HITECH'S IMPACT ON HEALTH INFORMATION EXCHANGES: KEY DECISION POINTS FOR PRIVACY AND SECURITY

Author: Jared Rhoads

By February 2010, the HHS Secretary must appoint a Chief Privacy Officer (CPO) of the Office of the National Coordinator (ONC). The duties of the CPO will be to advise the coordinator on privacy, security, and data stewardship of electronic health information, and to coordinate with other agencies at the federal at state levels to ensure the protection of electronic individually-identifiable health information.

Spotlight on HIE

Health Information Exchanges (HIEs) support secure electronic sharing of patient health information among authorized caregivers, patients, public health authorities, and other providers of healthcare and payment services across different settings and geographical areas. For example, a physician treating a patient would be able to get authorization from the patient to access the patient's entire medical history including a list of current medications, known allergies, and other vital information originally recorded in multiple systems across caregivers. In cases of emergency, caregivers would be able to "break the glass" to obtain secure, audited access to the medical history, in order to make the best care decisions for the patient.

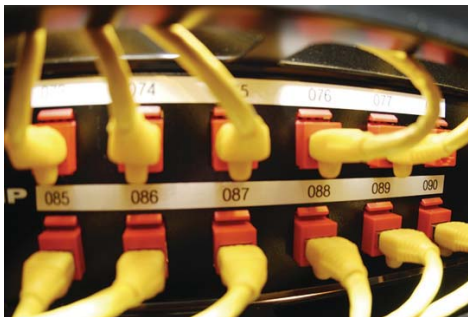
At its largest scale — and with consistent standards — connecting providers to local networks and then connecting the networks to each other makes it possible to create a nationwide health information infrastructure through which authorized providers can access any patient data that they need, regardless of where the data reside.

However, the benefits from HIE can only be as good as the patients' willingness to share their medical data.[1] This level of data access has generated concern among some patients and privacy advocates because it increases the risk of unauthorized access to patient information. Without trust and consent from patients to share their data the usefulness and sustainability of an HIE is severely undermined, making privacy and security critical to any HIE's success. Efforts have been delayed or stalled trying to reach consensus on these difficult issues.

HITECH: Supporting the HIE Vision

Recent legislation is helping to renew interest in HIEs. The Health Information Technology for Economic and Clinical Health (HITECH) Act provides financial incentives (up to $36 billion) to providers for using electronic health records (EHRs) that have the capability to support the exchange of health information; part of the Meaningful Use definition. The HITECH Act also provides more than $300 million in funding to regional or local health IT efforts, and instructs the Health and Human Services (HHS) Secretary to "invest in the infrastructure necessary to allow for and promote the electronic exchange and use of health information for each individual in the United States."[2]

HITECH also has the potential to make great strides in gaining patient trust by closing some of the HIPAA gaps not imagined possible more than a decade ago. New requirements include stiffer penalties and potential criminal charges against healthcare individuals, the establishment of security and privacy benchmarks, and security breach notification. These are just the new requirements for privacy and security in general. More specific requirements and standards will be defined. The HIE workgroup reporting to the HIT Policy and HIT Standards Committees has been charged with refining the security and privacy requirements specific to data sharing and patient consent.



Key HIE Decision Points

As a result of these new opportunities and new requirements, many providers will be restarting their discussions on how to build effective, secure patient data sharing exchanges. Whether an organization is considering joining an HIE or is starting one, there are key data access and sharing decisions that will their impact privacy and security needs and safeguards. These decision points relate to data sharing, central versus local data storage, authorized access rights, regulatory requirements, and patient consent. Thinking through the following points can help organizations determine policy and system requirements to ensure that the HIE data exchanges adhere to HITECH regulatory requirements and offer safe data exchanges that add value to care delivery.

