

Basic Patient Privacy Consents

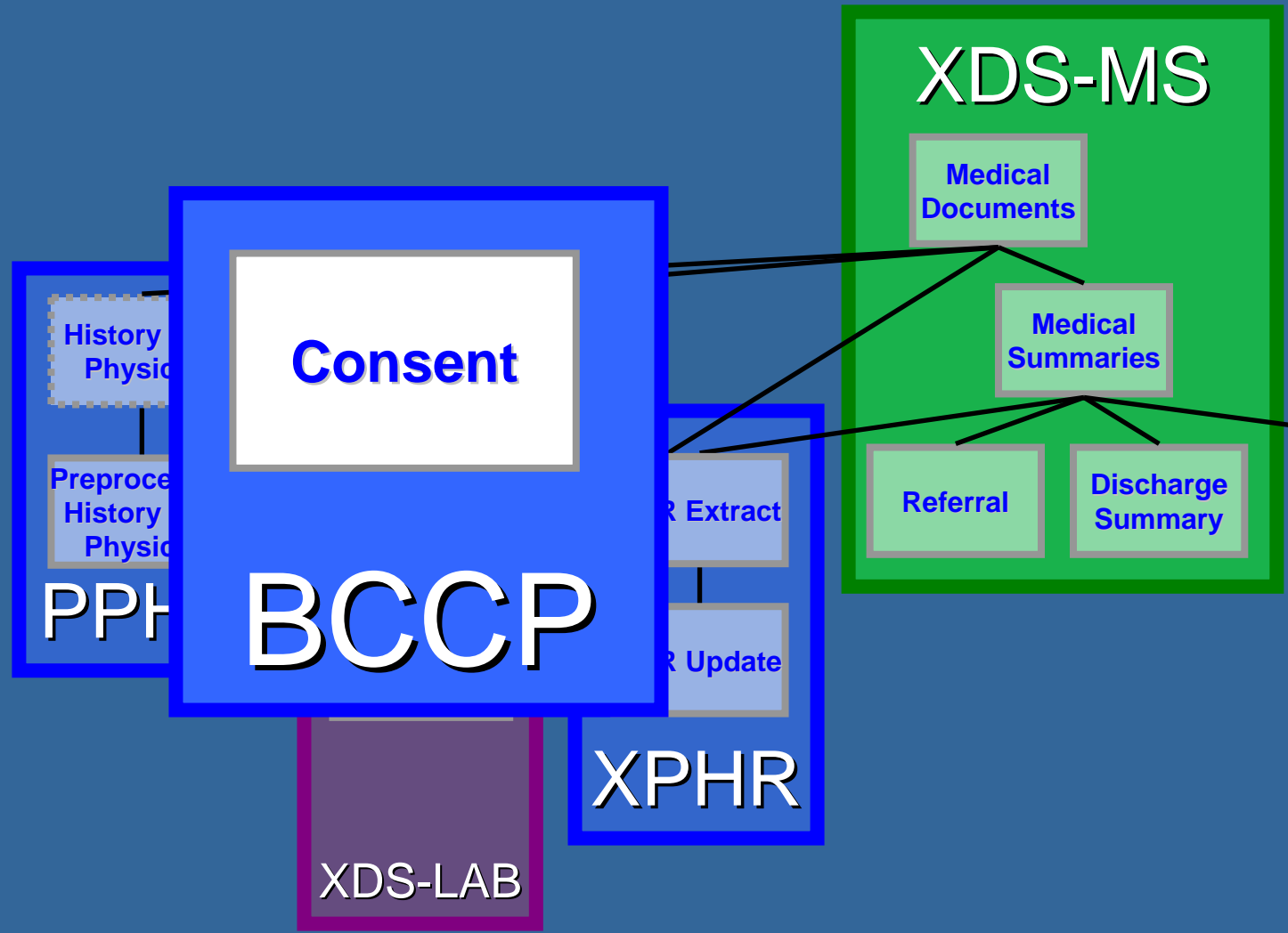
IHE Educational Workshop 2007

John Moehrke

Lori Forquet



Basic Patient Privacy Consents



What do Standards Define?

● Policy

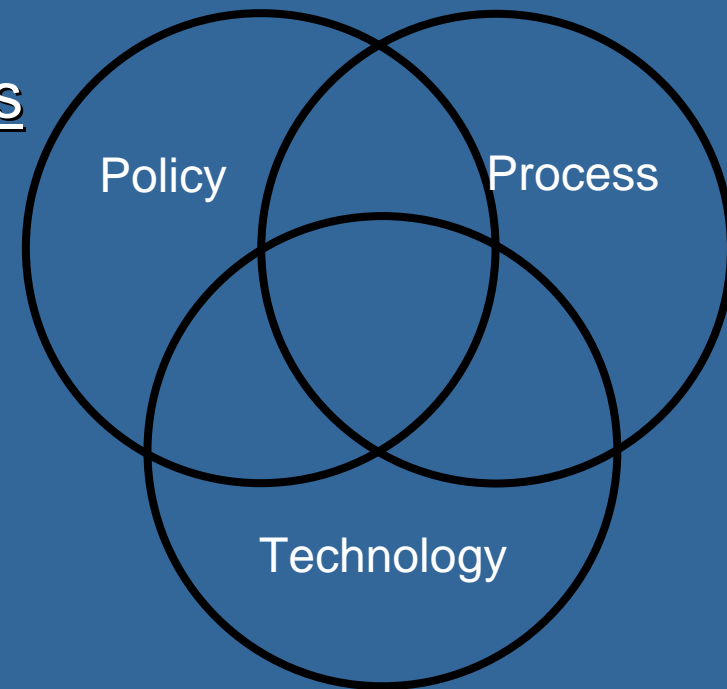
- Driven by business goals
- Informed by Risk Assessments
- Defines rights and responsibilities
- Defines punishment

