The Office of the National Coordinator for Health Information Technology

Privacy and Security Framework for Patient-Centered Outcomes Research (PCOR)

ENABLING GRANULAR CHOICE FOR HEALTH CARE DELIVERY AND RESEARCH CONSENT

July 2020

Table of Contents

1.0 Introduction

The Granular Choice Use Case was developed under the Privacy and Security Framework for Patient-Centered Outcomes Research (PCOR) project[1]. This project was funded by the Patient-Centered Outcomes Research Trust Fund[2] that is overseen by the Office of the Assistant Secretary for Planning and Evaluation (ASPE). The focus of the Privacy and Security Framework for PCOR project is to develop tools and resources that address the many privacy and security-related legal and policy issues that affect use of data for various types of PCOR. This work aims to support sharing of patient data and organizational efforts to comply with laws, regulations, or policies that require the capture of patient consent for electronic data sharing and compliance with that consent. Importantly, patient control over the use and disclosure of his or her electronic health data may be better supported by moving away from paper forms and toward an interoperable, electronic, and auditable consent process.

This document defines the interoperability requirements for health data exchange enabled when leveraging a granular consent model.[3] Consent at a granular data level can protect patients' privacy by maintaining confidentiality of their information in an interoperable environment. In this guide, the granular choice use case is framed through consent scenarios. Each consent scenario is a comprehensive description of the actors, interactions, activities, and requirements associated with the information exchange. It is a prototypical sequence of interactions in business collaboration or in an application context. This guide includes information about:

- Operational context for the data exchange,
- Affected stakeholders,
- Information flows that must be supported, and
- Types of data involved and their required specifications for data exchange.

This use case can support the development of implementation guides and tools that lead to consistent and reliable adoption of standards that enable patient choice of how and when their health data is shared.

1.1. Definition of Granular Choice

The granular choice use case focuses specifically on identifying data standards that support the use of granular privacy consent directive. Granular choice refers to a detailed choice an individual makes to share specific types of health data. This granular privacy consent directive will enable the capture and exchange of patients' preferences to advance coordination of care in multiple settings for treatment, payment, healthcare operations, and research.

[1] ONC Privacy and Security Framework for Patient-Centered Outcomes Research project: https://www.healthit.gov/topic/scientific-initiatives/pcor/privacy-and-security-framework-pcor-psp

[2] ASPE PCOR Trust Fund: https://aspe.hhs.gov/patient-centered-outcomes-research-trust-fund

[3] This document reflects the environment and technical capabilities that were current at the time this project was active.

Examples of granular choice include the ability to choose electronic sharing of information:

- Protected by law, including protections beyond the Health Information Portability and Accountability Act (HIPAA)
- Based on individual patient age
- By purpose of use (e.g., treatment, research), specific provider, and payer types

1.2. In Scope

- Semantic understanding of a granular choice and the corresponding information that comprises a granular privacy consent directive
- Demonstration of the use of computable consent to enable privacy policy implementation and information access controls

1.3. Out of Scope

- Exact methods through which consent is captured (i.e., whether consent is captured ahead of time via a patient portal or in-office using a tablet)
- User interface presented to the patient at the time that consent is captured
- Mechanisms for managing a research consent directive once supplied
- Organizational policies surrounding retroactivity (i.e., how to respond when a patient changes their research consent directive to "Do not share")
  - Organizational policies regarding subsequent restrictions on future use
- Mechanisms to update research consent directives
  - Maintenance and updating of consent repositories and registries

2.0 Communities of Interest

Table 1: Communities of Interest

Stakeholders / Communities of Interest	Description
Healthcare Providers	Healthcare providers with patient care responsibilities including physicians, advanced practice nurses, physician assistants, nurses, psychologists, emergency care providers, home health providers, definitive care providers, pharmacists, and other personnel involved in patient care.
Healthcare Organizations	Organizations that are engaged in or support the delivery of healthcare to include hospitals, ambulatory centers, provider practices, integrated delivery networks, community health agencies, and rehabilitation centers. They can also include specialty areas such as behavioral health organizations, dental organizations, cardiology, radiology, labs, etc. The requirements for these specialty areas may vary depending on laws, regulations, and other business workflow needs. These organizations query data for various purposes and provide data for others to query.
Government Agencies	Federal, state, local agencies, and other government organizations that deliver, regulate, or provide funding for health and healthcare.

Stakeholders / Communities of Interest	Description
Data Standards Organizations	Organizations whose purpose is to define, harmonize, and integrate standards that will meet clinical and business needs for sharing information among organizations and systems.
Health Information Exchange (HIE)/ Health Information Organization (HIO)	Health Information Exchanges (HIEs) and Health Information Organizations (HIOs) that exchange healthcare information electronically across organizations within a region, community, or hospital system, including Clinical Data Research Networks (CDRNs) and Patient-Powered Research Networks (PPRNs).
Health Information Technology (IT) Developers – EHR/ PHR/Third party application developers	Vendors that provide specific health IT solutions such as software applications and software services. These suppliers may include developers, providers, resellers, operators, the innovation community, and others who may provide these or similar capabilities. These organizations provide healthcare solutions such as EHR, patient health record (PHR) solutions, and other software applications and services. Examples include: integration vendors, data providers, medical device vendors, release of information (ROI) vendors, RMMS (Remote Monitoring Management System) vendors, diagnostic imaging service providers, clinical order system supply vendors, transcription service vendors, clearinghouses, drug knowledge suppliers, network infrastructure providers, clinical decision support (CDS) resource systems, practice-based registry system suppliers, public health registry systems, immunization information system providers, clinical genetic database/repository system vendors, healthcare record banking, etc.
Privacy and Security Experts	Consumer/patient and technology experts who represent privacy and security interests of the public or specific organizations.
Patients	Members of the public who receive healthcare services from ambulatory, emergency department, physician's office, and/or a public health agency/department.
Patient Advocates	Patient advocates who act as liaisons between a patient, healthcare provider(s), and research institutions, including disease-specific health groups.
Federal Demonstration and Pilot Projects	Selected communities or groups who have received federal funding through ONC to build and strengthen their health IT infrastructure and exchange capabilities to improve care coordination, increase the quality of care, and slow the growth of healthcare spending.
Public Health Agencies	Public Health Agencies who query data for public health purposes and provide data for others to query.
Researchers	Organizations and groups that conduct healthcare research including academic researchers, commercial researchers, and government research organizations.

