



# Security and Privacy Overview

## Part 2 of 2 – Access Control

**IHE IT Infrastructure Planning Committee**

**John Moehrke – GE Healthcare**



What IHE Delivers

# Agenda

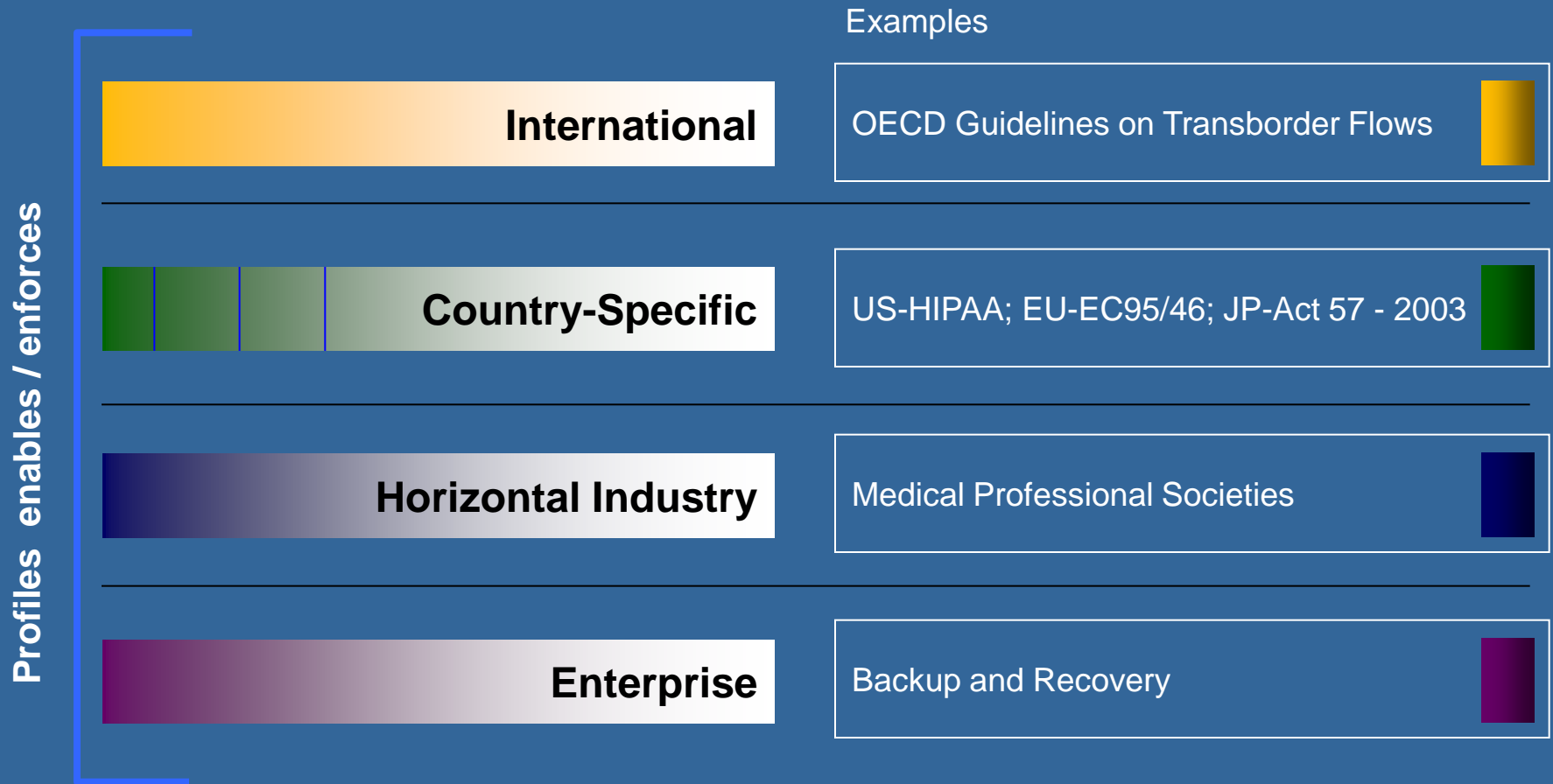
## Part 1

- Overall Security and Privacy controls
- Consistent Time (CT)
- Audit Trails and Node Authentication (ATNA)
- Enterprise User Authentication (EUA)
- Cross-Enterprise User Assertion (XUA)