1. Determining What to Share and How to Share It

The term "data sharing" has a wide range of interpretations that need to be carefully analyzed to determine the appropriate level of privacy and security procedures and system requirements. There are two questions any organization involved in exchanging health information needs to answer:

1. What data are being shared, and
2. How will it be shared?

The major factor for determining the data to share is the business or case reason for setting up the HIE. Successful efforts have found that starting small and then broadening the data sharing as the scope of the HIE expands brings early wins and increases participation. In Massachusetts, the New England Health Exchange Network (NEHEN) started with eligibility and benefits checking and then became the infrastructure for an e-prescribing solution called MA-Share. Another example is MidSouth eHealth Alliance (Memphis, TN). This HIE started by sharing primarily imaging data, including chest X-ray reports. The exchange succeeded in reducing repeat imaging and resulted in faster diagnoses, fewer unnecessary exposures to radiation, and lower costs for payers. Now, three years into operation, the exchange has been expanded to support patient demographics, lab results, cardiac study results, discharge summaries, and other dictated reports.[3]

Sharing data involves a variety of functions that end users can use to access and act on the data. Options include view-only, view with the ability to send a message to add or update information, and direct access to add or update.

The following are examples of approaches to data sharing and viewing for several major HIE and EHR (eHealth) initiatives:

- In Denmark, a central database stores patient record summaries, which contain basic encounter data and are viewable by general practitioners (GPs). Full records are stored locally with each patient's practitioner.
- In the Netherlands, GPs can view detailed data stored in each other's systems and send suggestions for updates and corrections via a messaging service.
- In the United Kingdom (UK), GPs can make additions and edits to patient records remotely; however, in order to protect the quality of the data, old information is flagged but not deleted.[4]
- In the United States, the Bidirectional Health Information Exchange (BHIE) allows clinicians at the Department of Veterans Affairs and the Department of Defense to view real-time electronic healthcare data stored on each other's local systems. Data such as lab orders, lab results, radiology reports, outpatient pharmacy data, and allergy lists are viewable bi-directionally for patients who receive care from both facilities.

It is important to understand the sharing capabilities that will be allowed and to make sure that each exchange has proper privacy, security, and data integrity policies and procedures in place. Regardless of the approach, it is essential to include an audit trail function to capture all interactions. Logs should be monitored continuously for security breaches, and reports of activity (including what was viewed and by whom) are available to patients on request.

2. Managing Authorized Access

Organizations need to develop policies that clearly describe who owns and controls the patient data, and that specify how relationships between participants will be formed, managed, and ultimately terminated. Since there is such as wide range of data access and sharing, the complexity of privacy and security requirements increases as more data are available and as end users are able to do more with the data than just view it. For instance, viewing an index of patient encounters requires that the end user be given access permissions. Viewing summary data typically requires role-based authentication. Access to detailed data is generally only allowed for physicians and under specific circumstances. If the end user is allowed to add to the patient data, then both the sending and receiving systems must authenticate and coordinate rights and permissions.

In the UK, the National Health Service has implemented highly-effective, role-based access policies across its network of EHRs. There are multiple levels of access, ranging from ward clerks, who can see only demographic information, to physicians, who can view nearly the entire record. (Mental health information may be excluded.) Access is further restricted to just those clinicians who have a "legitimate relationship" with a patient. This relationship can be defined with as much or as little flexibility as needed. For instance, caregivers can be assigned a legitimate relationship with a patient based on the caregiver's ward, floor, or work shift.

The UK has a second level of authentication that ensures end users are who they say they are. Every authorized user has a smart card that must be inserted into a reader in order for the user to log into the system. The smart card features photo identification and contains the user's credentials, including name, role, location, and any special activities for which the user is authorized.[5]

It is best to use a formal process for developing and implementing these policies. For example, the Maryland Health Care Commission (MHCC) set up a Policy Board to establish its own minimum requirements for role-based authorization. These policies are then reviewed and adopted by the commission.[6]

3. Preventing Unauthorized Access

HIEs need to implement technologies and procedures to prevent unauthorized access at vulnerable points, including the network, the data center, and end-user devices. One way to reduce unauthorized access is to host applications and data servers in a secure, remote, monitored data center. Desktop options such as virtual desktop infrastructure (VDI) or Citrix-based solutions that do not store data locally are the best end user devices for security and privacy. If the devices are lost or stolen, there is no patient information on the devices so the organization does not need to worry about a breach of patient privacy.