3.0 Granular Choice Use Case Assumptions

- Requirements of this use case can be implemented in a variety of architectures
- Researchers are aware of, and comply with, the federal and legal requirements regarding consent
- Electronic systems have the capability to manage and update consent registries/repositories
- Electronic service information is known to all systems involved in the exchange
- All parties in the exchange comply with applicable privacy and security rules
    - Policy is in place for handling missing or not yet recorded patient preferences for data sharing
    - All parties comply with patient privacy preferences and subsequent handling instructions unless law requires otherwise; for example, a subpoena or a search warrant
- Disclosures are appropriately updated in the system to be reflected in accounting for disclosures that may be requested by the patient
- Requesting entity is verified and authorized to conduct a query for patient data
- Appropriate security audit mechanisms are in place
- Appropriate methods for capturing consent are in place
- Appropriate methods for sending acknowledgments for receiving of data are in place
- Appropriate methods for storing data and consent information are in place

4.0 Preconditions

- Mechanisms are in place for handling missing or not yet recorded patient preferences for data sharing
- Mechanisms are in place for systems having patient data to enforce the appropriate legal and policy requirements
- Mechanisms are in place to comply with research consent directives and subsequent handling instructions

5.0 Post Conditions

- Receiving system complies with ongoing obligations
- Sending and receiving systems have recorded the transactions in their security audit records

6.0 Granular Choice Consent Scenarios

The following granular choice consent scenarios demonstrate how the patient, named Alice, can choose which providers can receive her substance use disorder (SUD) information. SUD information is protected by 42 Code of Federal Regulations (CFR) Part 2 Confidentiality of Substance Use Disorder Patient Records[4]. Alice can provide granular level consent through an Electronic Consent Management Service (eCMS), a service that was pilot tested as part of the Privacy and Security Framework for PCOR project.

The Michigan Statewide eCMS allows patients to specify consent based on their active care relationships. The Michigan Health Information Network (MiHIN) Active Care Relationship Service (ACRS) consists of

[4] Final Rule: https://www.federalregister.gov/documents/2017/01/18/2017-00719/confidentiality-of-substance-use-disorder-patient-records

provider attributions to a patient list.[5] Providers supply this list to MiHIN weekly or monthly as a declaration of their patient list. When a message is sent, ACRS allows MiHIN to route the message to a patient's entire care team, rather than one person.

6.1. Consent Scenario 1: Alice Is Treated for Abdominal Pain

Alice is a Michigan resident where protected health information is sent to a patient's care team as governed by HIPAA for reasons of Payment, Treatment, and Coordination of Care through the MiHIN Network.[6] Alice's active care team is determined based on patient lists provided by her physicians.

Alice regularly attends an opioid treatment facility. Alice's SUD information, which is protected by 42 CFR Part 2, is distributed through the MiHIN network to only those members of Alice's care team who are listed on her active Michigan Behavioral Health Standard Consent Form (MDHHS-5515) for care coordination purposes.

Due to abdominal pain, Alice seeks treatment from a new provider at an urgent care clinic, Dr. McCoy. Dr. McCoy adds Alice to her patient list, which is updated in the MiHIN ACRS. However, since Dr. McCoy is not listed on Alice's consent form, Dr. McCoy's electronic health system is not allowed to send or receive any health information protected by 42 CFR Part 2.

Alice visits her eConsent portal and grants consent for Dr. McCoy to send and receive health information protected by 42 CFR Part 2, including medication information. Dr. McCoy's electronic health system will now be allowed to send and receive SUD information, which has been appropriately tagged and labeled.

During Alice's next visit regarding her abdominal pain she informs Dr. McCoy of her opioid addiction. Dr. McCoy notes that her abdominal pain may be related to her SUD (opioid addiction) and to ensure the best possible care for Alice, Dr. McCoy's electronic health system queries eCMS to determine if Alice's SUD information may be shared with her care team. Because Dr. McCoy has been named on Alice's consent, Dr. McCoy's electronic health system requests Alice's SUD information. MiHIN routes the health information to authorized recipients.

NOTE: Recipients of the health information may not re-disclose SUD information, which is protected under 42 CFR Part 2 without Alice's consent.

During Alice's next visit to her opioid treatment facility, her doctor reviews her recent medical visits. Alice is prescribed medication that is protected by 42 CFR Part 2, which assists with detoxification in the treatment of opioid withdrawal symptoms. The opioid treatment facility's electronic health system queries eCMS to determine if SUD information may be shared with Alice's care team. The opioid treatment facility has been previously given consent to share Alice's SUD information, appropriately tags Alice's