## Part 2

- Document Digital Signature (DSG)
- Basic Patient Privacy Consents (BPPC)
- Access Control
- Gaps
- Conclusion

# Layers of Policies



# Profiles mapped to Security & Privacy Controls

Security & Privacy Controls		Audit Log	Authentication and Identification	Data Access Control	Secrecy	Data Integrity	Non-Repudiation	Patient Privacy
IHE Profile	Profile Issued							
Audit Trails and Node Authentication	2004	√	√	√	√	√	√	√
Consistent Time	2003	√	.				√	
Enterprise User Authentication	2003		√	.			.	.
Cross-Enterprise User Assertion	2006		√	.			.	.
Basic Patient Privacy Consents	2006			.				√
Personnel White Pages	2004		√	√			.	
Healthcare Provider Directory	2010		√	.			.	
Document Digital Signature	2005		√			√	√	
Document Encryption (in development)	2011			√	√	.		



# DSG

## Document Digital Signatures

# Document Signature Introduction

- **Provide a way to Digitally Sign a document**
- **Support XDS, XDM, XDR, and XCA**
  - May be used elsewhere
- **Support Non-Repudiation usecases**
- **Support Document Integrity**
- **Provide strong evidence of: Authorship, Approval, Review, and Authentication**
- **Allows Documents to be accessed independent of access to digital signature**
- **Support Multiple Signatures – counter and cosigned**

# Document Content Profile

## XDS Metadata

**Digital Signature is recorded like any other document**

- ClassCode = Digital Signature
- formatCode = xmldsig
- eventCodeList = sig purpose
- Transform = signs

## Signature Document

**W3C XML Signature**

**XadES profile**

- credentials,
- timestamp,
- Purpose of Signature
- Manifest of signed documents
- Signed documents stored independently (e.g. XDS)

# Document Signature Purpose

## Purpose of Signature (ASTM E1762 )

- “Author” - Author’s signature,
- “Author.Co” - Coauthor’s signature
- “Participant” - Co-participant’s signature
- “Transcriptionist/Recorder”
- “Verification” - Verification signature
- “Validation” - Validation signature
- “Consent” - Consent signature
- “Witness” - Witness signature
- “Witness.Event” - Event witness signature
- “Witness.Identity” - Identity witness signature such as a Notary
- “Witness.Consent” - Consent witness signature
- “Interpreter”
- “Review” - Review signature
- “Source” - Source signature
- “Addendum” - Addendum signature
- Administrative
- Timestamp

# Document signature + signed

## Original Document

Doc ID: 1.2.3.3  
 ClassCode: xphr  
 ...  
 Association :  
 Signed

## Signature Document

Doc ID: 1.2.3.4  
 ClassCode: d-sig  
 typeCode: E1762  
 ...  
 Association: signs

XDS  
 Metadata

I swear by Apollo the Physician and Aesculapius and Hygieia and Panacea and all the gods, and goddesses, making them my witnesses, that I will fulfill according to my ability and judgment this oath and this covenant: To hold him who has taught me this art as equal to my parents and to live my life in partnership with him, and if he is in need of money to give him a share of mine, and to regard his offspring as equal to my brothers in male lineage and to teach them this art—if they desire to learn it—without fee and covenant; to give a share of precepts and oral instruction and all the other learning to my sons and to the sons of him who has instructed me and to pupils who have signed the covenant and have taken the oath according to medical law, but to no one else.

