Privacy Architecture and e-Consent

by Kathleen Connor

As the US prepares to implement a nationwide health information network (NHIN), one issue that repeatedly surfaces is how to appropriately protect the privacy and security of electronic health information. Of particular concern is how such a system can accommodate the various legal restrictions on disclosing sensitive health information (e.g., HIV/AIDS status, genetic makeup, domestic abuse, mental health conditions or treatment, and chemical dependency), as well as patient consent requirements for disclosure of information for treatment purposes.

The NHIN must be compliant with a multitude of state and federal privacy laws without jeopardizing patient safety and quality of care. One approach to this challenge is to examine how other countries are implementing consent policies and practices, especially concerning sensitive health information, in their developing NHINs.

Obtaining a Global Perspective

A recent paper on this topic that I coauthored with Joy Pritts, JD, reviews in-depth the approaches taken in Canada, England, and the Netherlands.[1] This article is based in large part on that paper.

Pritts and I found that, like the US, these countries are faced with reconciling multiple and sometimes conflicting privacy laws that were adopted independently by jurisdictions in a siloed fashion. These laws were designed primarily to protect the privacy of patients' paper-based health records. And like the US, they are in the process of harmonizing laws where possible, usually where the legal intent is similar but the statutory protections are implemented differently.

Where they differ is the maturity of their technology approaches or "privacy architectures" for supporting electronic privacy protection, especially where the legal requirements remain jurisdictionally unique across their NHINs. They are developing technology solutions that will enable electronic consent (e-consent) mechanisms, consent registries, and computably negotiable privacy policies.[2] These privacy architectures may provide us with best practices and technology approaches for supporting existing consent requirements for sensitive health information in the US.

The three countries deployed several key technology components in different ways in their privacy architectures. These components are discussed in this article for two reasons. The first is to establish a baseline understanding about these technologies. The second purpose is to envision the look and feel (from the consumer perspective) of a desired future state of a conceptual privacy architecture by contrasting our current system with a potential world where technology supports robust consumer control over their health information.[3]

Looking Ahead to the Future

In the current paper-based privacy architecture, patients fill out consent forms by hand (likely more than once) and learn about privacy policies by reading the posters posted on providers' walls. Health records are masked or redacted with black pen or white ink before they are, for example, sent to a health plan for prior authorization of care.

In the paper-based privacy architecture, patients have very little control over what happens with their paper records. The extent of patient control is withholding information from providers or having special agreements such as putting all sensitive information on sticky notes, which are removed when the paper chart is copied.

In the fully automated privacy architecture of the future, consumers will go online to fill out their consent directives using a "wizard" much like the ones used today to set up browser privacy and security preferences. The wizard is a useful metaphor for envisioning how complex privacy rules can be given a user-friendly interface, because that's exactly what's behind the browser wizards—a myriad of complex Internet privacy and security rules made easy for consumers.

Following this same line of "to be" visioning, the same way that our browser wizard would warn us about the down sides of selecting a particular option with respect to our potential loss of privacy, the health privacy wizard's sliding scale would enable us to select who can do what, with what, and why while informing us about the risks to privacy and benefits of disclosure. For each type of health information, consumers can select those they consider sensitive.

For example, I may not care if all authorized providers have access to my preventive care records but may want to limit access to certain reproductive health records. In some cases, a jurisdiction may preset consent directives. For example, all chemical dependency treatment information must have explicit consent.

Among the choices consumers could make are permissions including collection, access, use, or disclosure. For each type of information, a consumer can select one or more "who" such as:

- A specific provider, using a national provider identifier
- A type of provider, using a drop-down box from which to select (e.g., a primary care provider, a care team, or emergency providers)
- A type of provider within a specific context of care (e.g., certain health information may only be accessed only by an emergency-care provider when I am unconscious)
- A provider to whom I give a password to a particular type of health information or a particular record

For each of these, consumers can select who can collect, access, use, or disclose their information and for what purpose. In addition, consumers could set limits on a provider's use and further disclosure of accessed health information by, for example, limiting access to "read-only" or "read and store," or by specifying the length of time for which a provider may have access.

The online consent directive wizard also lets consumers update or revoke consent directives, change their password when they no longer want a provider to be able to access their records, and delegate consents to a personal representative. If a consumer is unconscious in an emergency room, the decision support system would be capable of flagging adverse drug-drug interactions so that the provider knows to "break the glass" to prevent any harm, all supported by the e-consent infrastructure.

