Electronic Consent Management Service Overview

Jim Edwards, Director of Development - jim.edwards@mihin.org
Today’s Agenda

• Overview
• Objectives
• Use cases and use case scenarios
• Statewide eCMS architecture
• Sending specially protected information
  – Sender’s responsibility
  – Confidentiality and sensitivity tags
  – Checks and balances
Overview

• SAMHSA 42 CFR Part 2 requires written patient consent before certain information can be shared with “named recipients” identified by patients

• Michigan’s new law based on House Bill 5782 removes the requirement for patient consent to share other behavioral health information, which is now shareable under HIPAA for Treatment, Payment, and Operations

  – **Passed** 37 to 0 in the Senate and 106 to 1 in the House in 2016:
    • To revise the law that prohibits government public health agencies from sharing information about mental health services provided to an individual under various government programs
    • To add an exception for information considered necessary for treatment, coordination of care or payment

  **SAMHSA 42 CFR 2 is now only law in MI requiring consent**
The Challenge

• Ensure that a patient’s 42 CFR Part 2 consent is appropriately applied during the exchange of specially protected health information such as behavioral health or substance use information:
  – Understand complex patient-provider relationships
  – Carefully design an architecture that can support multiple participants working with individual patients

• Deploy a statewide electronic Consent Management Service (eCMS) in Michigan
eCMS Objectives

- Develop statewide, standard way to manage consumer consent choices as a shared service accessible to any Trusted Data Sharing Organization (TDSO)
- Enable standard statewide service via which consumer consent information can be sent, stored, found, and revoked
  - TDSOs may query to find consent using:
    - HL7 Query By Parameter (same as immunization history/forecast)
    - Fast Healthcare Interoperability Resources (FHIR) query
- Allow healthcare providers to quickly determine whether consumer has consented to share Specially Protected Information (SPI) while still protecting consumer privacy
Consumer Consent Information

Use Case Scenarios

• Consumer Consent Information use case has multiple use case scenarios for sharing specially protected information:
  
  – Send Consent Information
  – Find Active Consent
  – Send Consent Revocation
Distributed Statewide eCMS Architecture

Statewide Consumer Directory stores metadata:
- Consumer identifier (tied to common key)
- Consent document / information location(s)
- Consent period of performance (start, end dates)
- Consented provider associations (tied to provider directory)
- Consent status (active / revoked / expired)
eCMS Conceptual Flow

- Trusted Data Sharing Organization (TDSO) sends consent docs to local eCMS
  - TDSO ensures there is standard, computable consent metadata containing all data elements found in DCH-3927
- Local eCMS stores consent documents
- Local eCMS forwards metadata to statewide eCMS at MiHIN
- Statewide eCMS connects to Statewide Consumer Directory to:
  - Validate consumer demographics w/Common Key Service
  - Validate provider information w/Health Directory
- If exact match: consent metadata tied to common key, stored in statewide eCMS
- If no match: common key created, stored with metadata, key returned to TDSO
Send Consent Information

Data Collector

1. Signs consent document

2. Sends consent document

Consumer

3. Sends consent document

TDSO

4. Sends consent metadata

Local eCMS

5. Consumer / provider attribution

Common Key Service

SCD

HPD

Statewide eCMS
Send Consent Revocation

1. Consumer indicates that a previous consent should be revoked
2. Sends consent revocation
3. Sends consent revocation
4. Sends consent revocation
5. Consumer / provider attribution

Common Key Service

TDSO

Local eCMS

Statewide eCMS

1. Consumer
2. Data Collector

3. If TDSO is also Local eCMS, send consent document
Find Active Consent

1. A consumer is referred to a specialist and arrives for a visit

2. Sends request to “find/receive” SPI

3. Sends “find consent” request

4. Sends “find consent” request

5. Sends consent (authorization) = “yes”

6. Sends consent = “yes”

7. Sends authorizing response to the initial “find/receive” request

Consumer Interrogator

TDSO

Local eCMS

Statewide eCMS

Statewide eCMS

Local eCMS

TDSO

Interrogator Consumer
Integrating eCMS within current infrastructure

• Trusted Data Sharing Organization (TDSO) must query eCMS to see if consent exists for a patient before sending SPI for that patient to MiHIN

