

U.S. Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Privacy and Security Tiger Team
Health Information Technology Policy Committee

Consumer Choice Technology Hearing

June 29, 2010
Washington, D.C.

InterSystems Corporation
Written Public Testimony
Michael LaRocca

Introduction

On June 29th, 2010, the HIT Policy Committee (HITPC) is hosting a technology hearing on consumer choice technology. A Privacy and Security Tiger Team has been assigned the task of analyzing how technology can be applied to the complex and sensitive issues surrounding patient privacy. Upon completing this analysis, the Tiger Team will provide specific recommendations to the HITPC, and ultimately to the Office of the National Coordinator for Health Information technology.

In advance of this hearing, the Tiger Team requested that vendor participants complete an 11-question survey. Those questions are:

1. Describe how the technology implements the patient's consent and the granular choices given to the patient.
2. How did your system adopt the approach it has taken to patient consent and what was the motivation for doing so?
3. How long has the technology been in use?
4. How do the providers who use your system handle granular consent? Does it alter the way they view a patient's health record when they receive it?
5. What are the advantages to your approach to obtaining patient consent?
6. Is the technology scalable so that small and medium-sized providers could implement it?
7. Is the consent technology interoperable with other systems? (i.e. can the patient's consent preferences be passed to other systems within an HIE?)
8. If the consent is not interoperable, what technological change would be needed to make it interoperable?
9. What resources are necessary to implement the consent system in its current form? What further resources would be necessary to offer increased granular consent choices?
10. How many systems or users are currently implementing or adopting this technology?
11. How many unique consumers are covered by the technology that is implementing the consumer choice system?

Each of these questions is answered within this written testimony.