Privacy Architecture: Work in Progress

All of these e-consent capabilities are made possible by implementing a privacy architecture comprised of the type of standards being deployed in other countries. These standards are now under consideration by the Healthcare Information Technology Standards Panel Security and Privacy Work Group to meet the consent requirements of the American Health Information Community use cases. They include:

- Standards for conveying e-consent directives and passwords that a consumer may attach to masked health information. Health Level Seven is currently balloting version 3 consent topic specifications that are flexible enough to support privacy policies that vary by jurisdiction and are designed to support a migration path from the electronic transmission of scanned consent forms and privacy policies to fully encoded consents and policies as trading partners mature.4
- An e-consent repository associated with consumer identifiers, which provides the consent rules used when collecting, accessing, using, or disclosing the consumer's health information.
- A privacy policy repository of computably negotiable privacy policy, meaning that the applicable cross-jurisdictional policies can be blended using intersection algorithms that maximize adherence to collaboration rules dictated by participating jurisdictions.
- Robust user, role, and context-based access controls assigned to users in a health information exchange system. These rely on specifications such as the role-based access control healthcare permission catalog being balloted by Health Level Seven and the Tees Confidentiality Model piloted in England's National Health Service project.
- Access control services, which include service components for managing access control-related business rules such as those proposed by the Integrating the Healthcare Enterprise basic patient privacy consent profile.
- Ability for record locator services to index and search on standardized confidentiality codes and privacy-related data (such as diagnosis, treatment, demographics, and provider data) associated with health information messages and electronic documents in centralized or federated health information exchange systems.[5]
- Consent directives management service with components for managing consent-related business rules, consent directives, validating consent, mapping consent rules between and among jurisdictions, overriding consents, consumer

access control, and logging of consent directives and their application as detailed in the Canadian Infoway Privacy and Security Conceptual Architecture.[6]

Lacking in the US at this juncture is the "as is" and the "to be" concept of operations for a privacy architecture—a prerequisite to any enterprise architecture developed in accordance with the Federal Enterprise Architecture guidelines.[7] Once that happens, rather than trying to patch our "as is" paper-based privacy architecture into an electronic environment, consumers may be more fully engaged in the visioning of a "to be" NHIN privacy architecture. Only then will the policy vision of a healthcare system in which patients control their health information drive health IT, and not the other way around.

Notes

1. Pritts, Joy, and Kathleen Connor. "The Implementation of E-consent Mechanisms in Three Countries: Canada, England, and the Netherlands." February 2007. Available online at http://ihcrp.georgetown.edu/pdfs/prittse-consent.pdf.
2. This article uses the term "consent" policies and practices when referring to policies and practices that govern whether and how individuals have the right to control when and how their health information can be shared with others. The term "consent mechanism" is used to refer to the methods by which an individual can exercise such control. The term "e-consent" refers to the electronic technologies supporting consent mechanisms.
3. It's a given that a privacy architecture must be implemented within a supportive security architecture and cannot fulfill its requirements unless the appropriate security mechanisms are in place. There are likely privacy architecture capabilities that are not yet implementable because supportive security technology is not feasible, developed, or scalable at this time. For example, although role-based access is expected of all HIPAA-covered entities, enabling cross enterprise role-based access is less viable at this time outside of tightly coupled environments. However, it is possible to describe privacy architecture components in terms of maturity levels that can move us from the "as is" paper-based world to a "to be" fully automated environment without making assumptions about the availability of supportive security mechanisms. While the United States has moved to widespread use of secure electronic data interchange of HIPAA-covered transactions, its privacy architecture is still totally paper-based despite the implementation of key security components required to support it.
4. Health Level Seven. HL7 Version 3 Standard: Medical Records; Data Consent, Release 1. Available online at www.hl7.org/v3ballot/html/welcome/environment/index.htm.
5. See Health Level Seven version 3 vocabulary available online at www.hl7.org/v3ballot/html/welcome/environment/index.htm.
6. Canada Health Infoway. "Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture: Version 1.1," appendix A at 119. June 2005. Available online at www.infoway-inforoute.ca/en/home/home.aspx (registration to Infoway Passport required).
7. Chief Information Officers Council. "A Practical Guide to Federal Enterprise Architecture." February 2001. Available online at www.cio.gov/documents/bpeaguide.pdf

Kathleen Connor *(kathleen.connor@foxsys.com) is a senior consultant at FOX Systems, Inc., in Olympia, WA.*

Article citation:
Connor, Kathleen. "Privacy Architecture and e-Consent" *Journal of AHIMA* 78, no.6 (June 2007): 64-65; 70.