• If consent exists (i.e. the eCMS replies “yes”), TDSO may then send SPI to MiHIN.... **BUT....**(!!!)
  – TDSO *must* insert “Privacy Tags” into HL7 message that includes any SPI
  – “Message Inspector” determines who may receive SPI
Responsibility of sender

Sender “asks” if consent is on file before attempting to send SPI
- “No consent on file” response provided if:
  - No consent is on file
  - Consumer cannot be identified
  - **Sender is not listed on consent form**
  - Consent has been revoked
  - Consent form has expired
Checks and balances

Message inspector

- Find consumer
- Find relationships
- Find delivery preferences

Statewide eCMS

Current delivery infrastructure

**Message inspector**
- Detects Privacy Tags:
  - Confidentiality and sensitivity tags indicate permission level of authorized data sharing
  - Codes must be assigned in specific places
- Message discarded on failure
- Common key required
Thank You

Jim Edwards
Director of Development
Jim.Edwards@mihin.org
Patient Mediated Exchange
Present Day Problems

- Patients not well represented in healthcare information exchange today.
  - Patients healthcare information can be shared with little or no patient control.
  - Patients have limited choices over use and management of own healthcare information.
  - Patients may not know how their healthcare information is being used.
Patient Privacy Concerns

• We as patients want real choices over how our information is used (purpose of use) and with how it can be shared (disclosure).

• We want to have faith that our choices will be honored for as long as we want (trust).

• We want to have access to our own information and be able to share it with whomever we want.

• We want to have input into the healthcare system concerning our choices (informed consent) and when we want that treatment to end (DNR).

• We want our choices to be temporary, episodic, or permanent relative to our lives.

• We want our chosen representatives to have the same ability to also be able to make these choices on our behalf.
Patient Privacy Solutions

• Our choices are as restrictive or permissive as we want.

• Our choices operate 24 hours a day on our behalf without our having to actually be there.

• Our choices include designating our healthcare information as sensitive and the ability to decline to sharing with certain groups.

• Our choices are built in from the ground up into healthcare’s next-generation health information sharing system currently under development in HL7 FHIR: Fast Healthcare Interoperable Resources.
  – Making security, privacy, and choice integral to the way FHIR manages and controls its resources.
  – Auditing the use of our information to verify use and detect misuse.
Our Approach

• Provide a centralized consent management service for patients.
• Send or direct our own healthcare information to wherever we choose.
• Enforce our choices by granting authorization tokens encoding our choices including obligations.
• Record disclosures.
Technologies

• HL7 FHIR Consent: Capturing and storing patient privacy preferences in a structured format.

• OAuth/UMA: Responding to queries based on patient preferences acting as the patient agent.

• Security Labeling Service: Labeling patient health information automatically based on content.

• HL7 FHIR Audit: Capturing and storing a record of the event releasing patient health information in a structured format.
Patient Choice using FHIR Consent

- Who can receive patient healthcare information
  - Organization, Provider, Care Team, Device
- What kind of healthcare information
  - Immunizations, Prescriptions, etc.
- With what kind of labels
  - Sensitive Conditions
- Purpose of use
  - Treatment, Research
- Obligations
  - Handling Instructions
Patient Choice with OAuth/UMA

- Patients approving each request for each custodian
- Patients filing consent rules to each custodian
- Patients filing consent rules with a consent management authorization service
Patient Choice on Releasing Information: Security Labeling Service

Prescription
Date: 11/10/2009
Doctor’s Name: Dr. Bob
Patient’s Name: Alice
Clinic Name: Sample Clinic
1. Acetaminophen 300 MG / Codeine Phosphate 30 MG Oral Tablet
2. Methadone Hydrochloride 50 MG/ML Injectable Solution

Prescription
Date: 11/10/2009
Doctor’s Name: Dr. Bob
Patient’s Name: Alice
Clinic Name: Sample Clinic
1. Acetaminophen 300 MG / Codeine Phosphate 30 MG Oral Tablet
2. Methadone Hydrochloride 50 MG/ML Injectable Solution

Substance Abuse Sensitivity
Patient Record of Disclosure with FHIR Audit

• A structured record of the event releasing the patient information
  – What
  – Who
  – Why
  – When
Empowering Patient Control with Choice

- Enabling patients to express preferences with a centralized consent management service.
- Capturing and enforcing patient preferences without requiring patient involvement in every transaction.
- Labeling patient information automatically for sensitive conditions.
- Providing accountability in who had access to patient healthcare information, what type of information, why, and when.
Come Visit Us

Learn more about how patients can control their own health information with HL7 FHIR.

