Privacy and Confidentiality by Design: Fundamental Design Principles for Health IT

by Donald T. Mon, PhD

Virtually every stakeholder group-consumers, providers, payers, vendors, and HIM and IT professionals alike-is well aware of the importance of protecting the privacy and confidentiality of health information. Not everyone, however, is well acquainted with the actual guidelines, principles, and practices necessary to protect privacy and confidentiality. Yet privacy and confidentiality guidelines, principles, and practices are being built into emerging health IT standards.

Fundamental Design Principles for Health IT

Patients and consumers will be reluctant to share their health information with providers if they feel that their privacy and confidentiality are not protected. Consequently, protecting the privacy of health information through appropriate security procedures and ensuring that health information is kept confidential by authorized persons must be fundamental design principles for health IT, systems, and architectures.

Consider, for example, how privacy, as a design principle, can influence the way in which data are exchanged across a regional health information organization (RHIO). (Note that this example is simplified for explanatory purposes.)

In some RHIO architectures, health information is exchanged in a two-step process. In the first step, a provider makes a request to a record locator service (RLS), asking who in the RHIO has pertinent health information on the patient being cared for by that provider. The RLS then sends the request to participating hospitals and physician offices.

In response, those entities holding relevant health information for that patient disclose to the RLS that they possess such health information. The RLS then tells the requesting provider which entities have the health information being sought. In the second step, the requesting provider contacts those entities. After the appropriate release of information procedures are followed, the health information is then sent to the requesting provider.

In this architecture, the need to protect the privacy and confidentiality of health information influences some key actions. For example, in the first step a provider may not even make a request for health information if the request itself implies that the patient is being treated for a sensitive condition (e.g., mental health, substance abuse, HIV/AIDS). Responding providers may not disclose they have health information for that patient for the same reason. For example, even though it has not yet released health information at this point, the mere fact that a substance abuse clinic responds to the request tells you something about that patient.

In the second step, protecting the privacy and confidentiality of health information influences what health information is sent automatically to the requesting provider. If the sending provider has a number of records on that patient, some of which are sensitive, then the appropriate rules must be set up such that sensitive health information are not part of the automated exchange between information systems.

An Example: HL7

All facets of the e-HIM® environment must contribute to protecting the privacy and confidentiality of health information, even health information systems. One of the best ways to ensure that electronic systems support privacy and confidentiality is to build it into health IT standards.

Fortunately, many, if not all, of the standards are already moving in this direction. A clear example of this is the Health Level Seven EHR System Functional Model and Standard. The functional model consists of three sections: direct care, which

contains EHR system functions used during the hands-on care of the patient (e.g., problem list, medical history, orders); supportive, which contains surrounding functions that support clinical care and reporting (e.g., registries, public health reporting); and information infrastructure, which is comprised of records management, interoperability, and privacy and security functions.

Privacy, security, and confidentiality are recognized in the very beginning of the functional model. The first direct care function (DC 1.0) states, "Integral to…care management activities is an underlying system foundation that maintains the privacy, security, and integrity of the captured health information…" Moreover, privacy and confidentiality is required throughout the direct care section. For example, to produce a summary record of care (function DC 1.1.4), the system must "present a summarized review of a patient's comprehensive EHR, subject to jurisdictional laws and organizational policies related to privacy and confidentiality."

There are similar requirements for other direct care functions, among them present ad-hoc views of the health record (DC 1.1.5); manage consents and authorizations (DC 1.3.3); and care and treatment plans, guidelines, and protocols (DC 2.2). Also addressed are medication and immunization management (DC 2.3); orders, referrals, results and care management (DC 2.4); support for health maintenance: preventive care and wellness (DC 2.5); and population health (DC 2.6).

Each of these functions uses the privacy and confidentiality function in the information infrastructure section to enforce compliance to the requirement. That patient privacy and confidentiality function (IN 1.9) requires authentication, authorization, access control, nonrepudiation, and record auditing. Every time a direct care function requires privacy and confidentiality to be enforced, an individual must be authorized to care for the patient and document health information, and that individual must be authenticated when using the system. Additionally, the documentation of health information must be auditable.

Building Privacy and Confidentiality into Standards

So what does this all mean in the end? Privacy and confidentiality are clearly recognized by all stakeholders as key to the e-HIM environment. Privacy and confidentiality must drive the design of health IT, not the reverse.

One way to ensure that electronic systems, such as the EHR, comply with privacy and confidentiality requirements is to build the latter into standards and criteria for certification. Compliant systems can then help enforce privacy and confidentiality guidelines, principles, and practices during direct care work flow.

Everyone then-from consumers whose privacy and confidentiality will be protected, to clinicians who will find the assistance from electronic systems useful as they care for patients, to HIM professionals who maintain privacy and confidentiality practices in their facilities-will benefit from this kind of health IT support.

Reference

Health Level Seven. "EHR-S Functional Model and Standard." Available online at www.hl7.org/ehr.

Donald T. Mon *(don.mon@ahima.org) is vice president of practice leadership at AHIMA.*

Article citation:
Mon, Donald T.. "Privacy and Confidentiality by Design: Fundamental Design Principles for Health IT." *Journal of AHIMA* 77, no.10 (November-December 2006): 64-65.