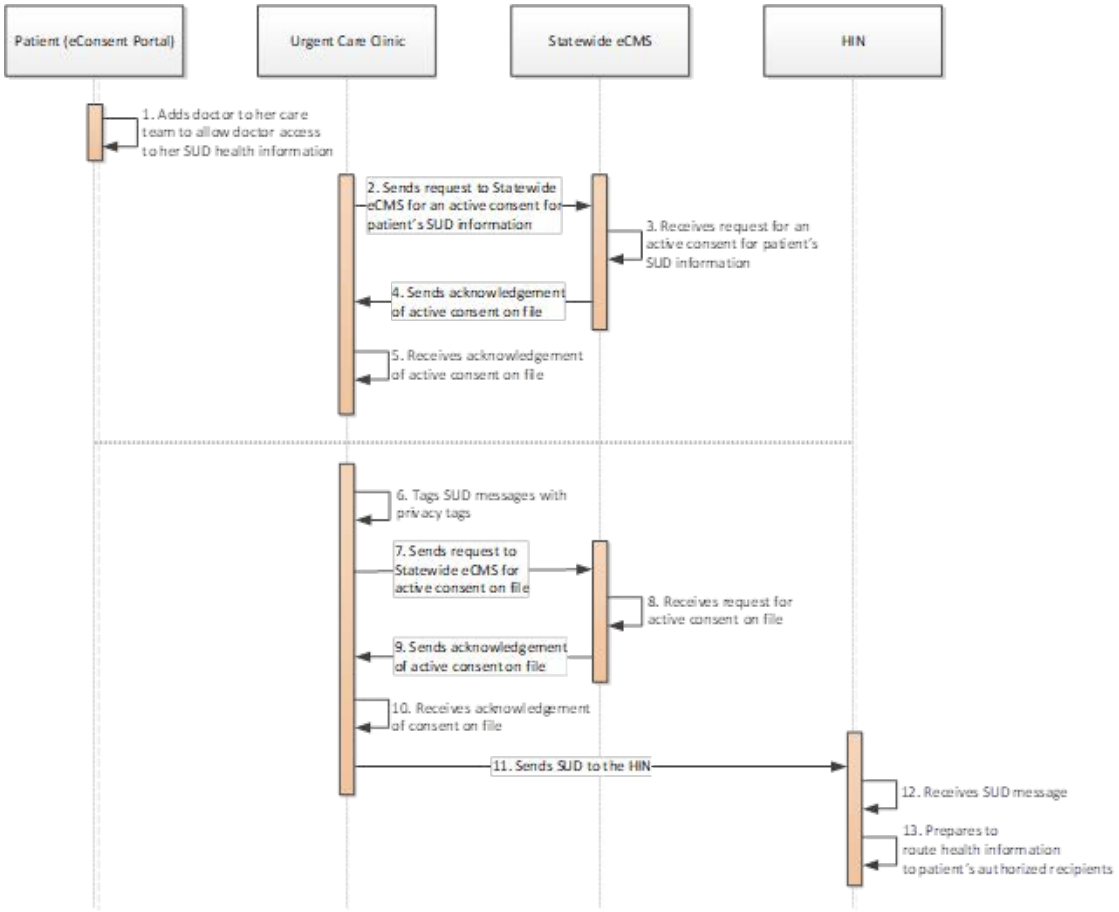
[5] Active Care Relationship (ACR): (a) For health providers, a patient who has been seen by a provider within the past 24 months, or is considered part of the health provider's active patient population they are responsible for managing, unless notice of termination of that treatment relationship has been provided to HIN; (b) for payers, an eligible member of a health plan; (c) an active relationship between a patient and a health provider for the purpose of treatment, payment, and/or healthcare operations consistent with the requirements set forth in HIPAA; (d) a relationship with a health provider asserted by a consumer and approved by the health provider; or (e) any person or Trusted Data-Sharing Organization (TDSO) authorized to receive message content under an exhibit which specifies that an ACR may be generated by sending or receiving message content under that exhibit. ACR records are stored by HIN in the ACRS.

[6] "Non-specially" meaning health information that does not have additional protection under law or extra protection under law beyond HIPAA.

Admit-Discharge-Transfer (ADT) and Medication Reconciliation information and sends through the MiHIN network. MiHIN routes the health information to authorized recipients.

NOTE: Dr. McCoy's electronic health system displays Alice's medications including SUD health information which are protected by 42 CFR Part 2.7

Figure 1: Sequence Diagram of Consent Scenario 1: Alice Is Treated for Abdominal Pain



[7] https://www.samhsa.gov/disorders/substance-use

Table 2: Base Flow of Consent Scenario 1: Alice Is Treated for Abdominal Pain

Step #	Actor	Role	Event/Description	Inputs	Outputs	Type of Requirement
1	Patient (eConsent Portal)	Data Source	Adds doctor to her care team to allow doctor access to her SUD health information	Addition to patient's care team	Access to patient's SUD health information	System
2	Urgent Care Clinic	Data Requestor	Sends request to Statewide eCMS for an active consent for patient's SUD information	Access to patient's SUD health information	Request for an active consent for patient's SUD information	Information Interchange
3	Statewide eCMS	Data Source	Receives request and sends acknowledgement of active consent on file	Request for an active consent for patient's SUD information	Acknowledgement of active consent on file	Information Interchange
4	Urgent Care Clinic	Data Receiver	Receives acknowledgement of active consent on file	Acknowledgement of active consent on file	Acknowledgement of active consent on file	Information Interchange
5	Urgent Care Clinic	Data Source	Tags SUD messages with privacy tags	SUD messaged with privacy tags	SUD messaged with privacy tags	System
6	Urgent Care Clinic	Data Requestor	Sends request to Statewide eCMS for active consent on file	Request for active consent on file	Request for active consent on file	Information Interchange
7	Statewide eCMS	Data Source	Receives request and sends acknowledgement of active consent on file	Request for active consent on file	Acknowledgement of active consent on file	Information Interchange
8	Urgent Care Clinic	Data Receiver	Receives acknowledgement of active consent on file	Acknowledgement of active consent on file	Acknowledgement of active consent on file	Information Interchange
9	Urgent Care Clinic	Data Source	Sends SUD to the HIN	SUD message	SUD message	Information Interchange
10	HIN	Data Receiver	Receives SUD message	SUD message	SUD message	Information Interchange
11	HIN	Data Source	Routes health information to the patient's authorized recipients	SUD message	SUD message	System

Table 3: System Requirements of Consent Scenario 1: Alice Is Treated for Abdominal Pain

System	System Requirement
Patient (eConsent Portal)	Adds doctor to her care team to allow doctor access to her SUD health information
Urgent Care Clinic	Tags SUD messages with privacy tags
Health Information Network (HIN)	Routes health information to only the patient's authorized recipients

6.2. Consent Scenario 2: Alice Participates in a Research Study

Based on a recommendation from Dr. McCoy, Alice visits a research organization that is accepting applicants for new research studies. After an interview with the research organization, Alice is asked whether she is interested in participating in a study regarding the effects of opioids on esophageal dysfunction. Alice agrees to participate and signs an informed consent form. She then signs a right of access form to share SUD information, but only for her message content, with the research organization.

During Alice's visit to the research organization, only Consolidated-Clinical Document Architecture (C-CDA) documents are generated for her SUD information.

NOTE: Alice's opioid treatment facility will receive the full C-CDA message from the research facility including medication. Dr. McCoy will receive a medication reconciliation C-CDA rather than the full C-CDA message. Neither Alice's opioid treatment facility nor Dr. McCoy will receive ADT messages.

Alice begins to feel uncomfortable with the direction of the research project and wishes to cease her participation in the effects of opioids on esophageal dysfunction research project. She confirms her removal with the researcher and logs into her patient portal to revoke authorization for the research organization to receive her health information. The change in her right of access updates the statewide eCMS. The research organization no longer receives any health information.

