

## Interoperability Scenarios

### Care Theme: Patient Privacy Protection

#### Act 18- Emergency Responder with Patient Privacy Protection

**Scenario Primary Goal:** To demonstrate clinical information exchanged with a Public Health Agency.

#### Key Points:

- This scenario demonstrates use IHE Profiles and HITSP constructs to demonstrate patient consent directives and policy management within the HIE. Consent Management is enforced within HIE if a patient decides to opt-in to put certain access restrictions on their records.
- Capture and manage patient consents; Managing document sensitivity for HIE clinical content
- Policy enforcement and access control; Audit

#### Meaningful Use Relevance

##### MU Objective 1: Improving Quality, Safety, Efficiency and Reducing Health Disparities

- Ensuring privacy and security protections for confidential information through operating policies, procedures, and technologies and compliance with applicable law. Provides transparency of data sharing to patient.
- Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

#### Clinical Workflow:

The patient signs up for their community Health Information Exchange (HIE) using the opt-in policy. The consent is captured and registered in the HIE Registry and stored in the HIE Repository. The 34 year old female patient returns to her primary care physician (PCP) after having been tested for HIV. The physician views the positive laboratory results with the patient. The provider is required to report the results to the Public Health Department, and retrieves the appropriate Public Health form through the EMR. The patient is diagnosed with a privacy-sensitive condition. The clinician shares sensitive documents marking them as 'Restricted' and normal clinical access documents omitting reference to the privacy-sensitive condition. The patient retrieves the clinical information using the PHR and publishes a subset of the clinical data to the HIE in case of emergency. When the patient is involved in an accident, privacy policy is enforced restricting access to the data by role with break-glass requirements. Audit logs are reviewed by security and privacy officer.

Care Scenario Steps	Care Setting From	Care Setting To	IHE Profiles*	Title	HITSP Capability / Construct	Title
18-1 Patient creates a consent and stored in the registry	PCP Office	HIE	BPPC (ITI)	Basic Patient Privacy Consents	HITSP /CAP143 HITSP/TP30	Manage Consumer Preferences and Consents Manage Consent Directives
18-2 PCP reviews and posts encounter summary and post restrictions to HIE	PCP office	HIE	BPPC (ITI) XPHR (PCC)	Basic Patient Privacy Consents Exchange of Personal Health Record Content	HITSP /CAP143 HITSP/TP30 HITSP/CAP119 HITSP/C32	Manage Consumer Preferences and Consents Manage Consent Directives Communicate Structured Document Summary Documents Using HL7 Continuity of Care Document (CCD)
18-3 PCP posts encounter summary and post without restrictions codes to HIE	PCP office	HIE	BPPC (ITI) XPHR (PCC)	Basic Patient Privacy Consents Exchange of Personal Health Record Content	HITSP/CAP119 HITSP/C32	Communicate Structured Document Summary Documents Using HL7 Continuity of Care Document (CCD)
18-4 Patient load clinical data to PHR, and publishes to HIE clinical data for emergency purposes	Patient Home	PHR	BPPC (ITI) XPHR (PCC)	Basic Patient Privacy Consents Exchange of Personal Health Record Content	HITSP/CAP119 HITSP/C32	Communicate Structured Document Summary Documents Using HL7 Continuity of Care Document (CCD)
18-5 911 Access patient PHR data through HIE	Dispatcher	HIE	BPPC (ITI) XUA (ITI)	Basic Patient Privacy Consents Cross-Enterprise User Authentication (Variant)	HITSP /CAP143 HITSP/TP30 HITSP/TP20 HITSP/C19 (Variant)	Manage Consumer Preferences and Consents Manage Consent Directives Access Control Entity Identity Assertion (Variant)
18-6 EMR breaks the glass views patient unrestricted data	EMR	HIE	BPPC (ITI) XUA (ITI)	Basic Patient Privacy Consents Cross-Enterprise User Authentication (Variant)	HITSP /CAP143 HITSP/TP30 HITSP/TP20 HITSP/C19 (Variant)	Manage Consumer Preferences and Consents Manage Consent Directives Access Control Entity Identity Assertion (Variant)
18-7 Review analysis of access to Personal Health Data in Audit Record Infrastructure	HIE	HIE	ATNA (ITI)	Audit Trail and Node Authentication	HITSP/T15	Collect and Communicate Audit Trail

Health Information Exchange (HIE) Core Services			
IHE Profiles		HITSP Service Collaborations / Constructs	
XCA XDS/XDR/XDM	Cross-community and Cross-enterprise Document Sharing	SC112 / TP13, T31, T33	Healthcare Document Management Manage Transfer of Documents, Document Reliable Interchange, Transfer of Documents on Media
PIX	Patient Identity Cross-reference	SC112 / TP22	Patient ID Cross-Referencing
PDQ	Patient Demographics Query	SC112 / T23	Patient Demographics Query
ATNA	Audit Trail and Node Authentication	SC112 / T15, T17	Collect and Communicate Security Audit Trail Secured Communication Channel
CT	Consistent Time	SC112 / T16	Consistent Time