

# Basic Patient Privacy Consents

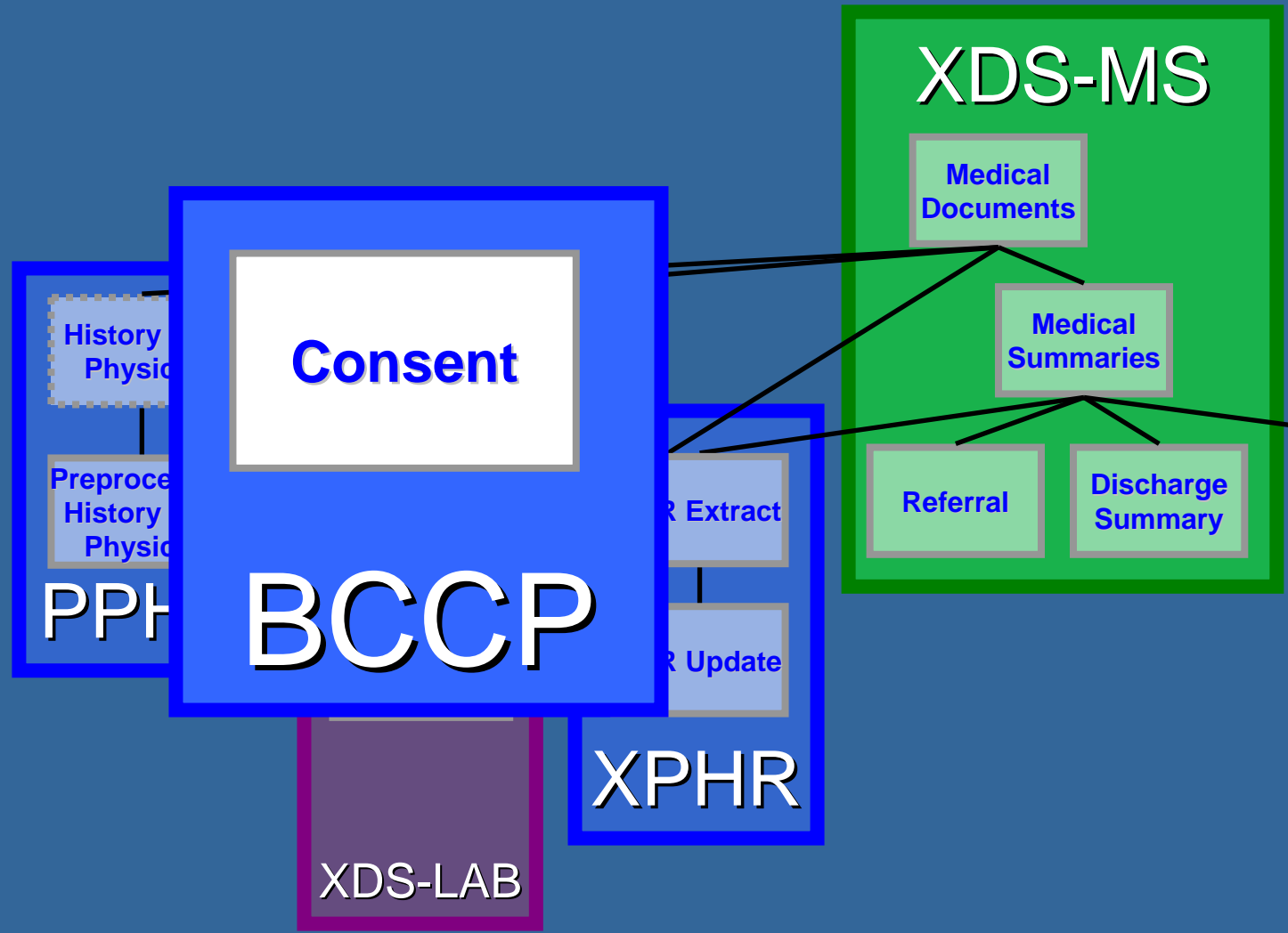
**IHE Educational Workshop 2007**

**John Moehrke    GE Healthcare**

**Lori Fourquet    e-HealthSign LLC**



# Basic Patient Privacy Consents



# What do Standards Define?

## ● Policy

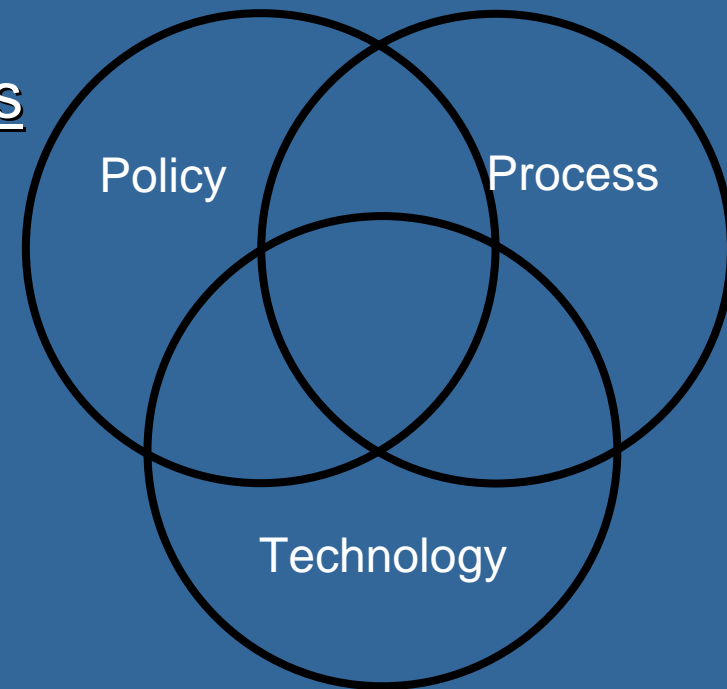
- Driven by business goals
- Informed by Risk Assessments
- Defines rights and responsibilities
- Defines punishment

## ● 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**

# Informed by Privacy Policy Standards

- **ISO IS22857 Trans-border Flow of Health Information**
- **ISO TS 26000 Privilege Management and Access Control (Parts 1, 2, draft 3)**
- **ASTM E1986 Standard Guide for Information Access Privileges to Health Information**



# 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)
  - templateID – BPPC document
  - XDS-SD – Capture of wet signature from paper
  - DSIG – Digital Signature (Patient, Guardian, Clerk, System)
- **XDS Metadata**
  - classCode – 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