Please come see our demonstration located in the Federal Health Architecture Vignette behind you. We are in the middle of the three.
The Patient Choice Technical Project
HIMSS 2017 Update
What is Computable Privacy?

• An individual’s electronic health information needs to be digitally connected to his/her sharing choices.

• All data holders and their health IT systems need to know what to do when an individual does not document a choice. Default rules cannot be ambiguous and should support data for health.

• Telemedicine, community health supports, and other innovative delivery processes will be stunted if the health care industry cannot make privacy computable.
**Explain HIPAA Better**

- **HIPAA Permitted Uses & Disclosures**
  - HIPAA is media agnostic and has supported health information exchange through permitted uses and disclosures for which an individual’s authorization is not required for the past 17 years.
  - ONC/OCR Fact Sheets illustrating permitted sharing for:
    - Treatment (Care planning & Referral)
    - Health Care Operations of
      - Payor Case Management
      - Multi-provider Quality Assessment/ Improvement
      - Multi-provider reduction in hospital acquired infections
- **HIPAA Right of Access**
  - Gives patients the right to access their health information electronically if stored electronically
  - Provides patients with the right to send information to a third party
- **HIPAA Basics**
  - See ONC [Permitted Use Fact Sheets and Blog](#) and OCR [New Access Guidance](#)
Three Levels of Rules All Must Be Computable

- **HIPAA runs in the background** and permits disclosure for health
- **Basic Choice** refers to the choice an individual makes about the use and disclosure of health information, including the electronic exchange of health information, irrespective of default rules.
- **Granular Choice** is the choice an individual makes regarding the distinctions between legally sensitive clinical conditions, such as mental health or HIV/AIDS status and evolves over time to enable choice about disclosure to specifically identified participants in the health care system.
Observations on Patient Choice

• Choosing to share to exchange or for research is the same process:
  – Compare
    • “Please let my data flow to other doctors/please do not let my data flow to other doctors” to
    • Please use my data in this research project/please do not use my data in this research project.
• Basic Choice, then, is a process, for which documentation and standards can be developed in a context-neutral way
• Which led OCPO to
  – Apply concept of Basic Choice to project underway to develop privacy and legal & policy framework for research; and
  – Expand the scope of a project underway on technical standards for research choice
Basic Choice vs Granular Choice

• “Basic choice” refers to an opt-in or opt-out choice offered to an individual to prevent his or her protected health information (PHI) from being available for electronic exchange for purposes of treatment, payment, and healthcare operations (TPO)

• “Granular choice” refers to a detailed choice an individual makes to share specific types of information. For example:
  – Information which is by law, protections in addition to HIPAA apply
  – Choice afforded to an individual based on their age
  – The choice to share information by specific provider or payer types
ONC Patient Choice Technical Project

- Goal: to encourage development of standards to capture patient consent in an electronic, computable way
  - Move away from paper-based consent!
  - Focus on the standards needed to capture consent for interoperable exchange
- Three phases:
  - Phase 1: Basic Choice for Treatment
  - Phase 2: Basic Choice for Research
  - Phase 3: Granular Choice
Project Timeline Overview

- **Phase 1:** Basic Choice for TPO
- **Phase 2:** Basic Choice for Research
- **Phase 3:** Granular Choice
ONC Patient Choice Technical Project Phase One Summary