Figure 2: Sequence Diagram of Consent Scenario 2: Alice Participates in A Research Study

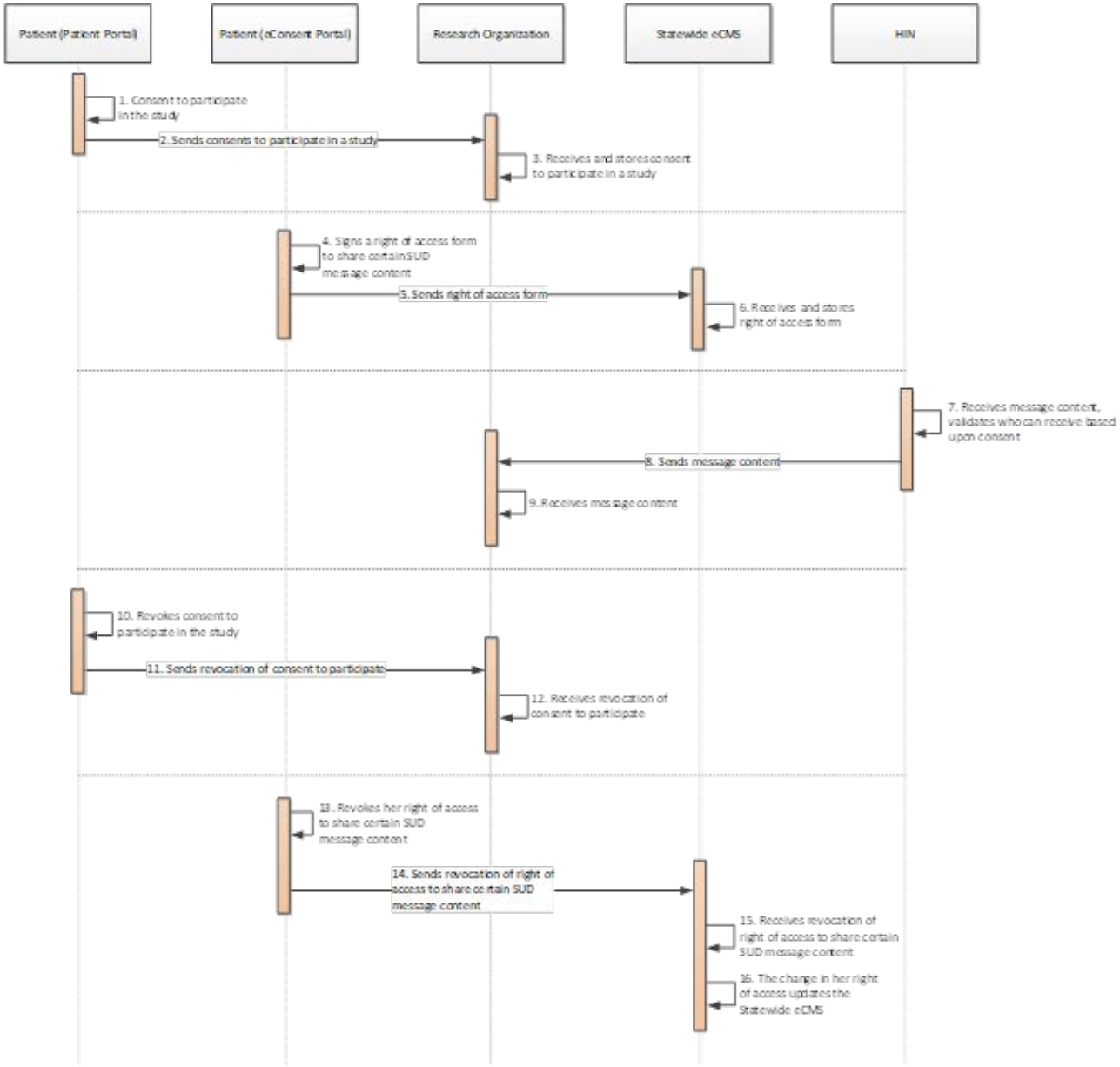


Table 4: Base Flow of Consent Scenario 2: Alice Participates in a Research Study

Step #	Actor	Role	Event/Description	Inputs	Outputs	Type of Requirement
1	Patient (Patient Portal)	Data Source	Consents to participate in a study	Consent to participate in a study	Consent to participate in a study	System
2	Patient (Patient Portal)	Data Source	Sends consent to participate	Consent to participate in a study	Consent to participate in a study	Information Interchange
3	Research Organization	Data Receiver	Receives consent to participate	Consent to participate in a study	Consent to participate in a study	Information Interchange
4	Research Organization	Data Receiver	Stores consent to participate	Consent to participate in a study	Consent to participate in a study	System
5	Patient (eConsent Portal)	Data Source	Signs a right of access form to share certain SUD message content	Right of access form	Signed right of access form	System
6	Patient (eConsent Portal)	Data Source	Sends right of access form	Signed right of access form	Signed right of access form	Information Interchange
7	Statewide eCMS	Data Receiver	Receives right of access form	Signed right of access form	Signed right of access form	Information Interchange
8	Statewide eCMS	Data Receiver	Stores right of access form	Signed right of access form	Signed right of access form	System
9	HIN	Data Receiver	Receives message content from various sources	Message content	Message content	Information Interchange
10	HIN	Data Receiver	Validates who can receive it based upon consent	Message content	Message content with validation of recipients	System
11	HIN	Data Source	Sends message content to authorized receivers	Message content with validation of recipients	Message content	Information Interchange
12	Research Organization	Data Receiver	Receives message content	Message content	Message content	Information Interchange
13	Patient (Patient Portal)	Data Source	Revokes consent to participate	Consent to participate	Revocation of consent	System
14	Patient (Patient Portal)	Data Source	Sends revocation of consent	Revocation of consent	Revocation of consent	Information Interchange
15	Research Organization	Data Receiver	Receives revocation of consent	Revocation of consent	Revocation of consent	Information Interchange
16	Patient (eConsent Portal)	Data Source	Revokes her right of access to share certain SUD message content	Patient's right of access	Revocation of patient's right of access	System
17	Patient (eConsent Portal)	Data Source	Sends revocation of her right of access to	Revocation of patient's right of access	Revocation of patient's right of access	Information Interchange