Written Testimony

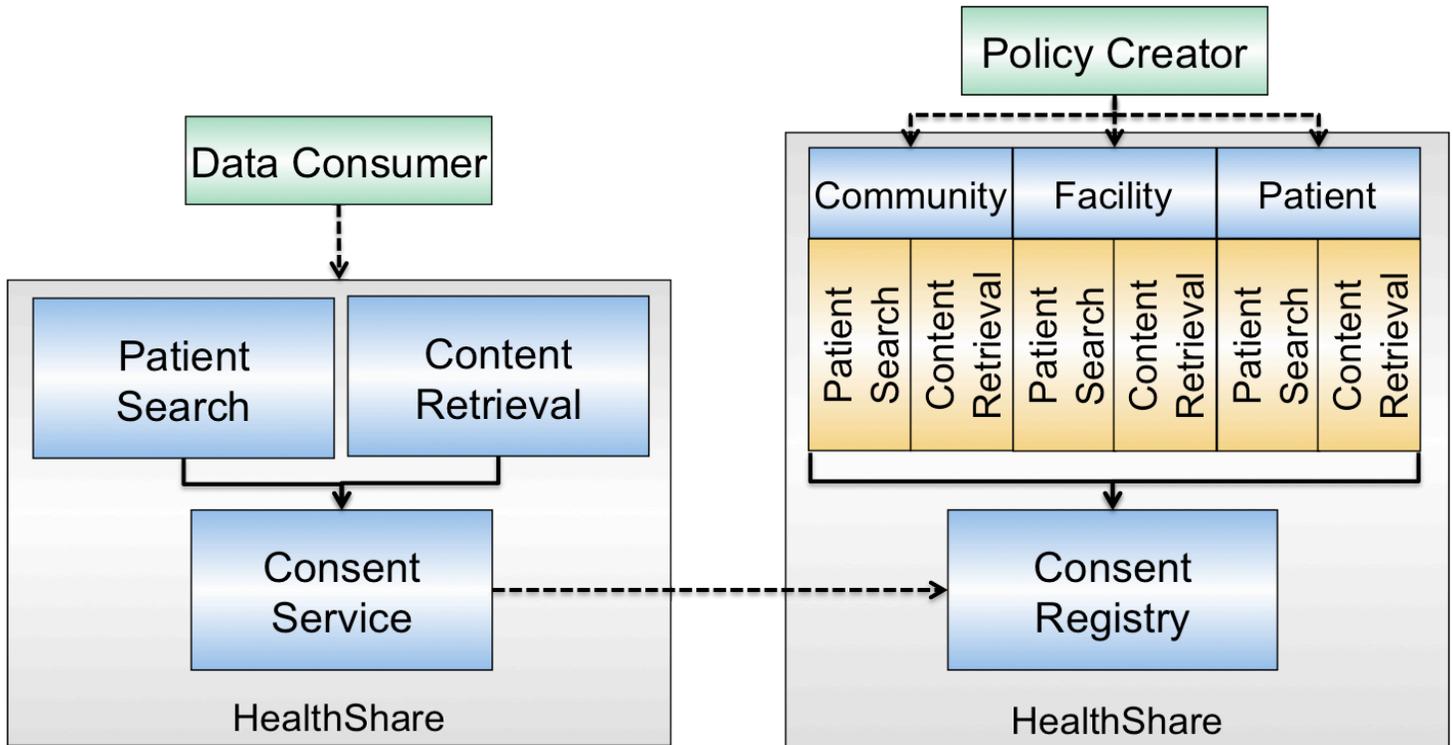
Question 1

Describe how the technology implements the patient's consent and the granular choices given to the patient.

Before describing how patient consent is handled, a short overview of HealthShare's consent framework should first be explained.

HealthShare Consent Framework

The following diagram depicts the high-level architecture employed by HealthShare's consent framework:



As depicted on the left-hand side of the image above, data consumers accessing Personal Health Information (PHI) are subject to verification of access by HealthShare's Consent Service; any unauthorized access to PHI will be blocked.

The HealthShare Consent Service obtains the privacy policy from a centralized Consent Registry, which is available to all nodes within the community. The Consent Registry contains policies that are created by one of 3 recognized entities in the exchange:

1. Community: the HIE itself, and ultimate authority regarding what content is permissible for exchange within their network
2. Facilities: the content sources within the HIE – such as hospitals, clinics, and primary care offices – which govern access to data they've contributed to the exchange
3. Patients: the individuals or subjects, who govern access to his or her PHI

Within each entity's consent policy, two filtering phases may be defined:

1. Patient Search: declares how identifiers and demographics requested by patient identity inquiries – those transactions traditionally associated with a Master Patient Index (MPI) – should be protected
2. Content Retrieval: declares how clinical information requested for an identified patient – such as a date range of results, a data type, or a coded value¹ – should be protected

HealthShare supports policy inheritance between the 3 recognized entities, where Community policies are inherited by each Facility, and Facility policies are inherited by Patients that have data at that particular facility. HealthShare applies priority to the different policy definitions such that the Patient may define privacy policies within the bounds established by the Facility and

¹ Consent filtering of coded values implies that terminology translation has been done during capture of source clinical data to put coded values into a "gold standard" for the community.

Community, and the Facility may define privacy policies within the bounds established by the Community. HealthShare utilizes object-orientation to support this functionality.

As both the Community and Facilities serve as consent authorities, each can define several behaviors to be inherited by subordinate entities:

Term	Action	Description
Always	Block	PHI is always hidden
	Block Except	PHI is always shared with a specified list of consent groups ²
	Show	PHI is always shared
	Show Except	PHI is always hidden from a specified list of consent groups
Default	Block	PHI is hidden, unless overridden in the subordinate policy
	Block Except	PHI is shared with a specified list of consent groups, unless overridden in the subordinate policy
	Show	PHI is shared, unless overridden in the subordinate policy
	Show Except	PHI is hidden from a specified list of consent groups, unless overridden in the subordinate policy

Before a data consumer may access PHI at run-time, the user must first authenticate. Upon successfully authenticating, one or more Security Roles and one or more Consent Groups are assigned to the requesting user's active session. Security Roles – such as “doctor”, “nurse”, or “administrator” – are evaluated by HealthShare's Authorization Service to see what tools the user may use³. Consent Groups – such as “Cardiologist at Good Health Hospital” or “Primary Care Physician at Manhattan Group Practice” – are instead evaluated by HealthShare's Consent Service to see what PHI the requesting user may access.