- Documented 5 scenarios for basic choice for treatment, payment, and healthcare operations
- Community-led pilots included VA, MiHIN, and SAMHSA
- Aided in successfully balloting HL7 Implementation Guide for CDA Release 2, Privacy Consent Directives, Release 1 resulting in an ANSI approved normative standard
- Come see us in the FHA demo area for an update on our progress!
ONC Patient Choice Technical Project
Phase Two – How You Can Get Involved

• Currently developing use cases for basic choice for research
• Actively recruiting pilot organizations
• If you’re interested in becoming a pilot, or just finding out more about our project, come join our working group calls!
Next Steps

• The Phase 2: Basic Choice for Research Use Case Working Group meeting meets weekly on Fridays at 11am ET

• Visit our confluence page for more information
  – [http://confluence.siframework.org/display/PATCH/The+Patient+Choice+Technical+Project+Homepage](http://confluence.siframework.org/display/PATCH/The+Patient+Choice+Technical+Project+Homepage)

• Review past meeting materials
  – [http://confluence.siframework.org/display/PATCH/Project+Materials](http://confluence.siframework.org/display/PATCH/Project+Materials)
<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCPO-ONC Lead</td>
<td>Rose-Marie Nsahlai</td>
<td><a href="mailto:Rose-Marie.Nsahlai@hhs.gov">Rose-Marie.Nsahlai@hhs.gov</a></td>
</tr>
<tr>
<td>Project Coordinator</td>
<td>Johnathan Coleman</td>
<td><a href="mailto:jc@securityrs.com">jc@securityrs.com</a></td>
</tr>
<tr>
<td>Project Manager</td>
<td>Ali Khan</td>
<td><a href="mailto:Ali.Khan@esacinc.com">Ali.Khan@esacinc.com</a></td>
</tr>
<tr>
<td>Project Support</td>
<td>Taima Gomez</td>
<td><a href="mailto:Taima.Gomez@esacinc.com">Taima.Gomez@esacinc.com</a></td>
</tr>
<tr>
<td>Staff SME</td>
<td>Amber Patel</td>
<td><a href="mailto:ayp@securityrs.com">ayp@securityrs.com</a></td>
</tr>
<tr>
<td>Staff SME</td>
<td>Kathleen Connor</td>
<td><a href="mailto:klc@securityrs.com">klc@securityrs.com</a></td>
</tr>
<tr>
<td>Staff SME</td>
<td>David Staggs</td>
<td><a href="mailto:drs@securityrs.com">drs@securityrs.com</a></td>
</tr>
</tbody>
</table>
Challenges for Consent Across Healthcare

Kenneth Salyards
Substance Abuse and Mental Health Services Administration
42 CFR Part 2: Overview

Restricts the disclosure and use of patient substance abuse records maintained in connection with the performance of any federally-assisted alcohol and drug abuse program.
42 CFR Part 2: Consent Requirements

- Requires patient consent for disclosures of protected health information even for the purposes of treatment, payment, or health care operations
- Consent for disclosure must be in writing
- No redisclosure without patient written consent
42 CFR Part 2: Ten Elements

1. Name of the entities making the disclosure
2. Name of the entities to receive the disclosure
3. Name of the patient who is the subject of the disclosure
4. Specific purpose or need for the disclosure
5. How much and type of information to be disclosed
6. The patient’s right to revoke the consent in writing and exceptions to the right to revoke

7. The program’s ability to condition treatment, payment, enrollment, or eligibility of benefits on the patient

8. The date, event, or condition on which the consent expires

9. The signature of the patient (and/or other authorized person)

10. The date that the consent is signed
C2S: Patient Provides Electronic Consent
C2S: Patient’s View of Signed Consent

---

**eSignature**

**Consent to Share My Health Information**

Created On: 04/06/2016
Consent Reference Number:
MHC.HCQAFlh&16.040.1.113953.3.704.100.200.1.0.1&ISO:151892963:1790710047:CEATAM

Patient Name: Bob Lastname  
Patient DOB: 07/04/1976

**AUTHORIZATION TO DISCLOSE**

**Authorized:**
Provider Name: GIANT OF MARYLAND LLC
NPI Number: 1952916092
Address: 8218 WISCONSIN AVE,
BETHESDA, MD, 20814-3107
Phone: 301-554-1111