I will apply dietetic measures for the benefit of the sick according to my ability and judgment; I will keep them from harm and injustice.

I will neither give a deadly drug to anybody if asked for it, nor will I make a suggestion to this effect. In purity and holiness I will guard my life and my art.

I will not use the knife, not even on sufferers from stone, but will withdraw in favor of such men as are engaged in this work.

Whatever houses I may visit, I will come for the benefit of the sick, remaining free of all intentional injustice, of all mischief and in particular of sexual relations with both female and male persons, be they free or slaves.

What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of man, which on no account one must spread abroad, I will keep myself holding such things shameful to be spoken about.

If I fulfill this oath and do not violate it, may it be granted to me to enjoy life and art, being honoured with fame among all men for all time to come; if I transgress it and swear falsely, may the opposite of all this be my lot.

Hash coded

```
<Signature Id="signatureOID" xmlns=http://www.w3.org/2000/09/xmldsig#
xmlns:xad="http://uri.etsi.org/01903/v1.1.1#">
<SignedInfo>
  <CanonicalizationMethod
    Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-
20010315#WithComments"/>
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
  <SignedInfo>
  <SignatureValue>base64SignatureValue</SignatureValue>
  <KeyInfo>
  <X509Data>
  <X509Certificate>base64X509certificate<X509Certificate>
  </X509Data>
  <KeyInfo>
  <Object>
  <xad:QualifyingProperties>
  <xad:SignedProperties>
  ....
  </SignedProperties>
  </QualifyingProperties>
  <SignatureProperties>
  <SignatureProperty Id="purposeOfSignature" target="signatureOID" >
  code</SignatureProperty>
  </SignatureProperties>
  <Manifest Id="IHEManifest">
  <Reference URI="urn:oid:1.2.840.97869786987.434536543"> <!--
document A-->
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>base64DigestValue</DigestValue>
  </Reference>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>base64DigestValue</DigestValue>
  </DigestMethod>
  </Reference>
  </Manifest>
  </Object>
</Signature>
```



Who?  
 When?  
 Why?



# BPPC

## Basic Patient Privacy Consent

# Problem

- In a cross-enterprise or cross-community environment how are the Privacy Preferences of the Patient (Consumer) made known and thus enforced?
- Consent is given and retracted
- Consent in some environments is only for a specific time
- There may be many consents relevant to different organizations or situations
- Need to support Privacy Policies beyond consent, such as authorizing research access

**The BPPC Solution is only BASIC, advanced consents not supported**

# How does it work? (1 of 3)

## A Patient Privacy Policy Domain (e.g. XDS Affinity Domain)

- **Develop “Patient Privacy Policies”,**
  - E.g. Opt-In, Opt-Out-fully, Opt-Out-Safe, No-Publish
- **Assign each “Patient Privacy Policy” a Privacy Domain wide unique identifier – “Patient Privacy Policy Identifier”**
- **Configure Access Control engines to recognize these “Patient Privacy Policies” with the rules necessary to enforce them**
- **Define the default rule that is used when no consent is found for a given Patient**

# How does it work? (2 of 3)

## Capture a Patient consent

- **Inform the patient about the available “Patient Privacy Policies” that they can chose from (Acknowledge)**
- **A “Patient Privacy Policy Acknowledgement Document” is created identifying that the patient has agreed to the policy or policies (a type of CDA document)**
  - May include a scanned image – such as a scan of the patient ink-on-paper signature on a replica printed version of the same policy
  - May be digitally signed – such as by the clerk witnessing the consent
  - May be time-limited
- **The “Patient Privacy Policy Acknowledgement Document” is made available using same mechanism as is used for clinical documents in that Privacy Domain (e.g., XDS)**
  - eventCodeList – holds the “Patient Privacy Policy Identifiers”