# Sample: HIMSS Privacy Demo

## ● Normal sharing

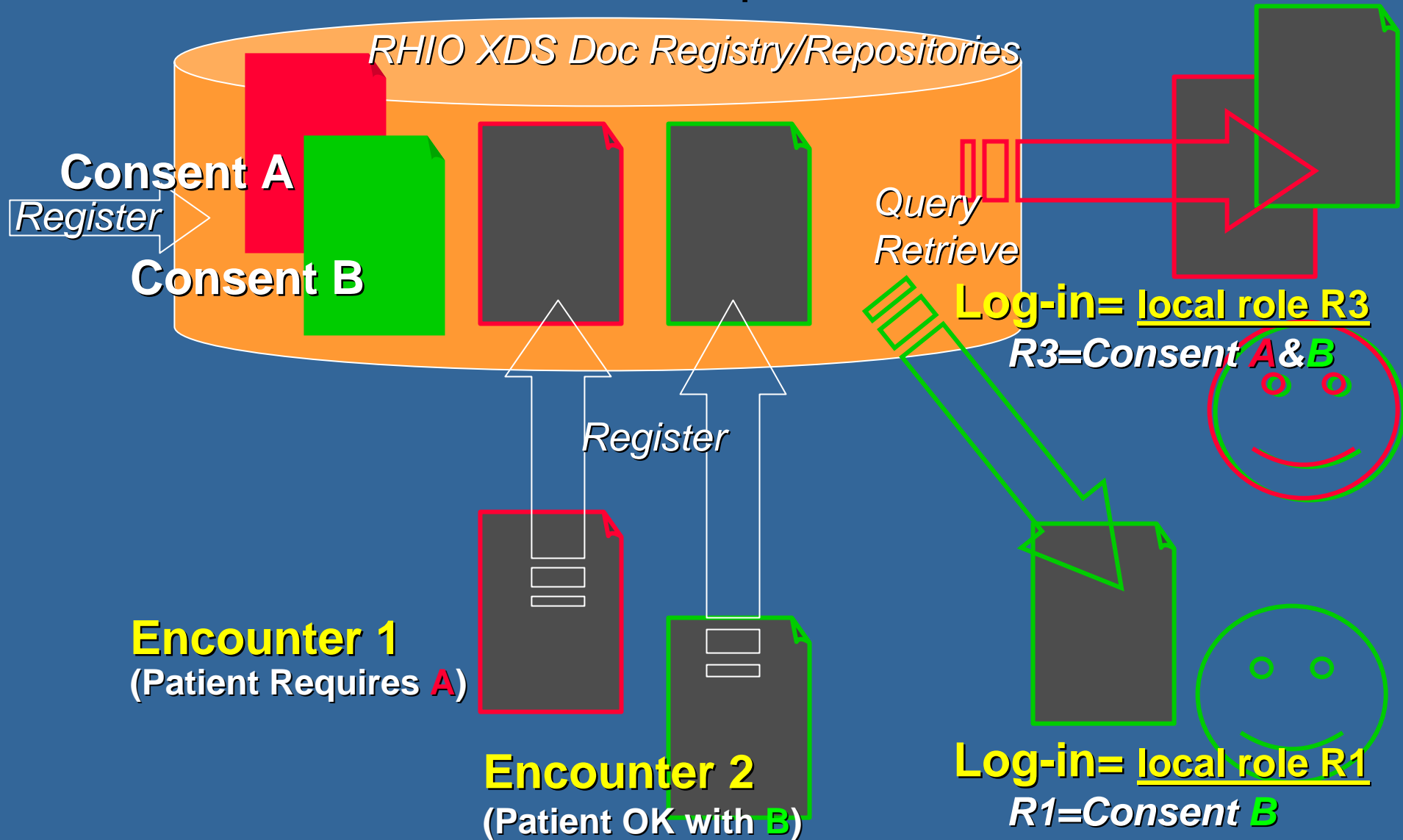
- treatment, operations, and billing.
- The normal sharing policy is implicit and does not need to exist prior to publication of documents
- OID-A = 1.3.6.1.4.1.21367.2006.7.107