Consent Groups are designed to support organizations, departments, and individuals. For example, a consent group of “GoodHealthHospital.Cardiology.JohnSmith”⁴ allows a patient to define a consent filter based on any of the following:

- GoodHealthHospital.*: policy applies to all members of Good Health Hospital
- GoodHealthHospital.Cardiology.*: policy applies to all cardiologists within Good Health Hospital
- GoodHealthHospital.Cardiology.JohnSmith: policy applies to Cardiologist John Smith within Good Health Hospital

All consent policy definitions are stored in HealthShare's Consent Registry. When queried by the HealthShare Consent Service on behalf of a user, the Consent Registry returns a single, merged version of the various consent policies, after it's evaluated each entity's consent filters and has applied the proper policy inheritance rules. This run-time consent policy is what's evaluated by the Consent Service to determine what PHI may be shared or not for the requesting user.

If permitted by the run-time consent policy, the requesting user may “break the glass” in the case of an emergency, effectively overriding the filters defined in the consent policy. The use of such emergency access requires immediate attestation by the user, which is audited in HealthShare's Audit Repository.

In all cases, non-consented PHI is never transmitted over the network; that is, HealthShare components that manage the requested data will suppress any protected PHI from their response.

Finally, every consent filter defined within a policy may be tagged with an effective date range, and where applicable an event start and end time.

Answer

Specifically from a patient's point of view, he or she may define the following (subject to policy inheritance, as described above):

1. A first-phase consent filter, applied during the patient search interaction
 - a. Do I want the presence of information at a facility to be revealed?
 - b. Are there certain groups or users I'll enable to know this information, yet others not?
 - c. For what date range do I want this filter to be active?

² The term “consent group” is defined in the proceeding paragraph.

³ Note, this functionality is not discussed in detail within this written testimony.

⁴ The “cascading dot syntax” of a Consent Group name can have as many levels as needed for the project's implementation; the three-tier consent group used here is for example only.

2. A second-phase consent filter, applied during the content retrieval interaction
 - a. Do I want certain data types (such as free-text notes, allergies, or lab results) to be shared?
 - b. Do I want certain classes of information (such as HIV status, STDs, or genomic test results) to be shared?
 - c. Do I want to hide a particular date range of events?
 - d. Are there certain groups or users I'll enable to know this information, yet others not?
 - e. For what date range do I want this filter to be active?
3. Emergency access control
 - a. Do I want to allow clinicians to “break the glass” and override my consent policy in the event of an emergency?

Question 2

How did your system adopt the approach it has taken to patient consent and what was the motivation for doing so?

Answer

When we first entered into the HIE arena approximately 3 years ago, we discovered quickly that data collected and shared by HIE infrastructure was dynamic. At the time, the need to support dynamic content seemed to contradict the guidelines published by Integrating the Healthcare Enterprise (IHE), and among other things, this contradiction complicated how privacy and consent filters would be applied to data. We determined that the IHE profile called Basic Patient Privacy and Consent (BPPC) was too simplistic for our project requirements as it was strictly a “document-based” consent model, and so developed our own framework allowing us to suppress certain sensitive information before we generated the clinical document dynamically.

Question 3

How long has the technology been in use?

Answer

HealthShare was officially launched in 2007, and was available for field test that same year. Our first international customer (the Swedish National Government) went live with this technology in May 2009, and our first domestic customer (the Long Island Patient Information Exchange, or LIPIX) went live in December 2009.

Question 4

How do the providers who use your system handle granular consent? Does it alter the way they view a patient's health record when they receive it?

Answer

A provider accessing PHI must pass through two phases of consent filtering, as described above. Depending on the consent filter applied, that provider may see nothing, or some sub-set of the available PHI. In cases where a sub-set of the PHI was returned to the requesting provider, a text message appears on the screen indicating that some data was filtered out due to consent policy settings.

HealthShare intentionally does not state *what* data was suppressed so not to reveal that certain sensitive information, such as a positive STD result, exists in the patient's record.

Question 5

What are the advantages to your approach to obtaining patient consent?

Answer

While we're proud of our product capabilities in the area of privacy and consent, we recognize that the operational tasks surrounding the collection of consent policies from patients is burdensome and potentially confusing. When it comes to collecting policies from patients, there's always a need to balance simplicity with functionality.

With our approach, sites can start simple and add functionality incrementally. Typically, sites will start with either a simple opt-in or opt-out model, based purely on Patient Search consent filtering. In an opt-in deployment, the Community creates a Patient Search filter of DEFAULT SHOW, and allows patients to override it; inversely, in an opt-out deployment, the Community instead creates a Patient Search filter of DEFAULT BLOCK.