# How does it work? (3 of 3)

## Access Controls enforce consent

- Assumes Access Control is implemented with sufficient ability to enforce any Patient Privacy Policy allowed by the Patient Privacy Domain
- Can Leverage any interoperability profile in use: ATNA, EUA, XUA, PWP and metadata (e.g. confidentialityCode)
- Can Leverage application functionality such as Break-Glass
- XDS Query on Patient ID for BPPC type documents
  - If zero results returned – use default rule
  - Else for each result returned validate entry startTime and stopTime (to eliminate expired consents)
  - Use configured logic for remaining using eventCodeList as the list of acknowledged “Patient Privacy Policy Identifiers”

# Standards and Profiles Used

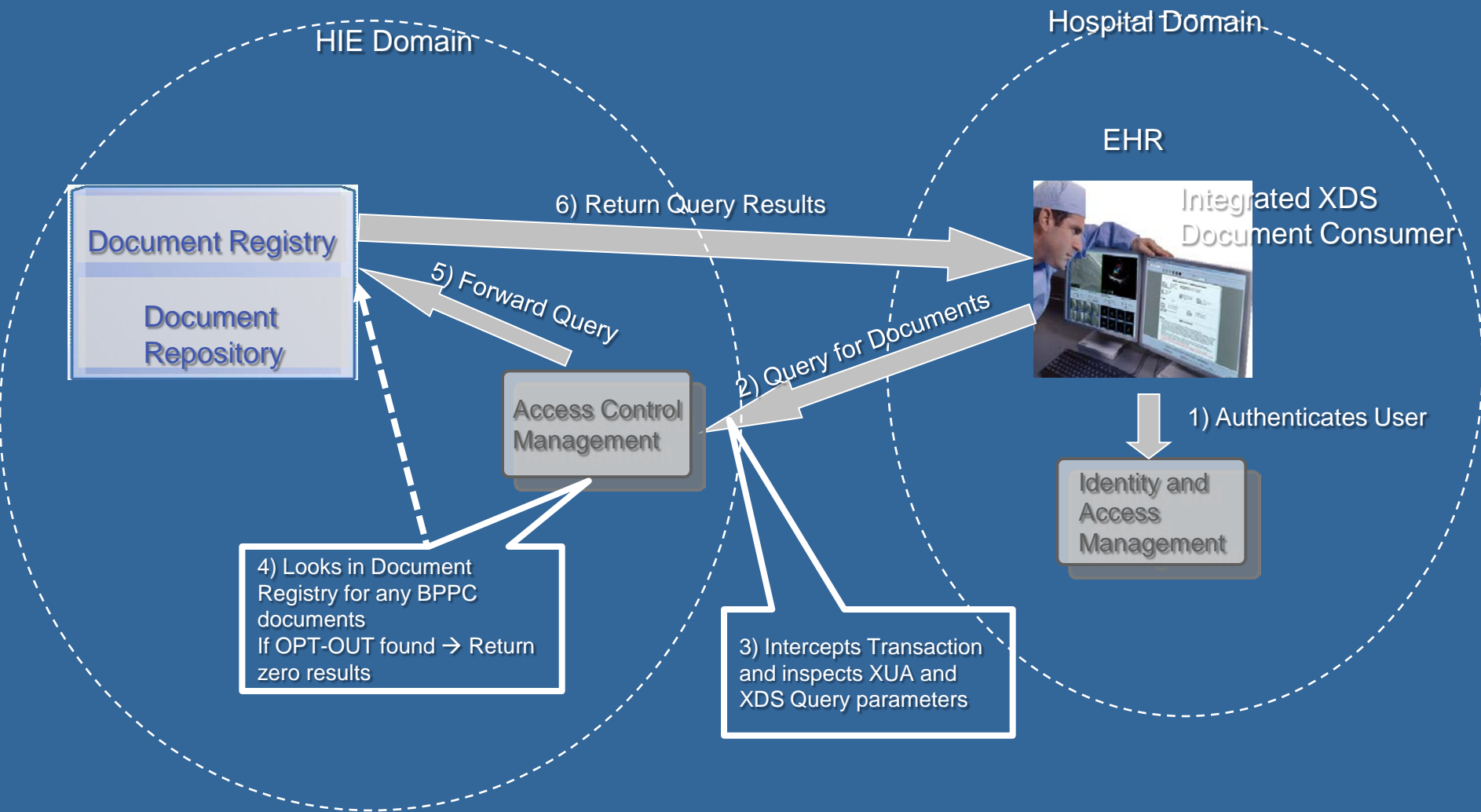
## ● Key Properties

- Support Human Readable Consents
- Support Machine Processable Access Controls
- Support for standards-based Role-Based Access Control

## ● Standards

- CDA Release 2.0
- XDS Scanned Documents
- Document Digital Signature
- Cross Enterprise Document Sharing (XDS, XDR, and XDM)
- Cross Community Access (XCA)

# Enforcing BPPC OPT-OUT at the HIE



# BPPC Enables

- **Basic Opt-In or Basic Opt-Out**
- **Specific cases → authorize a specific use**
- **Control Use or Publication**
  - Existence of Opt-Out could forbid publication
  - Typically Normal data is always published and control is on use of the data
- **Time based Consent → Episodic Consent**
- **Site specific Consent**

# BPPC: References

- **Status: Final Text**
- **IHE ITI Technical Framework**
  - Vol 1: Section 19
  - Vol 3: Section 5.1
  - Options added to other transactions
    - Vol 2a: Section 3.18
    - Vol 2b: Section 3.32, 3.41, 3.42, 3.43



