AHIC EHR WORKGROUP PRIVACY ARCHITECTURE CONSIDERATIONS

Submitted by:

John P. Houston
Director, Information Services Division;
Privacy Officer and Assistant Counsel

University of Pittsburgh Medical Center
Information Services Division
10072 F.T.200 Lothrop Street
Pittsburgh, PA 15213
Telephone: 412/647-8043
Fax: 412/ 647-6003
Internet: houstonj@upmc.edu

Overview

My comments are prefaced by the fact that the NCVHS Privacy Subcommittee is currently working on a comprehensive letter to Secretary Leavitt regarding privacy and confidentiality consideration related to the NHIN.

Patient input clearly indicates that a chief patient concern relates security and privacy. In order to achieve public buy-in, patient privacy and security concerns must be substantively addressed. Patient control is often viewed as the surrogate for privacy. Much discussion has taken place at the national level regarding what level of patient control is appropriate to satisfy the patient's privacy concerns. Key aspects of this discussion relate to such concepts as opt-in vs. opt out, the patient's right to block information, and the patient's right to audit access.

While the HIPAA Privacy Rule permits protected health information (PHI) to be shared for treatment purposes without a patient's authorization, individual state privacy laws effectively prevent uniform sharing of PHI on an interstate basis. Further, other types of disclosures are not permitted under the HIPAA Privacy Rule absent patient authorization.

The existence of disparate state laws may act as a barrier to the formation and operation of a NHIN, especially as it relates to the disclosure of PHI between providers that are located in states that have more stringent (or disparate) state laws governing the release of PHI.

In the near term, it is not practical to expect that HIPAA will be amended to preempt more stringent state law. Nor is it practical to expect the adoption of a uniform state privacy law. Therefore, to address patient privacy concerns, an infrastructure needs to be developed that provides a robust mechanism for patients to authorize providers (and others) to view a patient's PHI. Further, the infrastructure needs to authenticate users.

The authentication & authorization infrastructure need to be national in scope. Absent a national scheme to authenticate users, as well as to ensure that the user is authorized to view a patient's information, there will be no ability to share information across regions.

Authorization Infrastructure

I believe that the authorization infrastructure could be a secure web-based portal that would provide the following functionality:

- The patient could pre-authorize the release of PHI. This could be performed initially through a provider at the time of treatment. The provider would act as the patient's agent for the purpose of enrolling the patient in the authorization infrastructure. The provider would enter the patient's information in the authorization infrastructure, along with an initial set of authorizations (that describes which providers have the right to review what types of PHI). The authorization infrastructure would provide a "receipt" that the provider would print out and provide to the patient.
- By enrolling in the authorization infrastructure, the patient would be provided with a user account and password. This could be mailed to the patient, e-mailed to the patient (if the patient has e-mail) or printed on the receipt that the provider would give to the patient. This account could be used by the patient for such purposes as to authorize access to the patient's information and to audit access.
- The authorization infrastructure would provide the following types of authorization functionality:
    - PHI would be categorized. For example "psychiatric related PHI", "Medications", "HIV / AIDS related PHI", "Cosmetic Procedure related PHI", "STD related PHI", "Drug & Alcohol related PHI", etc.
    - Authorization could be established globally. For example "all providers can view all PHI", or "all providers can view all PHI from Provider X"
    - Authorization could be established specifically. For example "Provider X can view all PHI, except Psychiatric PHI", "Provider Y cannot view any PHI", or "Researcher Z can view all PHI from Provider X"
    - Authorizations could be established for a specific period of time. "Provider X can view all PHI until 12/31/06".
- The authorization infrastructure would allow the patient to perform the following:
    - View and change authorizations.
    - View which users requested PHI and what information was provided by which providers in response to a request for PHI.

Authentication Infrastructure

Likewise, an authentication infrastructure needs to be developed that would authenticate users (providers, researchers, public health authorities, etc). The authentication infrastructure could be tailored after commercial PKI application/services available from such sources as VeriSign (see http://www.verisign.com/products-services/security-services/pki/index.html).

To completely meet the needs of the NHIN, the authorization infrastructure and authentication infrastructure would need to be integrated so that user credentials could be evaluated against the information being requested and the authorizations that the patient has selected. Additionally, authentication information would need to be passed to the authorization infrastructure, so that

information regarding which users accessed the patient's information could be made available to the patient.