In time, sites may choose to offer Content Retrieval filtering to patients. In this case, sites create a library of Clinical Information Types, which themselves are a collection of rules that match clinical data to a type. For example, a type called “HIV Positive Status” could be created as follows:

- Diagnosis Code = 079.53, Diagnosis Code System = ICD 9
- Lab Result Order Code = 7917-8, Lab Result Order Code System = LOINC

- Medication Code = C0703903, Medication Code System = RxNorm

Once added to the library of Clinical Information Types, a patient (or community or facility for that matter) can then show or block any content that matches one of the rules within this type.

Since communities can pre-determine to what extent patients can configure their consent policies, they have full control over how simple or complicated the collection process will be. In any case, most of our projects tend to collect patient consent at registration time in one of two ways:

1. By collecting a paper form in the facility at which the patient presents
2. By asking questions verbally in the facility at which the patient presents

In either case, an authorized staff member of the facility enters the policy information using the default HealthShare Management Portal, a customized version of that portal, or a modified version of their registration system's registration screen.

In time, we believe patient portals designed to capture consent declarations is the best approach, but at present we don't offer our own portal to do so; instead, we offer a programmatic interface for managing consent policies that an external patient portal could leverage.

Finally, at any time, the patient could grant on-the-fly access to his or her data to the attending clinician. In this case, the clinician obtains the PHI through "emergency access", and attests that the patient (or proxy) gave verbal or written consent to access their information before doing so.

Question 6

Is the technology scalable so that small and medium-sized providers could implement it?

Answer

Yes, the technology is very scalable, and is designed to start small and end big. With a topic as complicated as consent, we expect sites to walk before they run, and offering an incremental adoption path is critical for success.

Question 7

Is the consent technology interoperable with other systems? (i.e. can the patient's consent preferences be passed to other systems within an HIE?)

Answer

Yes, consent policies are very interoperable with other systems. HealthShare offers three programmatic APIs for managing and/or accessing consent policies:

1. XDSb-based exchange of XACML documents
2. HL7v2-based exchange of CON segments⁵
3. SOAP-based exchange of HealthShare's proprietary format

What's most important here is that HealthShare's Consent Registry is a centralized database of policies, which may be accessed by any authorized system within the community, or across communities.

Question 8

If the consent is not interoperable, what technological change would be needed to make it interoperable?

Answer

HealthShare's consent model is interoperable today, but in our experience there is enough variation among vendor interpretations of XACML that custom implementation work is often needed to enable the integration with other vendor systems.

Question 9

What resources are necessary to implement the consent system in its current form? What further resources would be necessary to offer increased granular consent choices?

Answer

In general, to develop a workable privacy and consent model within a community, 4 key resources are needed:

1. A clinical expert to design the consent model deployed within the community
2. A systems implementer to create the core consent components, such as the Clinical Information Types, as well as any custom user interface for collecting the policy definitions
3. A terminology translation expert, to convert captured coded values into the community's "gold standard"
4. A data entry person, to enter consent policies captured on behalf of the patient

⁵ This is a pending feature, currently under development.

Question 10

How many systems or users are currently implementing or adopting this technology?

Answer

At present, 4 HealthShare communities are either live, or in acceptance test nearing their go-live date:

1. Sweden (NPO)
2. Long Island Patient Information Exchange (LIPIX)
3. Brooklyn Health Information Exchange (BHIX)
4. Health Information Exchange of New York (HIXNY)

The relevant statistics⁶ surrounding these 4 communities are as follows:

	Community	Active Users	Active Patients	State	Go-Live Date
1	Sweden	300	1,000,000	Live	May 2009
2	LIPIX	310	750,000	Live	December 2009
3	BHIX	40	2,500,000	Acceptance Test	July 2009
4	HIXNY	200	1,750,000	Acceptance Test	July 2009
Total		850	6,000,000		

Question 11

How many unique consumers are covered by the technology that is implementing the consumer choice system?

Answer

Please see the answer to question 10 above; the total number of unique consumers is indicated in the table above under the column "Active Patients".

⁶ Counts quoted here are approximate.