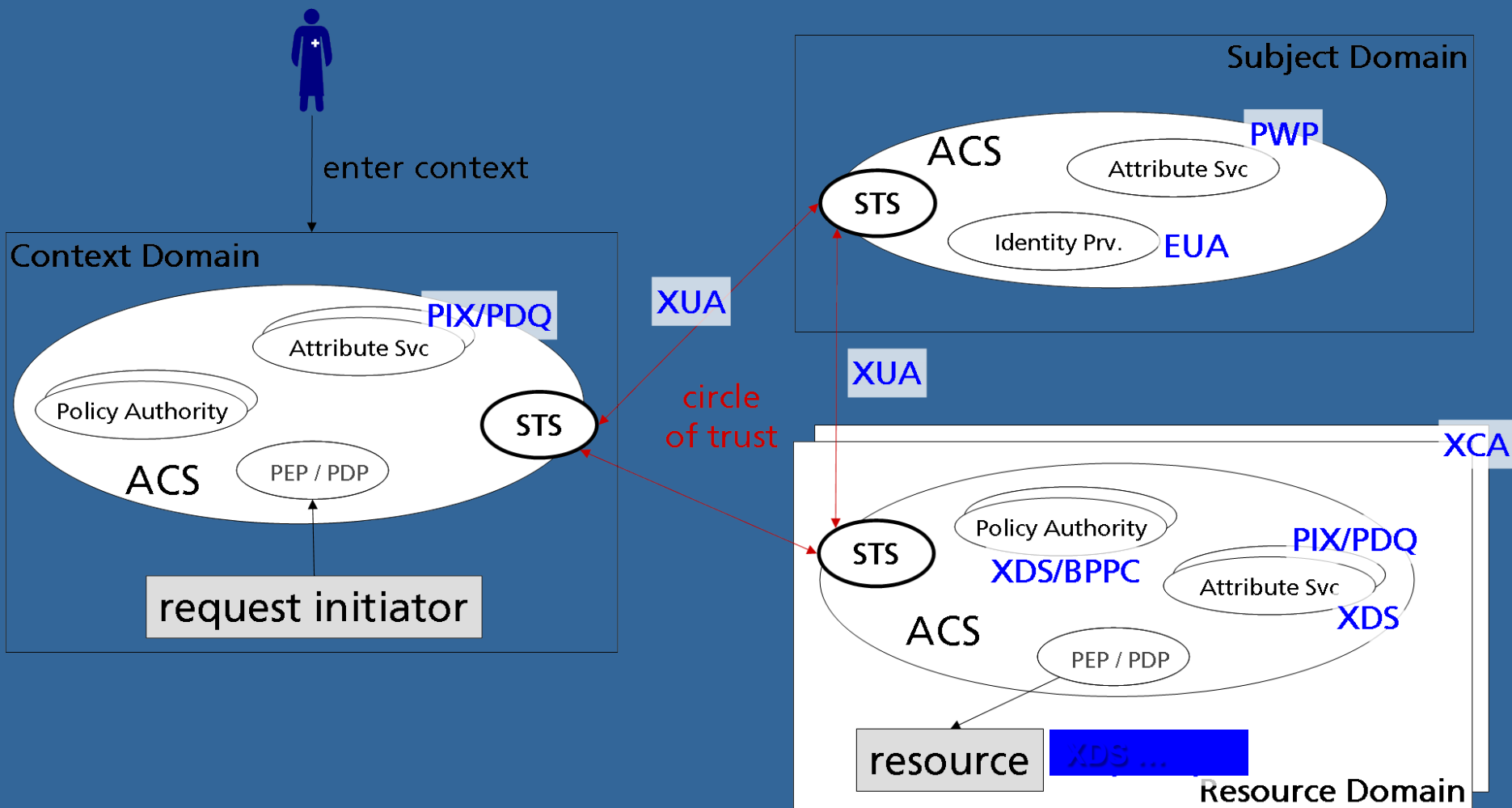
**ATNA + EUA + XUA + BPPC**

# **Access Controls leveraging the Security Profiles**

# Access Control Whitepaper

- **White Paper published in 2009**
- **Examines Access Control domain**
- **Identifies components for Federated Access Control**
  - User Identity and Roles
  - Patient Identity
  - Patient Consent Policies (e.g Opt-In, Opt-Out)
  - Resource Domain (e.g XDS Registry)
  - Context at Requesting (e.g. Purpose Of Use, Break-Glass)
- **Includes explicit recommendations**
- **Shows how IHE profiles can be used**

# Access Control model mapped to IHE Security and Privacy Profiles



# Role-Based-Access-Control mapped to confidentialityCodes for OPT-IN → Normal Sharing

**Example only**

Functional Role	Sensitivity	Billing Information	Administrative Information	General Clinical Information	Sensitive Clinical Information	Research Information	Mediated by Direct Care Provider
	HL7 confidentialityCode (2.16.840.1.113883.5.25)	L	N	D	R	V	T
Administrative Staff		X	X				
Dietary Staff			X				
General Care Provider			X	X			
Direct Care Provider			X	X	X		X
Emergency Care Provider (e.g. EMT)				X			
Researcher						X	
Patient or Legal Representative		X	X	X	X		