Encryption is necessary on all devices storing data and on the network to render the health information unusable, unreadable, or indecipherable to unauthorized users. For instance, the Louisville Health Information Exchange (LouHIE), operates under the health record bank model, and uses advanced encryption techniques borrowed from the financial services industry. (This was achieved in part through good governance: one of the four Functional Committees that reports to the LouHIE Board of Directors is dedicated to privacy.[7]) Another HIE, the Minnesota-based Community Health Information Collaborative (CHIC), uses a special service to encrypt the email messages that patients and providers send across its network.

A major goal of the committees, as stated by the HITECH Act, is to make recommendations that "minimize the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns."

Privacy and security standards for HIEs are still under development, but they are emerging rapidly. The HITECH Act established two new federal advisory committees on policy and standards to recommend technology standards to the National Coordinator, including standards for security and communications. Privacy and security topics are being prominently considered by both committees. The Standards Committee formed a distinct workgroup dedicated to privacy and security issues, while the Policy Committee has instructed each of its three workgroups to consider privacy and security as a pervasive concern in each of

their areas of focus. Initial work by the Standards Committee has included reviewing the work done by its precursor — the Health IT Standards Panel (HITSP) — in the areas of interoperability specifications. Both committees hold public meetings and post their meeting agendas, documents, and transcripts on the HHS Web site. An initial set of guidelines is due by December 31, 2009.

New technology standards have also been discussed that could require EHR vendors to isolate or segment sensitive personal medical information such as a patient's mental health history, drug or alcohol history, or certain treatments that are paid for out-of-pocket.[8] Some groups have also raised the possibility of creating an independent body to certify EHR systems for privacy, although this idea has yet to gain widespread support.[9]

4. Gaining Consent and Adoption

Gaining patient consent and provider adoption is based on timely education related to the purpose, benefits and risks of data sharing so patients make informed decisions. This includes understanding what information is being shared across the exchange, which organizations are participating, what safeguards have been put in place to protect their privacy, who can access and use the information, and where the data reside.[10]

Education to gain community support can take a number of forms — through printed materials, direct mailings, and possibly even paid advertising. Some HIEs post informational videos online or sponsor kickoff events that are open to the public. As part of its consumer education campaign, the Vermont Information Technology Leaders (VITL) health exchange showcased the fact that VITL's standards for privacy and security exceed those used by the federal government.[11] HIEs can also educate consumers on how technologies such as virtual private networking (VPN), digital certificates, smart cards, and encryption are used to protect privacy.

Most patients trust their physician's judgment and many will agree to participate if given the enough time to discuss the program in a trusted setting such as their local hospital or physician's office. For example, patients in the UK were made aware of the safeguards in place and were given plenty of advanced time to make their decisions. Less than 1 percent (0.78 percent) chose not to have their data shared.

Conversely, opt-in rates can suffer if patients are not given enough time. In the Netherlands, informed consent was not addressed until much of the system was built and was ready for rollout. The decision was made to send everyone a letter asking for permission. Citizens were taken by surprise by the consent letter they received in the mail, and consequently 300,000 people sent letters back with incomplete or inaccurate information. Every letter needed to be followed up to get an answer, resulting in a lengthy delay in rolling out the system.

Consent does not need to be an all-or-nothing decision. Some authorities, such as the California Office of Health Information Integrity, have suggested that context (e.g., a normal or emergency setting) and granularity (e.g., allowing data from only certain sources to be shared) can be effectively addressed by offering patients the additional alternatives of "Opt-Out with Exceptions" and "Opt-In with Restrictions."

5. Addressing Breaches in Privacy and Security

Although advanced security measures have come a long way to protect patient privacy, all breaches cannot be anticipated and avoided. The HITECH Act establishes new security and privacy requirements for notifying patients in the event a breach does occur. For example, providers must notify affected individuals by mail or email within 60 days of the discovery of the breach. Providers must also notify HHS and prominent media outlets in the event of a breach that affects more than 500 individuals. Under HITECH, these requirements and previous HIPAA requirements are specifically extended to include providers' business associates, such as HIEs, vendors of personal health records (PHRs), and other service providers. As consumer advocates have pointed out, much of privacy depends on the good behavior of covered entities.[12]

One of the more challenging new requirements for HIEs is to provide patients with a detailed accounting of disclosures. This log serves as an audit trail that shows patients who has accessed their information, which information was accessed, and when it was accessed. HITECH stipulates that individuals have a right to an accounting of all disclosures of protected health information within the past three years. This includes information relating to payments, treatments, and operations.

