Privacy and Security Challenges in HIEs: Unique Factors Add New Complexities to Familiar Issues

by Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS

On a recent trip out of town, I had a very enlightening conversation with a cab driver on the way to the airport. Even though it was early in the morning, the driver was extremely talkative and initiated a conversation about what I did for a living. This immediately led to direct questions regarding my position on plans to develop regional health information organizations.

To my surprise and delight the cab driver was very knowledgeable on the topic. However, in spite of my efforts to outline the many benefits of health information exchanges (HIEs), she remained unconvinced that the healthcare industry could be depended upon to protect the privacy and confidentiality of her health records.

The success of the nationwide health information network (NHIN)-the sum of local and regional HIEs-depends on consumer confidence in its privacy and security. HIE business practices must be unambiguous and transparent to the public.Without consumer buy-in, the NHIN will fail.

Unique Challenges

At a fundamental level the privacy, confidentiality, security, and information use challenges facing HIEs are the same as those faced by any healthcare entity. The uniqueness of HIEs-structures, relationships, funding, and authority-adds new complexities to the familiar issues of privacy, confidentiality, security, and information use. These unique issues include:

- The diversity of stakeholders
- Contradictory viewpoints
- A wide assortment of hardware and software
- A variety of organizational structures
- A diversity of data standards
- A range of communication models
- A wealth of policies and procedures
- Multiple business practices

Adding to the challenge of implementing privacy and security policies and procedures in information-sharing systems is the diversity of opinions and definitions about privacy and confidentiality. In HIE networks the very concept of privacy becomes difficult to define. Privacy has been described as a "notoriously vague, ambiguous and controversial term that embraces a confusing knot of problems, tensions, rights, and duties."[1]

Those that take on the challenge of implementing HIE networks are soon faced with the enormity and diversity of stakeholders, laws, regulations, and business practices. Yet, for the NHIN to improve safety, efficiency, and healthcare quality, all participants must reach a consensus and commit to a uniform set of policies, procedures, and business practices.

Resolving HIE Privacy, Security Issues

Efforts to resolve the barriers to the free flow of electronic health information, while preserving privacy and security requirements, are currently under way at many different levels. One of the most ambitious and comprehensive efforts is a survey by the Health Information Security and Privacy Collaboration, whose goal is to gain national consensus on the privacy and security solutions that will facilitate interoperable health data exchange.

Under a contract from the Department of Health and Human Services and funded by the Agency for Healthcare Research and Quality, the survey is being led by the research firm RTI International in conjunction with the National Governors' Association Center for Best Practices. The contract provides funding for the establishment of up to 40 individual state projects designed to evaluate the perceived barriers in existing privacy and security laws and business practices that pose interoperability challenges and hinder the free flow of electronic health information.

The contract objectives include:

- Assessing variations in organization-level business policies and state laws that affect health information exchange
- Identifying and proposing practical solutions, while preserving the privacy and security requirements in applicable federal and state laws
- Developing detailed plans to implement solutions

States and territories that receive a contract will be required to undertake certain activities, including:

- Examining privacy and security policies and business practices regarding electronic health information exchange and the current legal requirements in the state that may be driving those policies
- Identifying challenges that privacy and security policies might pose to interoperable health information exchange
- Identifying best practices and solutions for maintaining privacy and security protections while enabling operation of a health information network
- Developing an implementation plan to address organization-level business practices and state laws that affect privacy and security practices in order to permit interoperable health information exchange
- Convening and working closely with a wide range of stakeholders in the state, including clinicians, physician groups, health facilities and hospitals, payers, public health agencies, government health agencies, pharmacies, long-term care facilities and nursing homes, and consumer organizations
- Identifying and organizing a steering committee to lead the effort within each state
- Participating in regional and national meetings with other states to share knowledge and collaborate on HIE privacy and security issues and related issues

Chosen states must complete their work within a year.

Nine Principles for HIEs

In a policy guide titled "The Architecture for Privacy in a Networked Health Information Environment," the Markle Foundation's Connecting for Health outlines nine principles that should be built into any information-sharing system or network in order to ensure confidentiality and privacy of patient data:

- 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
- Remedies

Connecting for Health believes that technical and policy challenges stand in the way of widespread health information exchange; however, there is no perfect technical or policy solution to the interoperable exchange of health information. If we are to create interoperable exchange, we must:

- Establish uniform access management policies
- Set acceptable limits on the appropriate use of information
- Agree upon the extent of patient control over personal health information
- Make technology choices that support privacy and security policy objectives

Developing an HIE Model

Connecting for Health also recently published "A Model Contract for Health Information Exchange," which outlines the terms and conditions addressing the confidentiality, security, and use of protected health information. The model names the following essential elements for an HIE contract:

- Each HIE participant must comply with healthcare privacy, confidentiality, security, and use standards.
- Each HIE participant must comply with state and local privacy, security, and use laws.
- Each HIE participant shall report to the other serious breaches of confidentiality.
- Established limitations will be placed on the use and disclosure of protected health information.
- Protected health information will be secured by appropriate administrative, physical, and technical safeguards.
- Each HIE participant shall report to the other any use of protected health information outside the established terms and conditions.

Healthcare consumers will not accept a health information exchange network fraught with uncertainty and confusion. We have come to a point in the evolution of health information management where we can no longer go it alone. As healthcare professionals we must ask ourselves, are we working on a solution, are we working toward consensus? We must reach out to all HIE stakeholders, guided by a shared vision that puts patient privacy first.

Note

1. Bennett, Colin. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press, 1992.

References

Connecting for Health. "The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange." Available online at www.connectingforhealth.org/commonframework.

Health Information Security and Privacy Collaboration. "Status of the Health Information Security and Privacy Collaboration (HISPC) Proposal Evaluation." Available online at www.rti.org/hispc.

Harry Rhodes *(harry.rhodes@ahima.org) is director of practice leadership at AHIMA.*

Article citation:
Rhodes, Harry B.. "Privacy and Security Challenges in HIEs: Unique Factors Add New Complexities to Familiar Issues." *Journal of AHIMA* 77, no.7 (July/August 2006): 70-71,74.