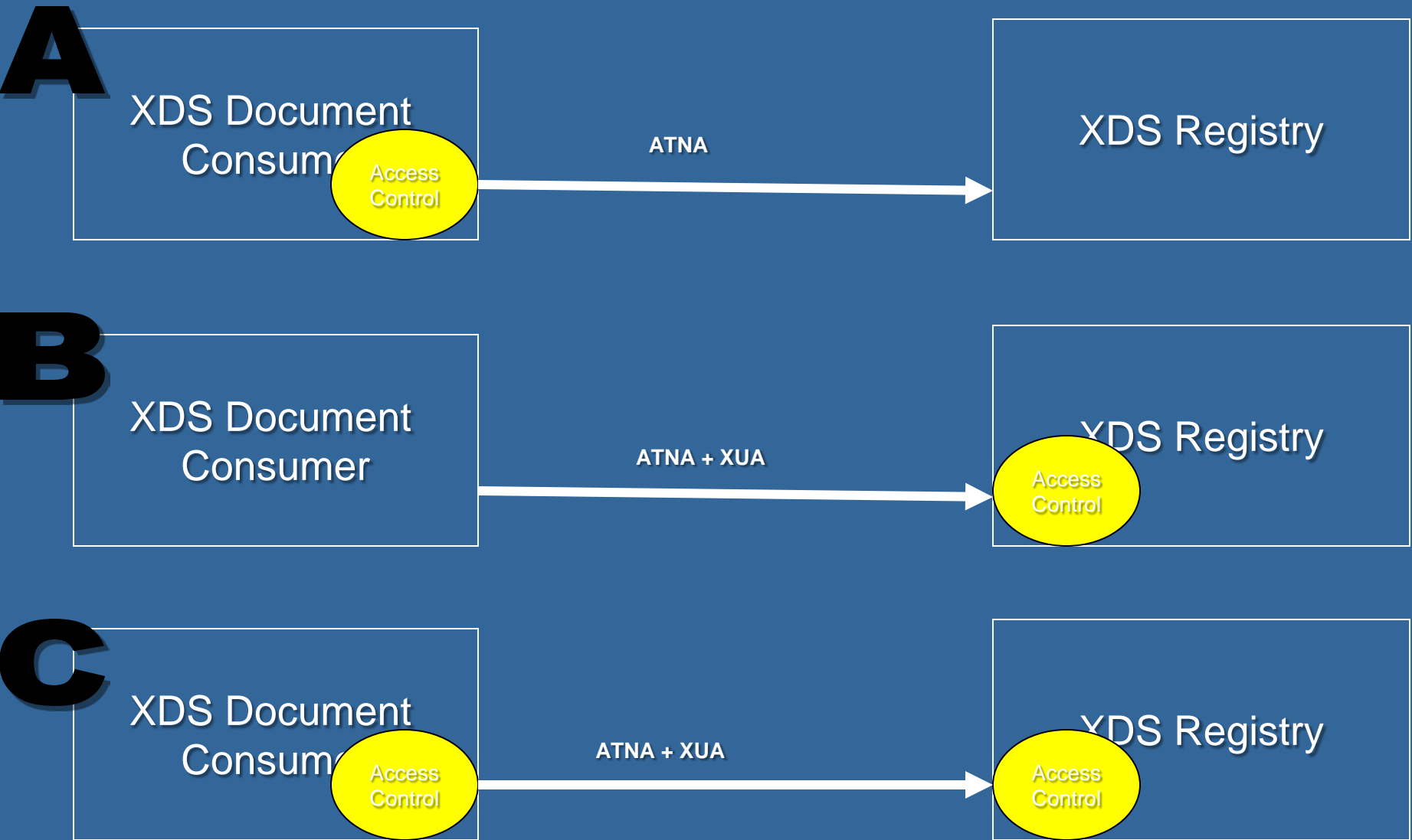
# Role-Based-Access-Control mapped to confidentialityCodes for OPT-OUT

→ Only Direct Care

**Example only**

Functional Role	Sensitivity	Billing Information	Administrative Information	General Clinical Information	Sensitive Clinical Information	Research Information	Mediated by Direct Care Provider
HL7 confidentialityCode (2.16.840.1.113883.5.25)	L	N	D	R	V	T	
Administrative Staff							
Dietary Staff							
General Care Provider							
Direct Care Provider				X			
<i>Break Glass Permission</i>				X			
Emergency Care Provider (e.g. EMT)							
Researcher							
Patient or Legal Representative	X	X	X	X			

# Distributed Access Control – enabled by XUA





# PWP, HPD, ENC

**Additional Profiles related to Security and Privacy**

# Other Profiles of Interest

## Covered in a different Webinar

- Personnel White Pages (PWP)
  - Organizational Directory of Users
- Healthcare Provider Directory (HPD)
  - External Directory of Individuals and Organizations