## ● Sensitive topic

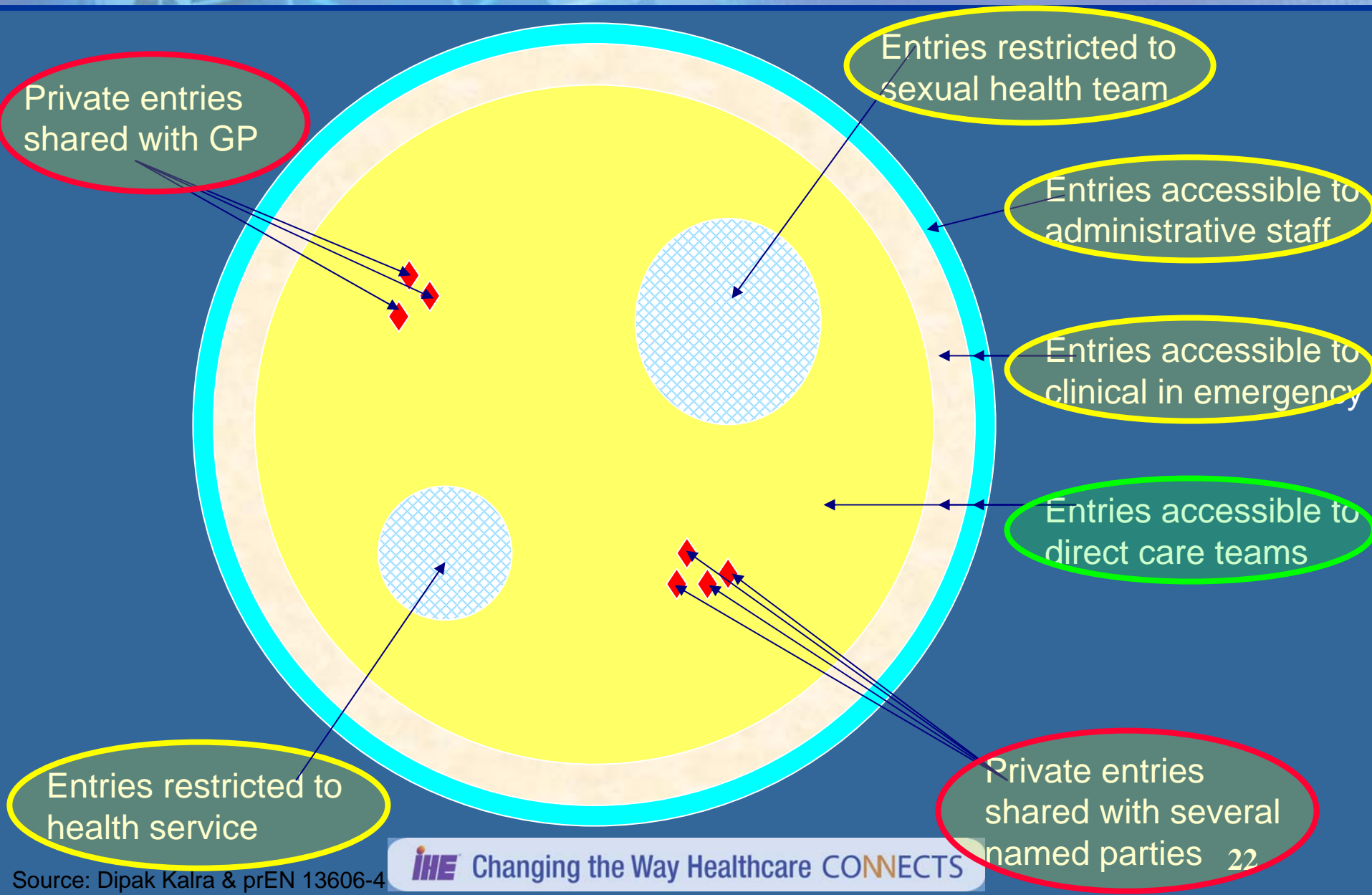
- (e.g. HIV tests, and victims of domestic violence)
- restricted sharing for treatment operations and billing.
- Emergency override is allowed in cases with serious threat to patient safety, emergency override audit logging must be done.
- OID-B = 1.3.6.1.4.1.21367.2006.7.109

