Privacy Consents and HIE

How IHE's Basic Patient Privacy Consents Profile Helps Manage Privacy in HIE

by **Michael Berry** and **Noam H. Arzt**

The potential benefits of health information exchange (HIE) are well documented, as are the privacy concerns of data sharing. In this new environment, patients are seeking increased control and transparency regarding how, with whom, and under what circumstances their electronic records are shared. Health IT standards are an important part of the effort to meet these needs.

Standards make it easier to transmit clinical data from one electronic health record system to another, and they play an important role in the implementation of privacy policies across organizations. Widely used standards such as the HL7 Clinical Document Architecture can be used to help implement privacy management and control features in an HIE. However, there are various ways these standards can be applied for this purpose.

This is where Integrating the Healthcare Enterprise (IHE) comes in. IHE provides technical frameworks for the use of existing standards, reducing variability in their implementation. The integration profiles that make up IHE technical frameworks specify how standards should be used to achieve specific needs within the framework.

The Basic Patient Privacy Consents

IHE's Basic Patient Privacy Consents (BPPC) is one such profile, part of a family of profiles for health information exchange based on Cross-Enterprise Document Sharing. The BPPC provides a mechanism to record a patient's privacy consents as documents in the exchange.

A consent may be as simple as an opt-in or opt-out to an HIE; it can be more complex, such as an assertion that particular kinds of health information can be accessed by particular types of participants. Storing consents in a standards-based document repository within the exchange opens the door for patients to be able to view the policies to which they have consented and to add or withdraw their consents over time.

In addition to recording consents, the BPPC provides methods to associate clinical documents with the policies that govern their disclosure and to enforce consents by limiting disclosure when consent to these policies has not been granted. For example, a document containing a laboratory result that reveals a patient's HIV status might be marked with a set of policies that describe the circumstances under which sensitive medical information can be disclosed in an HIE. Consider these three sample policies:

- Policy 1: Sensitive medical information can be disclosed to any clinician but only in an emergency.
- Policy 2: Sensitive medical information can be disclosed to the patient's primary care physician only.
- Policy 3: Sensitive medical information can be disclosed to any physician with a treatment relationship to the patient.

If the patient has consented to none of these policies, the document will not be retrieved from the exchange. On the other hand, if the patient has consented to at least one of the policies, or if one or more of the policies was included as part of a larger opt-in or opt-out decision to which the patient has consented, the document can be retrieved.

The final step before document disclosure requires confirmation that the circumstances of the retrieval meet the requirements of a consented policy. For example, is the situation an emergency situation, and is the person requesting disclosure a clinician? The BPPC does not provide a mechanism for this final step, and it is left up to the system that executes the document retrieval.

This represents a strength as well as a weakness of the BPPC. While it can support virtually any disclosure policy that can be written down, the BPPC in practice is limited to the set of policies that can be prenegotiated among the HIE's stakeholders. In other words, the flexibility of the BPPC also somewhat constrains its scalability. A policy that allows medical information to be accessed by physicians with a direct treatment relationship to the patient, for example, requires that the definition of "physicians with a direct treatment relationship to the patient" be understood and consistent across the various hospitals and practices within the HIE.

The BPPC is also limited to static policies, those that can be written down in advance. It cannot support dynamic exceptions to the predefined policies, such as a list of doctors who should or should not have access to a record. The granularity of the BPPC is limited to the document level; policies cannot apply to only certain subsets of documents. These issues may be addressed in future revisions of the profile.

The Healthcare Information Technology Standards Panel has endorsed the BPPC as one of the eight composite security and privacy standards in its Interoperability Specification Catalog. A number of electronic health record vendors and HIEs have already developed prototype implementations.

Access Control Matrix

An access control matrix can help develop policies and explore policy alternatives. In the simplified example here, different sensitivity classes of medical information are represented in columns, and the various functional roles are represented as rows. An "X" in a cell indicates that the policy grants access for the corresponding sensitivity class to the corresponding role.

Access Rights (Functional Role)	Type of Health Information (Sensitivity)			
	Sensitive Medical Information	Laboratory Results	Radiology Results	Immunization Data
Any clinician in an emergency, so long as appropriate "break-the-glass" provisions apply	X	X	X	X
The patient's primary care physician	X	X	X	X
Any physician with a treatment relationship to the patient		X	X	X

Planning for Consents in HIE

For those who are not ready to implement, designing for the BPPC can be a valuable part of the HIE planning process. This is because the profile requires an HIE to clearly delineate its privacy policies—to state them in plain language, number them, and identify which policies patients can explicitly accept or reject.

Furthermore, the BPPC encourages planners to think about consent as a document in the exchange, an asset that can be leveraged to provide more transparency and patient control in an HIE. Soliciting requirements for applications and interfaces to help collect and manage these consents should be part of the HIE planning process from the earliest stages. Finally, the BPPC profile draft suggests some techniques that can be used to help develop policies and explore policy alternatives. One of these techniques is to create an access control matrix based on functional roles and sensitivity classes.

Consider again the three sample policies mentioned previously. These policies describe three functional roles to which a particular class of medical information can be disclosed. For simplicity assume that emergency circumstances, which may involve additional "break-the-glass" policies, may modify the functional roles to which a clinician belongs. When illustrated in a matrix, as shown above, the policies can be easier to understand and supplement.

In the matrix, different sensitivity classes of medical information are represented in columns, and the various functional roles are represented as rows. A single policy, such as policy examples 1, 2, or 3 may involve a single cell or an entire column depending on the desired granularity of the policy. An "X" in a cell indicates that the policy grants access for the corresponding sensitivity class to the corresponding role. As shown, it can be easy to add additional types of health information to the matrix and explore the policy possibilities using this technique.

These examples are admittedly simplistic; real-world matrices will be much larger and more complex. Furthermore, roles and sensitivities represent just one dimension of access control policy. Other dimensions that could result in modifications to the matrix or additional matrices may include purpose of disclosure (whether it be for treatment, payment, research, or other purposes), timeframe of disclosure, the care setting, and the type of authentications. As mentioned, the BPPC is flexible, and there are endless possibilities.

The sooner that regional health information organizations and others that are developing HIEs begin to explore these possibilities, the better the policy will be in the end. More about IHE, the BPPC, and other profiles is available at www.ihe.net. ❖

Michael Berry (berrym@hln.com) is senior project manager and **Noam H. Arzt** (artz@hln.com) is president of HLN Consulting, LLC.