Basic Patient Privacy Consents (BPPC) provides a mechanism to record the patient privacy consent(s), a method to mark documents published to XDS with the patient privacy consent that was used to authorize the publication, and a method for XDS Consumers to use to enforce the privacy consent appropriate to the use.

Summary

Basic Patient Privacy Consents profile provide mechanisms to:

1. Record the patient privacy consent(s),
2. Mark documents published to XDS with the patient privacy consent that was used to authorize the publication,
3. Enforce the privacy consent appropriate to the use.

Benefits

An Affinity Domain can

- develop privacy policies,
- and implement them with role-based or other access control mechanisms supported by EHR systems.

A patient can

- Be made aware of an institutions privacy policies.
- Have an opportunity to selectively control access to their healthcare information.

Details

First: The Affinity Domain organizers create a set of policies. Each of the policies are each given an OID. This OID now is an Affinity Domain specific vocabulary. Each OID can clearly identify one of the policies defined by the HIE. There are examples of how one might build these policies in a way that allows the patient to select appropriately the type of sharing they agree to. This was important as it allows the Affinity Domain to define their own policies in as clear of language as was necessary for the patients, providers, and systems to understand. This level of policy writing is necessary before one can even hope to commit the logic to computer encoding.

Second: The BPPC profile shows how to capture a patient's acknowledgment and/or signature of one or more of these policies. This is captured using HL7 consent structure within an CDA document with optionally a scanned copy or optionally a digitally signature. The scanned copy might be the patient's ink on paper acknowledgment. This capability has been very well received as providers like to see that ink was put to paper. I suspect that this step will never be replaced. Patients have a need to know what they are consenting to. They can understand human text, but not many can understand computer logic.

Third: When a clinical document is published, the OIDs defined in the First step are used to label each document with the acceptable use (permissions, restrictions, obligations). The system actually supports multiple OIDs being attached to each document, so that multiple acceptable uses can be represented (something not allowed inside a CDA document). This confidentiality code is in XDS Metadata and thus can be applied to ANY type of document, not just CDA documents. Thus if a ECG is captured in a PDF file, it can be appropriately labeled with the acceptable uses.

Fourth: When a document is used, the metadata shows the acceptable use OIDs. The document consumer Actors are obligated to enforce this acceptable use. The document consumer Actor is required to block access to documents that don't have acceptable OIDs. Any OIDs that are not understood by the document consumer Actor must not be used.

Obligations

Possible things that the BPPC policies might include are not fully known at this time. The following is a list that has been discovered through use by researchers, health information exchanges, and vendors. The following are some thoughts of things that might be orchestrated by BPPC Policies.

General

1. Is the existence (metadata) about a document that can't be read by the user shown in a list of available documents for this patient
2. Map local role codes into some Affinity Domain defined role codes

Prior to publication

1. one site specific code to publish documents against
2. prompt user for the code to apply to the document (drop-down-list)
3. document-type based codes
4. validate that the code to be published against has been consented to
5. validate that a site specific code (opt-out) is NOT currently consented to.

Prior to allowing access to a document

1. should documents with unrecognized codes be shown?
2. prompt the user with some site defined text "do you really want to do this?"
3. allow the user to review the base consent policy
4. allow the user to review the patient's specific consent
5. allow the user to override a consent block (break-glass)
6. require that a new consent be acquired first
7. validate that a site specific code (opt-out) is NOT currently consented to.
8. validate that the code on the document has been consented to
9. Document can only be viewed, it can not be incorporated or copied.
10. use of this document shall result in an ATNA emergency access audit event
11. policy may demand that for deprecated documents, the confidentialityCode of the approved document be applied. (e.g. because the reason for deprecation could have been because a patient changed their consent).

Models It has also been suggested that documents should simply be published with the expected codes, and that only on use of a document is ALL current consent policies are evaluated against with the code on the document. In this way revocation is more dynamic. This model was not fully expressed in BPPC.

Possible Privacy Policies

BPPC can not support all forms of privacy policies. This is a list of potential policies.