● Process

- Enforces policy
- How people or organizations act
- who / what / where / when / how

● Technology

- Enforces policy
- How equipment should act
- Algorithms and data formats



Before

- **One Policy for the Affinity Domain**
- **Patient doesn't agree → Don't publish**
- **VIP Patient → Don't publish**
- **Sensitive Data → Don't publish**
- **Research Use → No Access**

Basic Patient Privacy Consents

- **Small number of pre-coordinated Affinity Domain Privacy Consent**
 - Patient can choose which ones to agree to
- **Data is classified and published under the authority of a specific Privacy Consent**
- **Data is used in conformance with original Privacy Consent**
- **Applicable for XD* mechanism**

Abstract

The Basic Patient Privacy Consents (BPPC) profile provide mechanisms to:

- Record the patient privacy consent(s),
- Mark documents published to XDS/XDR/XDM with the patient privacy consent(s) that was used to authorize the publication,
- Enforce the privacy consent(s) appropriate to the use.

XD* OPTIONS

- **XDS Document Source**
- **XDS Document Consumer**
- **XDR Document Source**
- **XDR Document Recipient**
- **XDM Document Sources**
- **XDM Document Receivers**

- **Nothing new for XDS Registry and Repository**

Key Technical Properties

- **Human Readable**
- **Machine Processable**
- **Supports standards-based Access Controls**
- **Multiple Consent Types and Documents (e.g., HIPAA)**
 - Opt-in or Opt-out
 - Implicit or Explicit
 - Time Limited
- **Wet Signature Capture (i.e. XDS-SD)**
- **Digital Signature Capture Possible (i.e. DSG)**
 - Provider, Witness, Patient or Legal Representative
- **Extensible**

Value Proposition

- **An Affinity Domain (RHIO, HIE)**

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

- **A patient can**

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

Standards and Profiles Used

- **CDA Release 2.0**
- **XDS Scanned Documents**
- **Document Digital Signature**
- **Cross Enterprise Document Sharing**
- **Cross Enterprise Sharing on Media**
- **Cross Enterprise Sharing with Reliable Messaging**

Deeper Dive



Value Proposition

● An Affinity Domain (RHIO, HIE)

- develop a set of privacy policies. For Example:
 - No HIE use allowed (e.g. Opt-Out)
 - All clinical use (e.g. Opt-In)
 - Restricted to Assigned Clinician + Emergency Mode
 - Emergency Data Set
 - De-Identified document
- Each policy is given a number (OID)
- implement them with role-based or other access control mechanisms supported by EHR systems.

Capturing the Patient Consent act

- **One of the Affinity Domain Consent policies**
- **CDA document captures the act of signing**
 - Effective time (Start and Sunset)
 - XDS-SD – Capture of wet signature from paper
 - DSIG – Digital Signature (Patient, Guardian, Clerk, System)
- **XDS Metadata**
 - templateId – BPPC document
 - eventCodeList – the list of the identifiers of the AF policies
 - confidentialityCode – could mark this document as sensitive

Consent document

XDS Metadata:

Consent Document
Digital Signature

XDS-MS + XDS-BPPC + XDS-SD

Structured and Coded CDA Header

Patient, Author, Authenticator, Institution,
Time of Service, etc.

Structured Content with coded sections:

- Scanned Document details
- Privacy Consent details
 - Policy 9.8.7.6.5.4.3.2.1

Base64 encoded

Sample consent: by A Patient. It's OK



IHE-DSG – Digital Signature
Signature value
Pointer to Consent document

Marking all XDS Documents

- **Use Affinity Domain well formed vocabulary**
- **Indicated in XDS Metadata – confidentialityCode**
 - List of appropriate-use consents
 - OR logic
- **Registry rejects non-conformant confidentialityCodes**
- **Affinity Domain Policy must indicate rules for publishing documents with codes for which the patient has not specifically consented to.**

Using documents

● XDS Registry Stored Query Transaction

- Consumer may request documents with specific policies → Filtered response

● XDS Consumer Actor

- Informed about confidentialityCodes -- Metadata
- Knows the user, patient, setting, intention, urgency, etc.
- Enforces Access Controls (RBAC) according to confidentiality codes
- No access given to documents marked with unknown confidentiality codes

XDR & XDM

- **XDR & XDM Same responsibilities**
- **Should include copy of relevant Consents**
- **Importer needs to coerce the confidentiality codes**
- **Need to recognize that in transit the document set may have been used in ways inconsistent (e.g. Physical Access Controls)**

Examples





Questions?