To disclose to:
Provider Name: CAPITAL CARDCIOVASCULAR ASSOCIATES OF SILVER SPRING, LLC
NPI Number: 1871783456
Address: 15225 SHADY GROVE RD,
ROCKVILLE, MD, 20850-3258
Phone: 301-938-8977

**HEALTH INFORMATION TO BE DISCLOSED**

To SHARE the following medical information:
- Addictions Information
- Alcohol use and Alcoholism Information

To SHARE for the following purpose(s):
- Health Treatment

**CONSENT TERMS**

I, Bob Lastname, understand that my records are protected under the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR part 2, and cannot be disclosed without my written permission or as otherwise permitted by 42 CFR part 2. I also understand that I may revoke this consent at any time except to the extent that action has been taken in reliance on it, and that any event this consent expires automatically as follows:

Effective Date: 04/08/16  
Expiration Date: 04/08/17

---

I, Bob Lastname, hereby accept, and understand the terms of this consent.
Data Segmentation for Privacy (DS4P)

- An initiative sponsored by SAMHSA and ONC to improve the ability to securely share sensitive health information, specifically substance abuse patient records
- Demonstrated how standards can support current privacy policies to share sensitive health information across organizations
- Developed standards to enable sensitive electronic health information to be securely shared with authorized users
The Current Environment

- Client’s right to share or withhold
- Compliance with confidentiality and privacy laws
- Demand for coordinated patient centered care
- Increase in EHRs and Health IT
- Greater interoperability
- More electronic client data-sharing
Need for DS4P & Consent Management

- Elicit client consent
- Classify clinical data
- Comply with client choices
- Comply with 42 CFR P/2
Segmentation and Security Labeling

- It requires an algorithm to identity and label sensitive information
  - Assign a “confidentiality” as “Restricted” if information is sensitive
  - Use the client consent to identify “intended recipients” for sensitive information (e.g. Dr. Jane)
- Security labels may be applied to any data intended for exchange (i.e. document, messages, resource)
Dr. Jane

- Restricted
- Intended for Treatment
Consent2Share Components

Consent2Share includes 30 distinct components, including:

- **Patient User Interface**—for patients to review and conduct consent management
- **Patient Management User Interface**—for admins to create and manage user accounts
- **Management Component**—to create and manage consent policies
- **Information Exchange Hub**—allows the retrieval of data from a HIE irrespective of the format of the data
- **Data Segmentation Service**—manages a patient’s sensitive health information as directed by the patient’s consent choices
Consent Process in the Cloud

- Consent2Share includes discrete components
- Uses OAuth to separate application components to make them easier to implement
- *Example:* Consent user interface can be separated from the segmentation component
- Allows greater customization
- Using FHIR to store consents
Runtime Components

- Consent Application
  - Includes Patient and Provider Identity Certificate and references Security Label Definitions
  - Create, update, revoke Consent

Runtime Components Diagram:

- Authorization Domain
  - Authorization Server
  - Security Labeling Service
  - Resource Server
  - Intended Recipient
  - Label Definitions
  - Apply Labels
  - Protection API
  - PAT

- Initiating Domain
  - Identity Manager
  - Client Application
  - RequestToken
  - Initiator

1: POST/token (client_id, client_secret) returns access_token
2: GET/resource (access_token) returns protected resources
Security labels could be pre-processed when a resource is persisted, in batch, or on-demand.

Security Labeling Process

Sensitivity computed based on clinical value sets and NLP

SLS assigns a confidentiality tag based on sensitivity

SLS adds intended recipients based on consent

SLS adds purpose of disclosure based on consent
Sharing data based matching initiator and data attributes

Evaluate security label

Compare request token with security label
Opportunities for Data Segmentation

- Separation of Concerns
  - Consent Management
  - Data Redaction/Tagging
    - Put segmentation at the data instance
- Increase patient access to consent management applications
- Enable EHR applications to honor data tagging
- Use HL7 FHIR
Questions?

Kenneth Salyards
Information Management Specialist
Center for Substance Abuse Treatment
Substance Abuse and Mental Health Services
Kenneth.Salyards@SAMHSA.hhs.gov