## Not yet available

- Document Encryption (DEN)
  - Encryption of Documents

# Conclusion



# Supported Security Mis-Use-Cases

- Prevent Indiscriminate attacks → Mutual Auth TLS
- Normal Patient that accepts XDS participation
- Patient asks for Accounting of Disclosures → informed by ATNA log
- Protect against malicious neighbor doctor → informed by ATNA log
- Patient that retracts consent to publish → Repository is local, manual
- Provider Privacy → User identity is not exposed
- Malicious Data Mining → queries are all patient based
- Access to Emergency data set → BPPC policy
- VIP → XDR/M, BPPC (Local enforcement)
- Domestic violence victim → BPPC policy (Local enforcement)
- Daughter with sensitive tests → XDR/M BPPC policy
- Sensitive topics → Don't publish, BPPC policy
- Legal Guardian (cooperative) → BPPC policy (Local enforcement)
- Care Giver (assists w/ care) → BPPC policy (Local enforcement)

# Profiles mapped to Security & Privacy Controls

Security & Privacy Controls		Audit Log	Authentication and Identification	Data Access Control	Secrecy	Data Integrity	Non-Repudiation	Patient Privacy
IHE Profile	Profile Issued							
Audit Trails and Node Authentication	2004	√	√	√	√	√	√	√
Consistent Time	2003	√	.				√	
Enterprise User Authentication	2003		√	.			.	.
Cross-Enterprise User Assertion	2006		√	.			.	.
Basic Patient Privacy Consents	2006			.				√
Personnel White Pages	2004		√	√			.	
Healthcare Provider Directory	2010		√	.			.	
Document Digital Signature	2005		√			√	√	
Document Encryption (in development)	2011			√	√	.		

# Gaps for potential future development

- **Better coded vocabulary for confidentiality codes**
  - Complex policies on a document by document basis
  - Extension to objects other than XDS (e.g. DICOM)
- **Patient Access to**
  - Sensitive health topics (you are going to die)
  - Low sensitivity (scheduling)
  - Self monitoring (blood sugar)
  - Authoritative updates / amendments / removal
- **Complex Privacy 'consent' Policy capabilities**
  - Supporting Inclusion Lists
  - Supporting Exclusion Lists
  - Exceptions, and Obligations
  - Supporting functional role language
- **Access Control Service**
  - Centralized Policies
  - Policy Decision Point / Policy Enforcement Points
- **Accounting of Disclosures reports, alerts, messaging**
  - To support reporting to the 'consumer' when their data is accessed
- **Un-Safe Client machine (home-computer)**

# Cookbook for Security Considerations

- **Consistent Process followed for all IHE Profiles during development**
- **Risk Assessment – Risks introduced by the existence of the new Profile**
- **Security Considerations section in Profile documentation**
- **Any residual risks that need to be handled in system development or deployment**
- **Any required or recommended grouping with security or privacy profiles**
- **Consistent with similar process in HL7 and elsewhere**

# Conclusion

- **IHE provides the Interoperability Profiles needed to enable Security and Privacy**
  - Much of Security and Privacy is policy, operational environment, procedures, and functional capabilities of systems
- **As standards develop and mature new profiles will be created**
- **Continuous Risk Assessment is necessary at all levels**
  - Profile writing (Cookbook for Security Considerations)
  - System design and implementation
  - Network design
  - Physical layout
  - Organizational
  - Privacy/Security Domain
  - Community

# More Information

- **IHE Web site: [www.ihe.net](http://www.ihe.net)**
  - *IHE official material*
  - *Technical Framework documents*
  
- **IHE Wiki site: [wiki.ihe.net](http://wiki.ihe.net)**
  - *IHE committee pages*
  - *Implementation Notes*
  - *Ongoing committee work*
  
- ***IHE ITI technical committee mailing list***
  - *Instructions on the bottom of :*
  - *[http://www.ihe.net/IT\\_Infra/committees](http://www.ihe.net/IT_Infra/committees)*



***IHE*** Changing the Way Healthcare **CONNECTS**

**WWW.IHE.NET**

October 11, 2011