It is fully expected that these policies would need to include very specific language around defining exactly what they mean. For example an Opt-In policy does not mean that any person has access, there would be well written rules about what types of structural and functional roles are allowed access under specific conditions and workflows. For example: This would make clear what access the dietary staff have to the information in order to properly prepare the food diet. It would outline what minimal information is provided to billing, and what allowances there are for system maintenance. It would include references to recourse and patient right to change or access. It would include conditions at which the normal access could be overridden by emergencies including safety to patient, safety to providers, safety to public, etc. Even the most simple policy must be spelled out in very exacting detail.

Supportable

1. Opt-In to clinical use
2. Opt-Out of sharing outside of local event use, allowing emergency override
3. Opt-Out of sharing outside of local event use, without emergency override
4. Specific document is marked as available in emergency situations
5. Additionally allow specific research project
6. Additionally allow specific documents to be used for specific research projects
7. Limit access to functional roles (eg: healthcare) (direct care) providers
8. Limit access to structural roles (eg: organizational) (radiologist, cardiologist, billing clerk)
9. multiple policies apply to each document
10. Change the consent policy (change from opt-in to opt-out)
11. Allow direct use of the document, but not allowed to re-publish
12. when the document is published on media using XDM
13. when the document is published point-to-point using XDR
14. when the document is retrieved across communities using XCA
15. individual policy for opt-in at each clinic
16. individual policy for opt-in for a PHR choice (choosing from all possible PHRs - HIMSS 2008)

Possible

These might be possible depending on complex additional services that are not known at this time.

1. Allow access only to care providers with a direct treatment relationship
2. Spouse not allowed access (to all or specific document)
3. Parent is not allowed access (to all or specific document)
4. Restrict access to a specified care-setting
5. All accesses to the data will result in a notification of the patient (eg: email or such)
6. All accesses to the data require that a new consent be captured (eg: capture new signature)
7. when HL7 v2 or v3 messages are used. This would require further profiling of the use of confidentialityCode in those messages.
8. when DICOM is used. This would require further profiling of the use of confidentialityCode in those messages.

9. temporarily allowing a use of a document that would be not allowed by the current policies. This could be done with a new consent being registered that is soon after deprecated, but this is not very good solution.

Not Possible

1. Patient identifies individuals that have rights to their data
2. Patient identifies individuals that do not have rights to their data
3. Each access of the data must be individually authorized by the patient
4. a document with a mixture of more/less sensitive information thus needing different levels of protection
5. Notification to those that have used a document under consent that is now revoked
6. pulling back copies of documents that have been used under a consent that is now revoked

Systems Affected

All systems publishing or using XDS. Also may apply to XDR and XDP.

- EHR System
- PACS System
- EMR System
- Cardiology
- PHR
- etc...

Future

The BPPC profile is very clearly "Basic" because we know that there is many gaps in what we can do vs what is desired.

Advanced Consents

HL7 is working hard to define a vocabulary that can be used to capture consents in computer processible form. The following is the information related to the consent work that has been done or is in progress under the umbrella of HL7:

- Data Consent Release-1 Specification.
- Data Consent Draft Release-2 Specification: Composite Privacy Consent Directive

This should also look at combinatorial logic where multiple policies may apply, and where mixture of policies apply to different parts of the document/message.

Protecting more than Documents

The same confidentialityCode mechanism that BPPC sets up for XDS Metadata can be used in HL7 messages and DICOM transactions. In both cases there is already a confidentialityCode that is defined for this purpose. The important part is to have a policy domain declare that the confidentialityCode is constrained to a specific vocabulary and that this vocabulary must be enforced.

Specification

Profile Status: Final Text

Documents: IHE IT Infrastructure Technical Framework Version 5 or later

- Vol. 1 - Section 17
- Vol. 2 - Sections 5.1

Underlying Standards:

- HL7 CDA Release 2.0 (denoted HL7 CDA R2, or just CDA, in subsequent text)