Gramm-Leach-Bliley Act, and the Food, Drug, and Cosmetic Act. Although there should be few instances of conflict among these laws, any conflicting statutes need interpretation to achieve compliance with each regulation.

HIE participation agreements. 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 exchange of information, these agreements will need to address matters such as HIPAA business associate provisions, protecting proprietary information of the parties, intellectual property rights, software licensing, insurance, indemnification, audit rights, and dispute resolution.

Operational Issues

The HIPAA privacy and security rules require that protected health information be accessible to patients; be maintained in a manner that maintains patient privacy, security, and data integrity; and be released in accordance with state and federal laws. Health information professionals are most familiar with these requirements, and as such, are well-positioned to consider the following operational issues when involved in an HIE.

Minimum necessary. The "minimum necessary" regulation under HIPAA's privacy rule requires that reasonable effort be made to limit protected health information to the minimum necessary to accomplish the intended purpose. For routine and recurring disclosures, standard protocols must be implemented, such as the Continuity of Care Record standards. For all other disclosures, reasonable criteria must be developed for making the minimum necessary determination, and disclosures must be individually reviewed in accordance with these criteria.

Access to health information. Organizations will need to define who needs access to the information in the HIE and must ensure that there is appropriate authentication and auditing processes.

Patients have the right to access their health information in order to be informed consumers and to have control of their healthcare information. Due to the fact that healthcare decisions may have been made based upon information from the exchange, organizations in the HIE may need to redefine their designated record set.

Identity management. The adopted exchange model should have robust patient identification capabilities. The patient identification process raises at least two privacy concerns. First, is the correct patient identified? If not, detailed patient information may be inappropriately disclosed about the person who was falsely identified as the patient. 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 identify the correct patient record without exposing unnecessary information about other patients.

Opt in or opt out. Whether patients choose to include their health information in the exchange is not a simple question. An opt-in or opt-out decision can occur at various points in the process by which demographic or clinical information is made available to the HIE. The HIPAA state pre-emption analysis, particularly as it relates to authorization, may determine an opt-in or opt-out approach.

Quality of information. Organizations exchanging health data must take responsibility for quality of the data they made available to the HIE. They must establish rules addressing data definition, timeliness, accuracy, relevancy, reliability, accessibility, specificity, precision, currency, and comprehensiveness.

The HIE must adopt standards for data content and data definitions to maintain data integrity and quality. A key component of these data standards is the 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.

Security and communication standards. HIE participants must agree on standards for security and communications. The Certification Commission for Healthcare Information Technology, a voluntary, private-sector initiative, has established minimum, uniform security criteria for EHR ambulatory care product certification. They are expected to publish criteria for inpatient products in 2007. The National Institute of Standards and Technology, a government agency, develops information security tools and standards to improve information security. The standards and practice tools created by its Computer Security Division are available at www.csrc.nist.gov.

Operational impact of variations in state law. The technology available to a multistate exchange may not easily support variations in state laws and therefore may require manual intervention. For example, an HIE operating in state A and state B may need to respond differently to requests for information, 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 information may be provided. In states where suppression of specific clinical information may be required, it is important to consider when or whether to include a notice to clinicians receiving information in the HIE that certain types of data have been redacted and that the information provided may be incomplete.

Notice of privacy practices. As covered entities governed by HIPAA enter into relationships with other organizations to exchange information, the notice of privacy practices should explain their participation and exchange of health data.

Patient 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 information technology, and that these benefits can be realized without sacrificing the privacy and security of their information.

Recommendations

The legal and organizational matters related to privacy and security are essential issues to be addressed in the development and implementation of an HIE. Establishing guiding principles to protect privacy and security of health information, developing procedures for patient identification, and ensuring minimum necessary data are released are key functions that the HIM professional can lead. HIM professionals need to accept a leadership role in the privacy and security of an HIE.

Reference

Connecting for Health. "Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy." February 2005. Available online at www.connectingforhealth.org/ assets/reports/linking_report_2_2005.pdf.

Prepared by

Patricia Carter, JD
Chrisann Lemery, MS, RHIA
Debra Mikels

Rita Bowen, MA-HMT, RHIA, CHPS
Beth Hjort, RHIA, CHPS

Acknowledgments

Resources

AHIMA e-HIM Work Group on EHR Data Content. "Guidelines for Developing a Data Dictionary." *Journal of AHIMA* 77, no. 2 (February 2006): 64A–D.

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 (January 2006): 64A–D.

AHIMA and the American Medical Informatics Association. "Statement on Health Information Confidentiality." *Journal of AHIMA* 77, no. 10 (November–December 2006): 22.

Article citation:
Carter, Patricia; Lemery, Chrisann; Mikels, Debra A; Bowen, Rita K.; Hjort, Beth M..
"Privacy and Security in Health Information Exchange." *Journal of AHIMA* 77, no.10
(November-December 2006): 64A-C.

Driving the Power of Knowledge