# Basic Patient Privacy Consents

## Example



# Sensitive Document Accessibility

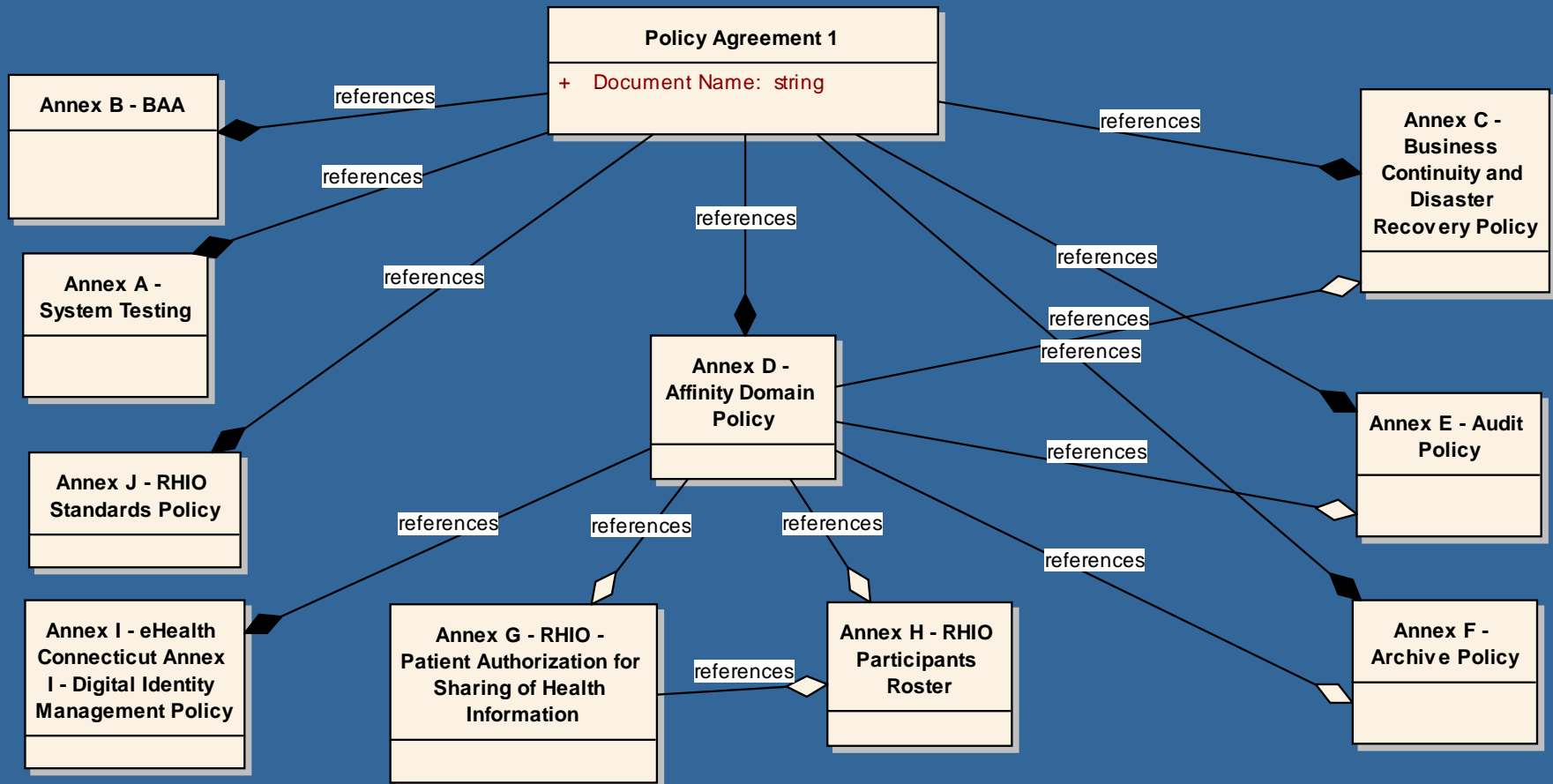


# eHealthConnecticut

## Policy Agreement Interoperability and Standards Document Map

Example: using ISO TS26000 Health Informatics PMAC- Part 1 Overview and Policy Management

cd Class Model



# eHealthConnecticut

## Operational Policies

### Content Dependent Upon Service Provision

- Annex A – System Implementation
  - *This document describes the system process and testing requirements for RHIO participants both for implementation and routine monitoring.*
- Annex C - Business Continuity & Disaster Recovery Plan
  - *This document describes the responsibilities and processes to protect business continuity in the event of system availability issues or failures*
- Annex E – Audit Policy
  - *This document describes the audit requirements for RHIO participants including retention times, investigation support, and routine monitoring.*
- Annex F – Archive Policy
  - *This document describes archival requirements for RHIO participants.*
- Annex H – Participants Roster

# eHealthConnecticut

## Policy Documents

- **Policy Agreement**
  - *Legal Umbrella Document*
- **Annex B – BAA**
- **Annex D - Interoperability Policy**
  - *This document describes the interoperability requirements and specifications including standard content, identification schemes, vocabularies, actors and transactions supported by the RHIO and required of RHIO participants*
- **Annex G – RHIO Patient Authorization for Sharing of Health Information**
  - This document serves as a common patient authorization for access to and disclosure of health information, and is aligned with system information access management configuration.