Step #	Actor	Role	Event/Description	Inputs	Outputs	Type of Requirement
			share certain SUD message content			
18	Statewide eCMS	Data Receiver	Receives revocation of patient's right of access to share certain SUD message content	Revocation of patient's right of access	Revocation of patient's right of access	Information Interchange
19	Statewide eCMS	Data Receiver	The change in her right of access updates the Statewide eCMS	Revocation of patient's right of access	Revocation of patient's right of access	System

Table 5: System Requirements of Consent Scenario 2: Alice Participates in a Research Study

System	System Requirement
Patient (Patient Portal)	Consents to participate in a study
Research Organization	Stores consent to participate
Patient (eConsent Portal)	Signs a right of access form to share certain SUD message content
Statewide eCMS	Stores right of access form
Health Information Network (HIN)	Validates who can receive message content
Patient (Patient Portal)	Revokes consent to participate
Patient (eConsent Portal)	Revokes her right of access to share certain SUD message content
Statewide eCMS	The change in the right of access updates the Statewide eCMS

7.0 High Level Business Issues and Obstacles

- Limited experience in the healthcare industry with electronically making data sharing decisions based on a combination of variables for granular choice that addresses patient preferences for data sharing based upon diagnosis, source of treatment, type of treatment, data recipient, and purpose of data use
- There are complex and variable federal, state, and local laws and regulations for capturing granular consent that must also be electronically represented appropriately[8]
- Laws and regulations are subject to change and will require that electronic workflows be updated based on the applicable law at a point in time
- Patients may provide conflicting consent directives, which will be difficult to arbitrate electronically; unless the electronic consent management architecture has mechanisms for preventing conflicting consent directives
- There is emerging experience with the automated enforcement of prohibitions on re-disclosures
- There may be information in a consent directive or transmission wrapper that may be considered sensitive that has been addressed by current consent directive standards, including the HL7 Privacy and Security Healthcare Classification System, the Clinical Document Architecture (CDA) Consent Directive Implementation Guide, Data Segmentation for Privacy (DS4P) CDA Implementation Guide, Data Provenance CDA Implementation Guide, and V2.9 Chapter 2 Message Header Segment
- Electronic consent management systems must be properly configured to avoid providing responses to queries that contain sensitive information
- Ownership of institutions may change resulting in changes to privacy policy and the sharing of accumulated data in ways that are unanticipated by consenters
- To provide some consistency in situations resulting in changes to privacy policies and data sharing agreements, organizations should consider overarching trust frameworks to govern the persistence of consenter preferences using security labels and the requirement of all downstream recipients to comply with the policies

8.0 Dataset Considerations

8.1. Core Consent Directive Data Requirements

The following steps outline the core consent directive workflow that can be used as a starting point to detail workflows for other types of consent directed data sharing.

[8] ONC has worked with the National Governors Association to understand the various complexities in state law to improve information flow between health care entities.
https://www.nga.org/files/live/sites/NGA/files/pdf/2016/1612HealthCareRightInformation.pdf

- **Step 1** - Patient (eConsent Portal) Data Source *adds* doctor to her care team to allow doctor access to her SUD health information
- **Step 2** - Data Requestor *sends* request to statewide eCMS for an active consent for patient's information
- **Step 3** - Statewide eCMS Data Source *receives* request and *sends* acknowledgement of active consent on file
- **Step 4** - Urgent Care Clinic Data Receiver *receives* acknowledgement of active consent on file

The following list provides examples of other types of granular consent directives that could also be further developed based on this core consent directive workflow. While there are numerous state laws stipulating additional protections for sensitive health information, which require granular consent, this list is focused on federal privacy laws governing specially protected information.

Table 6: Types of Consent Directives that can be Granular

Types of Consent Directives that can be Granular	Description
HIPAA Authorization (45 CFR 164.508)	Mandated for purposes other than treatment, payment, operations (e.g., marketing and research), and other allowable uses and disclosures under HIPAA. A patient may specify which records to send to, e.g., an attorney related to a pedestrian accident.
HIPAA Consent	Not legally required, but voluntarily used to obtain consent for uses and disclosures of protected health information for treatment, payment, and health care operations.[9] A patient may, for example, ask for specific restriction on disclosure of records of specific types, instances, purposes of use, and recipients.
Informed Consent for Research (45 CFR 46.116)	An individual's agreement to participate in a research study including a description of the study, anticipated risks and/or benefits, and how the confidentiality of records will be protected. A patient may have discretion to limit information shared with a research project to more granular research purposes of use, e.g., not for genomic research.
Compound Authorization (45 CFR 164.508)	An authorization for the use or disclosure of protected health information for a research study may be combined with Informed Consent for Research for the same or another research study. A patient may have discretion to limit research information use and disclosure to certain recipients.
HIPAA Individual Right of Access Request (45 CFR 164.524)	Individuals have a right of access to inspect and obtain a copy of their protected health information in a designated record set. Individuals can exercise this right to pass certain information held by one entity to another. An individual has the right to specify the portion of the designated record set to be copied or disclosed. This may include specifying record types and instances by condition, e.g., only medications not related to SUD or human immunodeficiency viruses (HIV), and may include limiting recipient's purposes of use.

[9] No mandated terms are included in a HIPAA Consent, and this term is often used interchangeably with HIPAA Authorization, and may contain similar policy elements. Non-covered entities such as a HIE sometimes require that patients opt-in for collection and use of information by and disclosure through the HIE. While these HIE opt-in authorizations are generally referred to as Consents, they include HIPAA Authorization policy elements, as well as policy elements from other national privacy laws such as 42 CFR Part 2, state privacy laws, and HIE organizational policies

Types of Consent Directives that can be Granular	Description
Consent Requirements (42 CFR 2.31)	Consent to disclose a specific amount and kind of information, including an explicit description of the SUD information to be disclosed, the specific purposes of use, and the name of recipient individuals, treating provider, payer, or entities without a treatment or payer relationship, such as health information exchange or research institution, and the name of individual participants, treating provider participants, or general designation of an individual or entity participant(s) or class of participants that must be limited to a participant(s) who has a treating provider relationship with the patient whose information is being disclosed.