Finally, because state laws vary and federal law has recently changed, organizations should conduct a preemption analysis to compare current HIPAA and HITECH laws in a given locale and evaluate how this may affect compliance. The clearer the understanding of what is legally required, the more likely physicians and patients will be willing to participate.[13] This type of legal review is particularly important for organizations that are considering participating in a multi-state HIE initiative.

Looking Ahead

HITECH requirements, incentives and penalties related to privacy and security will continue to make healthcare organizations, physicians and patients more comfortable with and willing to exchange health information. In addition, there is a growing body of documented best (exemplary) practices to help newly-formed HIEs avoid making mistakes.

- The Common Framework published by the Markle Foundation has already helped health information networks devise ways to share information among participants securely.
- The new Action Implementation Manual published by the Health Information Security and Privacy Collaboration (HISPC) shares new tools, processes, and materials designed to solve state-level privacy and security challenges.[14]
- The HITRUST Alliance maintains a Common Security Framework to assist organizations in protecting electronic health information. The framework normalizes the security requirements of federal, state, and other bodies and provides configuration checklists for EHRs and privacy guidelines for clinical systems.
- HHS will be establishing Regional Extension Centers at state and local levels to disseminate best practices on the use of health IT, including HIE.

As these pieces fall into place, it will be important for organizations interested in HIEs to have the groundwork already started and continue to look to these resources for guidance and the latest developments related to the HITECH requirements and exemplary practices.

About the Author

Jared Rhoads is a Senior Research Analyst in CSC's Emerging Practices, the applied research department of CSC's Healthcare Group. The author was assisted by Fran Turisco, a Research Principal in CSC's Emerging Practices.

References

1. Tripathi, et al. "Engaging Patients for Health Information Exchange." *Health Affairs* 28.2.435, March/April 2009
2. Text of the Health Information Technology for Economic and Clinical Health Act
3. Frisse, M. "Update on MidSouth eHealth Alliance." April 2009, http://www.markfrisse.com/docs/2009-april-mseha-talking-points.pdf
4. "Large-Scale eHealth Initiatives: Decision Points and Best Practices." Deutsch, Berend, Lykke, Spence and Turisco, CSC white paper, 2009.
5. National Health Service. "Registration, User Roles & Smartcards." NHS website http://www.chooseandbook.nhs.uk/staff/implement/deployment/readiness/registration/index_html Accessed June 1 2009
6. Maryland Health Care Commission. "A Consumer-Centric Health Information Exchange for Maryland." April 15 2009
7. Louisville Health Information Exchange, Inc. "LouHIE Structure." May 13 2006
8. Text of the Health Information Technology for Economic and Clinical Health Act
9. Ball, KL, and Yasnoff, WA. "Averting the Collision: Privacy Doctrine and Health Information Exchange." Presentation to the eHealth Initiative, Washington DC, December 5, 2008
10. American College of Physicians. "ACP Statements on Electronic Health Information Exchange." October 2006
11. "Vermont Health Information Technology Plan: Strategies for Developing a Health Information Exchange Network." Vermont Information Technology Leaders, July 1, 2007
12. Ball, KL, and Yasnoff, WA. "Averting the Collision: Privacy Doctrine and Health Information Exchange." Presentation to the eHealth Initiative, Washington DC, December 5, 2008
13. Carter, Patricia, et al. "Privacy and Security in Health Information Exchange." *Journal of AHIMA* 77, no.10 (November-December 2006): 64A-C.
14. "Action and Implementation Manual." Health Information Security and Privacy Collaboration, June 2009

CSC
266 Second Avenue
Waltham, Massachusetts 02451
United States
+1.800.272.0018

Worldwide CSC Headquarters
The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Europe, Middle East, Africa
Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia
139 Cecil Street
#08-00 Cecil House
Singapore 069539
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

www.csc.com

WA09_0141

July 2009