## Policy for Sensitivity Classification

- **RHIO-wide specification for classification of sensitive data**
- **CEN/ISO Standards-based Sensitivity What defines**
  - Care Management data that is accessible administrative staff
  - Clinical Management data that is accessible to health related professionals
  - Clinical Care data that is accessible to Healthcare professionals
  - Privileged care that is accessible to privileged health professional
  - Personal Care data that is accessible to personal health professionals

# eHealthConnecticut

## Sensitivity classes

- **Care Management**
  - Patient admission, clerk, billing
- **Clinical Management**
  - Technicians, lab,
- **Clinical Care**
  - Direct and indirect care
- **Privileged Care**
  - Mental Health, Substance Abuse, AIDS
- **Personal care**
  - Patient directed blocks

## Functional Role

- **Subject of Care**
- **Subject of care agent**
- **Personal health professional**
  - Named by patient
- **Privileged health professional**
  - Role specific
- **Health-related professional**
  - technician
- **Administrator**
  - clerk

# eHealthConnecticut

## Provide **Authorization** to Access History

Standards-based expression to enable automated processing

- **which data** – Standards-based **Sensitivity**
  - Care Management (e.g. administrative staff)
  - Clinical Management (e.g. radiology staff)
  - Clinical Care (e.g. most clinical staff)
  - Privileged care (Mental Health, HIV...)
  - Personal Care (abortion, substance abuse...)
- **to whom** – Standards-based **Functional Role**
  - Subject of Care
  - Subject of Care Agent
  - Personal Healthcare Professional
  - Privileged Healthcare Professional
  - Healthcare Professional
  - Health-related Professional
  - Administrator
- **for what purpose** (***HIE Policy is to restrict all use to clinical care purposes***)
  - At the request of the individual (no purpose need be specified)
  - Insurance Eligibility/Benefits  Marketing
  - Additional Medical Care  Research
  - Teaching

# Consent Matrix

	Care Mgmt	Clinical Mgmt	Clinical Care	Privileged Care	Personal Care
Subject of Care	Yes	Yes	Yes	Yes	Yes
Subject of Care Agent	Yes	Yes	Yes	Yes	Yes
Personal Health Professional	Yes	Yes	Yes	Yes	Yes
Privileged Health Prof	Yes	Yes	Yes	Yes	Yes
Health Prof	Yes	Yes	Yes	Special	Special
Health-Related Prof	Yes	Yes	Yes	Special	No
Administrator	Yes	Yes	Special	No	No

# eHealthConnecticut

Treatment allowed uses are enforced through typical role-based-access referencing functional role

A Policy Table shows allowed use between sensitivity classes vs functional role

Some table entries include special behaviors

- Healthcare Professional needs to get a consent-to-disclose on each publication and/or use of Privileged Care and Personal Care sensitivity classes
- Personal care sensitivity class data when accessed by a healthcare professional requires the review the patient's published consent.

# Active Consents Centric

- All clinical documents are published with subset of confidentiality codes, indicating the type of data only, not the status of consent at the moment.
- Consent acts are captured and managed as indicated. Including replacement, and time constraints
- On USE, the Document Consumer is responsible for pulling down all current consent document, and treating the clinical documents according to current consent documents

# Not currently available

- **Lab results that shouldn't be disclosed to the patient until they are consulted to by their GP.**
  - Could be supported with xds-metadata change transaction
- **Patient block for specified individual**
  - Could be through required viewing by the human user of current patient consent policy, with human enforcement
  - Future policies may be machine processable
- **Patient authorization of specified agent**
  - Could be through required viewing by the human user of current patient consent policy, with human enforcement
  - Future policies may be machine processable



Questions?