8.2. Dataset Considerations: Query for Consent Location

The following consent dataset tables are intended to capture the information in a request and response for consent location as well as a query for a consent directive. While the consent dataset is neutral to consent storage and retrieval architecture, a potential implementer may leverage these in a manner that is compatible with their architecture.

Table 7: Dataset Considerations: Query for Consent Location

Section	Data Element	Data Element Description
Query for Consent Location	Patient Identifier	Identifier for the patient who is the subject of the consent
	Patient Name	Name of the patient who is the subject of the consent
	Administrative Gender	Female/ Male/ Unknown
	Patient Date of Birth	Birth date of the patient
	Patient Address	Address of the patient
	Requester ID	The unique identifier for the person or organization requesting the consent directive
	Requester Name	Name of the person requesting the consent directive
	Requester Organization	Organization that the requester is associated with or the organization that is requesting the consent.
	Requester Address	Address of the person or organization requesting the data
	Requested User(s)	Person, organization, or role permitted to use the data
	Requested Purpose(s)	Purpose for which the data may be used
	Requester Role	Role of patient requesting patient data
	Consent Originator ID	Unique identifier for the organization that is responsible for the consent
	Consent Originator Organization	Name of the organization that is responsible for the consent
	Community ID	How you request documents across HIE's
	Document ID	An identifier for the patient consent directive document

Table 8: Dataset Considerations: Response for Consent Location

Section	Data Element	Data Element Description
Response for Consent Location	Consent ID	The unique identifier associated with the consent directive
	Patient Identifier	Identifier for the patient who is the subject of the consent
	Patient Name	Name of the patient who is the subject of the consent
	Consent Originator ID	Unique identifier for the organization that is responsible for the consent
	Consent Originator Organization	Name of the organization that is responsible for the consent
	Consent Directive Location	Identifier or other information that will allow the requester to determine where to send the query for the consent directive
	Denial Code	An indicator that the query recipient is unable to respond to the query (should not indirectly expose additionally protected data)

8.3. Dataset Considerations: Query for Consent Directive

Table 9: Dataset Considerations: Query for Consent Directive

Section	Data Element	Data Element Description
Query for Consent Directive	Consent ID	The unique identifier associated with the consent directive
	Patient Identifier	Identifier for the patient who is the subject of the consent
	Patient Name	Name of the patient who is the subject of the consent
	Patient Gender	Male/Female
	Patient Date of Birth	Birth date of the patient
	Patient Address	Address of the patient
	Requester ID	The unique identifier for the person or organization requesting the consent directive
	Requester Name	Name of the person requesting the consent directive
	Requester Organization	Organization that the requester is associated with or the organization that is requesting the consent
	Requester Address	Address of the person or organization requesting the data
	Requested User(s)	Person, organization, or role permitted to use the data
	Requested Purpose(s)	Purpose for which the data may be used
	Information Requested	Information which is being requested (query you want answered)
	Requester Role	Role of patient requesting patient data
	Type of Consent Requested	A code indicating the type of consent directive that is of interest to the requester

Section	Data Element	Data Element Description
	Consent Originator ID	Unique identifier for the organization that is responsible for the consent
	Consent Originator Organization	Name of the organization that is responsible for the consent

8.4. Dataset Considerations: Granular Choice Consent Directive

Table 10: Dataset Considerations: Granular Choice Consent Directive

Section	Data Element	Data Element Description
Consent Directive	Consent Directive ID	Unique identifier that refers to a specific privacy consent directive instance
	Consent Directive Status	Incomplete, Active, Update, Revoked, Inactive, etc.
	Revocation Reason	Code that indicates the reason that consent directive was revoked (Exceptions to default policy)
	Header Security Label	Includes the most restrictive confidentiality privacy tag assigned to any contained content (Also known as the "high water mark"). Includes the minimum necessary Purpose of Use, Obligations, and Refrain privacy tags required for intermediary handling. (Must not include any sensitivity codes. Under certain circumstances determined to be acceptable by risk assessment, privacy marks that may leak sensitivity of content may be included if, for example, the recipient cannot process granular security labeling and there are trust contract provisions that mitigate this risk. Example includes the 42 CFR Part 2 Prohibition against Redisclosure.)
	Confidentiality	The consent directive governed content's classification based on the HL7 Confidentiality code systems, which is a hierarchical code system per H7 Healthcare Privacy and Security Classification System (HCS), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO). Minimum required for access control based on role-based access control (RBAC) or attribute-based access control (ABAC), and likely other authorization provisioning schemes
	Purpose of Use	The types of activities or services that the consent directive allows
	Obligation Code	Obligations to which the recipient must comply (May be multiple)

Section	Data Element	Data Element Description
	Privacy marks	Text that describes the handling caveats, i.e., the obligations, refrains, and purpose of use restrictions that the recipient must comply (May be multiple, includes prohibition on re-disclosure)
	Refrain Policy Code	Prohibitions to which the recipient must comply
	Time period for disclosure of specific record types	Time period for disclosure of specific record types
	Document Image	Copy of the signed consent directive document
	Consent Directive Location	Locator address that may be used by the recipient to retrieve the patient consent directive (This field may be a URL that would allow the recipient to retrieve the consent records)
	Custodian	Organization that has the official record of the consent directive
	Patient/Subject	Person whose records are covered by the consent directive
	Originator	Organization that is responsible for the patient consent directive
	Allowed Recipient	Persons, organizations, and roles that are permitted to use the data (repeating dataset)
	Allowed Information	Types of data that are permitted to be disclosed (repeating dataset)
	Security Labels for Information permitted to be disclosed	Security Labels may be assigned to information content permitted to be disclosed with the following privacy tags: At minimum 1..1 Confidentiality Code and 0..* Sensitivity, Policy, Compartment, Provenance, Integrity, Trust, Purpose of Use, Obligation, Refrain, and Privacy Mark
	Sensitivity	The consent directive governed content's codes sensitivity is based on risks of stigma and other vulnerabilities (e.g., risk of abuse)
	Policy	The consent directive governed content's sensitivity is classified [confidentiality code assigned] based on policy lens(e.g., HIV content under HIPAA has confidentiality code = Normal; HIV under 42 CFR Part 2, Title 38 Section 7332, and various state laws is assigned a Restricted Confidentiality code) Handling caveats, Purpose of Use (POU), Refrain, Obligation, and Privacy Mark labels are assigned based on the resulting classifying Confidentiality code

Section	Data Element	Data Element Description
	Compartment	The consent directive governed content's "need to know" categorization based on the healthcare version of national information security classifications as a "special access program" In healthcare, this equates to Emergency team, Research team, Care team, etc. per local requirements
	Provenance	The consent directive governed content's labeled provenance information, which is "short-hand" for a full Provenance record to enable computable decisions about whether and how to incorporate received content into record systems (e.g., a consent directive can indicate differential handling of patient generated vs. patient reported/provider asserted/provider asserted and recorded information) A patient or the default organizational consent directive provisions may stipulate who can access patient generated content
	Integrity	The consent directive governed content may require differential treatment based on the integrity metrics (e.g., if the content is sourced from a patient selected app, then the consent directive or the organizations default consent directive settings may require that this content be marked at a lower level of integrity confidence)
	Trust	The consent directive governed content may indicate the trust regimes under which it may be exchanged (e.g., a patient portal may only allow a patient to consent to disclose to recipients that belong to approved trust domains)
	Signature	Electronic signature or image of signature
	Signer	Name of person who signed the consent directive
	Relationship of Signer to Patient	Relationship of the person who signed the consent directive to the subject of the consent directive
	Witness	Person who attested to the consent directive signature
	Signature Date	Date the consent directive was signed
	Effective Date/Time	First date and time when the consent directive is in effect
	Expiration Date/Time	Last date and time when the consent directive is in effect
	Expiration Condition	Status that would cause the consent directive to expire

Section	Data Element	Data Element Description
	Expiration Event	Event that would cause the consent directive to expire
	Insurance Type	Source of payment for the services covered by the consent directive (optional)
	Privacy Consent Form ID	Unique identifier for a privacy policy
	Privacy Policy Description	Text description of the privacy policy
	Privacy Policy Type	Reference to the law or policy that governs the consent directive
	Legally Binding Consent Directive Location	Consent directives are often the computable version of a paper or electronic form that is what the patient read and signed (The legally binding consent directive should be locatable)

9.0 Candidate Standards for Consideration

The following standards could be leveraged by a pilot or implementer to exchange granular level data under a granular consent directive. The data elements in section 8: Dataset Considerations are reflected with varying degrees across those listed below.

9.1. For eConsent Form

- FHIR Questionnaire Resource
    - A Questionnaire resource is an organized collection of questions intended to solicit information from patients, providers, or other individuals involved in the healthcare domain. This resource may include simple flat lists of questions or can be hierarchically organized into groups and sub-groups each containing questions. The Questionnaire resource defines the questions to be asked, how they are ordered and grouped, any intervening instructional text, and what the constraints are on the allowed answers. The responses to questions in the Questionnaire resource can be communicated using the QuestionnaireResponse resource.

- FHIR QuestionnaireResponse Resource
    - The QuestionnaireResponse resource provides a complete or partial list of responses to a set of questions included in the Questionnaire resource. The questions may be included directly or by reference to a Questionnaire resource that defines the questions as well as the constraints on the allowed answers. In some cases, both formal rules for editing the questionnaire (via link to Questionnaire) and local information to allow rendering of the questionnaire may be provided.
    - Each time a questionnaire is completed for a different subject or at a different time, a distinct QuestionnaireResponse is generated, though it may be possible for a previously entered set of answers to be edited or updated.

9.2. For Encoded Report About A Consent Directive

- HL7 Version 2.x (V2) Consent Segment in a Medical Document Management Message[10]
- FHIR Consent Resource[11]
    - This resource can contain a record of a healthcare consumer's choices, which permits or denies identified recipient(s) or recipient role(s) to perform one or more actions within a given policy context for specific purposes and periods of time.
    - Requires FHIR Provenance to convey consenter's signature.
    - Is a "report" about the existence of a paper or electronic legally binding consent directive but is not an encoding of a legally binding consent directive.

9.3. For Encoded Legally Binding Consent Directive

- HL7 CDA® R2 Implementation Guide: Privacy Consent Directives, Release 1[12]
- FHIR Consent
    - This resource can be used with type valued as a privacy consent directive, to be considered legally binding in jurisdictions that recognize electronically executed contracts.

9.4. Difference Between the FHIR Consent and FHIR Contract Resources

- The FHIR Consent status "indicates the current state of this consent" by pointing to the consent directive.[13] For example, when a FHIR Consent instance is revoked, it means the "report" is rescinded.
- In contrast, the FHIR Contract resource is "the status of the resource instance", which is the contract business workflow step. This means that the instance has been revoked rather than a report that the instance has been revoked.[14] When a FHIR Contract consent directive's status is "revoked", it means that the consent directive is no longer legally binding.
- The FHIR Consent can report on the revocation of an instance of a FHIR Contract typed as a consent directive.

9.5. Consent Standards Not Included

Candidate standards IHE Basic Patient Privacy Consent (BPPC) or IHE Advanced Patient Privacy Consent (APPC) were not included at the time of authoring this report due to interoperability limitations and lack of support for security labeling.

The IHE Basic Patient Privacy Consent (BPPC) and Advanced Patient Privacy Consent (APPC) specifications were considered as Candidate Standards during the use case development for the Basic Choice Phase of the Patient Choice Technical Project. The findings summarized in the Patient Choice Use Case Working Session, March 25, 2016, determined that while these two specifications are interoperable within a given IHE Affinity Domain, they are not interoperable outside of a particular Domain and the Basic Patient Choice candidate standards did not include IHE BPPC or APPC:

[10] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=185
[11] https://www.hl7.org/fhir/consent.html
[12] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=280
[13] http://build.fhir.org/consent-definitions.html#Consent.policy
[14] http://build.fhir.org/contract-definitions.html#Contract.status

1) Each IHE Affinity Domain must be federated HIEs architected according to IHE XDS.b with an IHE conformant registry and repository, which support only CDA document exchange while many HIEs either do not fully support CDA documents and/or also support other consent directives and content standards (e.g., those that predominately push HL7 Version 2 Admission, Transfer, Discharge messages, and may communicate consent directives using HL7 MDM Consent message);
2) Each IHE Affinity Domain must agree out-of-band to accept the underlying consent policies either as OIDs referencing unstructured consent forms or eXtensible Access Control Markup Language (XACML) representations of a patient's choice that agrees or disagrees with one or more XACML base policies agreed to by the Affinity Domain;
3) BPPC does not represent interoperable security labels at all;
4) APPC only supports the confidentiality and purpose of use privacy tags rather than the minimum set needed to computationally represent consent directives in interoperable security labels; and
5) APPC recipients outside of the source Affinity Domain (a) may not support XACML for access control, and/or (b) would not be willing to consume a patient's XACML consent directive because of liability for breach, i.e., because there is no one way to write an instance of a patient's XACML consent directive.

9.6. Candidate Standards for Vocabulary

- HL7 Healthcare Privacy and Security Classification System (HCS)[15]

[15] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=345

Appendix: Glossary

Definition	Description
42 CFR Part 2	Regulation that addresses the limitations on the release of patient information related to treatment in a federally-designated Alcohol and Drug Abuse Treatment Program (Reference 42 CFR § 2.13).
HITECH §13405 and Proposed Rule 45 CFR Part 164.522(a) (1) (iv)	Regulation that addresses the rights of patients to restrict the sharing of their health information with payers for self-pay care.
Accounting of Disclosures	A listing of the disclosures of an individual's individually identifiable health information as limited by the HIPAA Privacy Rule (45 CFR § 164.528).
Additional Protected Patient Data	Patient healthcare data for which there are legal or regulatory constraints on the sharing of the data that go beyond those defined under HIPAA.
Authorization	Method and form to secure permission from an individual for the use or disclosure of individually identifiable health information for any activity not specifically allowed without one. Uses and disclosures related to treatment, payment, and healthcare operations generally do not require a HIPAA authorization; but some non-healthcare related activities such as marketing do. Authorization is a new term used in the HIPAA Privacy Rule to denote an activity that has often been called a consent or a release (Per 42 CFR § 2.13 and 38 CFR § 1.475).
Consent or Consent Directive or Consent Document	The record of one or more instruction(s) regarding an individual's privacy preferences that a provider or organization agrees to or is required by law to enforce.
Consent Management	Consent management is a system, process, or set of policies for allowing consumers and patients to determine what health information they are willing to permit their various care providers to access. It enables patients and consumers to affirm their participation in e-health initiatives and to establish privacy preferences to determine who will have access to their protected health information (PHI), for what purpose, and under what circumstances. Consent management supports the dynamic creation, management, and enforcement of consumer, organizational, and jurisdictional privacy directives.
Consent Metadata	The minimum consent content necessary to determine who may send and receive PHI/ Specially Protected Information (SPI) and is derived from a Consent Document.
Consent Subject	The person whose data is covered by the consent directive.
Coordination of Care	1. Monitoring a person's goals, needs, and preferences. 2. Acting as the communication link between two or more participants concerned with a person's health and wellness. 3. Organizing and facilitating care activities and promoting self-management by advocating for, empowering, and educating a person. 4. Ensuring safe, appropriate, non-duplicative, and effective integrated care.

Definition	Description
Diagnosis	Identification of a disease or condition by a scientific evaluation of physical signs, symptoms, history, laboratory test results, and procedures.
Disclosure	Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information (HIPAA Section 160.103).
Electronic Health Record (EHR)	An electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. The EHR can generate a complete record of a clinical patient encounter—as well as supporting other care-related activities directly or indirectly via interface—including evidence-based decision support, quality management, and outcomes reporting.
Health Information Organization (HIO)	An organization that oversees, governs, and provides services to enable the exchange of health-related information among disparate healthcare information systems.
Healthcare Payers	Insurers, including health plans, self-insured employer plans, and third-party administrators providing healthcare benefits to enrolled members and reimbursing organizations
Healthcare Provider	Refers to a person licensed, certified, or otherwise authorized or permitted by law to administer healthcare in the ordinary course of business or practice of a profession, including a healthcare facility. This includes primary care providers, other physicians, nurse practitioners, physician assistants, etc.
Information Interchange Requirements	Specifies the transactions that are exchanged between systems and the role of each system in the exchange
Message Content	Information related to a consumer and their consent for sharing their SPI and/or PHI with specific named recipients, may be derived from a Consent Document.
Patient	Person who is the recipient of healthcare services. For the purposes of the Data Segmentation Use Case, the patient is the subject of the consent, consent directive, or authorization.
Preference	A patient request regarding the use and disclosure of his or her health information. Preferences can be recorded but would not be enforced until there was an agreement by one or more providers to implement the preference.
Primary Care Physician (PCP)	A primary care physician is a generalist physician who provides care to the patient at the point of first contact and takes continuing responsibility for providing the patient's care.
Privacy Policy Model	An abstract representation of the variables or rules that can be associated with data to express the constraints that can be imposed on data sharing. The Policy Model may also be used to define and communicate constraints that emanate from sources

Definition	Description
	other than patient preferences, e.g., laws, regulations, and organizational practices.
Protected Information	Information that is protected by a security policy. In healthcare, this includes a variety of clinical and administrative information that can be identified as belonging to a specific patient.
Provider	An individual clinician in a healthcare delivery setting.
Provider Organizations	Organizations that are engaged in or support the delivery of healthcare. These organizations could include hospitals, ambulatory clinics, long-term care facilities, community-based healthcare organizations, employers/occupational health programs, school health programs, dental clinics, psychology clinics, care delivery organizations, pharmacies, home health agencies, hospice care providers, and other healthcare facilities.
Specialist	A physician who has completed sub-specialty training beyond his or her initial residency.
Specially Protected Information (SPI)	Health information that is protected beyond the scope of HIPAA such as under 42 CFR Part 2, the Michigan Health Code, or other state or federal privacy laws.
Substance Use Disorder (SUD)	"Recurrent use of alcohol and/or drugs [which] causes clinically and functionally significant impairment, such as health problems, disability, and failure to meet major responsibilities at work, school, or home."[16]
System Requirements	Requirements internal to the system necessary to participate successfully in the transaction.
Treatment	The management and care of a patient condition in order to reduce or eliminate the adverse effects upon the patient.

[16] SAMHSA. *Mental Health and Substance Use Disorders.* Accessed 13 January 2020. https://www.samhsa.gov/disorders/substance-use