Use Case Summary

Use Case Name:	Consumer Consent Information
Sponsor:	Michigan Department of Health and Human Services
Date:	March 6, 2019

Executive Summary

This brief section highlights the purpose for the use case and its value. The executive summary gives a description of the use case's importance while highlighting expected positive impact.

State and federal laws offer privacy protection for individuals and their health information. Certain categories of health information require greater protection than physical health information. For example, state and federal laws require healthcare providers to obtain written consent from a patient before disclosing behavioral health or substance use disorder information to another person or organization.

Although laws require this written consent, there has been no standard written form for patients to use for providing consent. This lack of standardization has led to confusion and conflicting consent forms, and has become a barrier to information sharing and care coordination.

Purpose of Use Case: The Consumer Consent Information use case addresses the need for a standard, shared way to manage consent forms and consent-related information in a health information exchange (HIE) environment. This use case helps organizations determine what information, if any, a patient has consented to share and with which providers the information may be shared.

Overview

This overview goes into more details about the use case.

Some states have attempted to address security concerns around health information by legislating standard consent forms that will be accepted and honored on a statewide basis.

There is also a need for a standard statewide method for consumer consent information to be electronically stored, managed, found, revoked, or deleted when expired.

This use case enables a standard, statewide service to easily find and manage consent information, so that healthcare providers can quickly determine whether they can share specially protected health information. The use case also enables better privacy and protection for patient health information.

This use case utilizes the Statewide Consumer Directory (SCD), as well as one or more electronic consent management service (eCMS) repositories containing patient consent forms that are connected to HIE organizations.[1]

The SCD helps patients make sure their health information is available to their chosen healthcare providers when needed. A short video summary of the SCD is available at: https://www.youtube.com/watch?v=1YyqMm8H1w0.

For this use case, mental health and substance use disorder records are referred to as "behavioral health information." Behavioral health information should be distinguished from "physical health information," which is generally shareable without consent for the purposes of Treatment, Payment, and Operations (TPO) under the federal Health Insurance Portability and Accountability Act (HIPAA).

Historically, the behavioral health community has been limited in its ability to participate in the electronic exchange of health information because the disclosure of behavioral health information requires more specific consent than is required under HIPAA, as mandated in Michigan by 42 CFR Part 2 and the Michigan Mental Health Code.

According to the report "An Electronic Consent Management Architecture to Support Behavioral Health Information Exchange in Michigan" by the CIO Forum Data Exchange Workgroup (a leadership forum for Chief Information Officers (CIOs) from Community Mental Health Service Providers and Pre-Paid Inpatient Health Plans)[2], two components must be in place for the behavioral health community to participate fully in the sharing of health information:

1. *A standard, statewide behavioral health consent form for care coordination purposes.* Such a form, accepted by all parties, would allow consumer consent to be collected wherever the consumer is present and shipped electronically to providers and health information exchanges (HIEs) that need this consent to release information.[3] A

[1] Because there are multiple HIEs in Michigan, there can be more than one eCMS. The SCD helps coordinate between the eCMS repositories so that consent can be managed or queried on a statewide basis.

[2] Chief Information Officers Forum Data Exchange Workgroup, *An Electronic Consent Management Architecture to Support Behavioral Health Information Exchange in Michigan*, March 26, 2015.

[3] "Consent to Share Behavioral Health Information for Care Coordination Purposes," Michigan Department of Health and Human Services, (Lansing: DCH-3927), accessed January 16, 2017, https://www.michigan.gov/documents/mdch/DCH-3927_Consent_to_Share_Health_Information_477005_7.docx

standard form facilitates care coordination and supports integration of physical and behavioral healthcare.

2. *Description, specifications and implementation of an eCMS.*[4] For an HIE to efficiently and effectively handle behavioral health consent, it needs to be consistent with the consent methodologies of other HIEs. This allows interoperability.

The approach recommended by the CIO Forum allows the behavioral health community to transition from a paper- and fax-based system of communicating patient privacy and consent preferences to an electronic system that supports data sharing (including Continuity of Care Documents) while maintaining compliance with federal and state laws, including 42 CFR Part 2 and the Michigan Mental Health Code, respectively.

The Consumer Consent Information use case includes the CIO Forum's recommendations and reflects the eCMS architecture (discussed more fully in the use case implementation guide).

Persona Story

To explain this use case, this section follows a persona example from start to finish.

Alex Gonzales and his family have been going through some difficult times. A motorcycle accident left him disabled, and he was recently let go from his job as an auto mechanic.

Alex has always been a private and proud individual, and his new life has challenged that attitude. He feels like he has lost control of his privacy and his own life. Events from his past keep coming up with caregivers, even reaching back to a problem he had with alcohol before his marriage. Everything from Alex's past seems to be in his health records and it makes him feel uncomfortable every time he sees a healthcare office worker open a file or type on a laptop.

Recently, Alex has been working with a care coordinator as he considers a move to a new city. Alex sees the move as a chance for him and his family to start afresh, but he is concerned about his healthcare information and his past coming back to haunt him. Having just built up trust and rapport with his current healthcare providers, Alex doesn't like the idea of sharing his health information with strangers at new healthcare institutions. And he

[4] An electronic consent management service (eCMS) is a repository that stores original consent data and documents and may be associated with one or more HIEs and/or healthcare organizations.

is concerned that his health information could leave the doctor's office. What if a new employer found out about his former alcohol addiction?

His care coordinator was able to reassure Alex that modern protections will keep his information safe. Their practice participates in the Consumer Consent Information use case, which means the forms Alex signs relating to his private information are automatically checked any time someone wants access to Alex's information. This gives Alex an added comfort regarding his privacy, ensuring control over his information, and his past, are in the right hands. His own.

Diagram

This diagram shows the information flow for this use case.

Sending Consent

The satellite eCMS can register a consent with the SCD – simply notifying SCD that a consent exists between two parties for a certain period. The satellite eCMS provides metadata about the consent form to the shared eCMS for storage, but does not share the actual consent form.

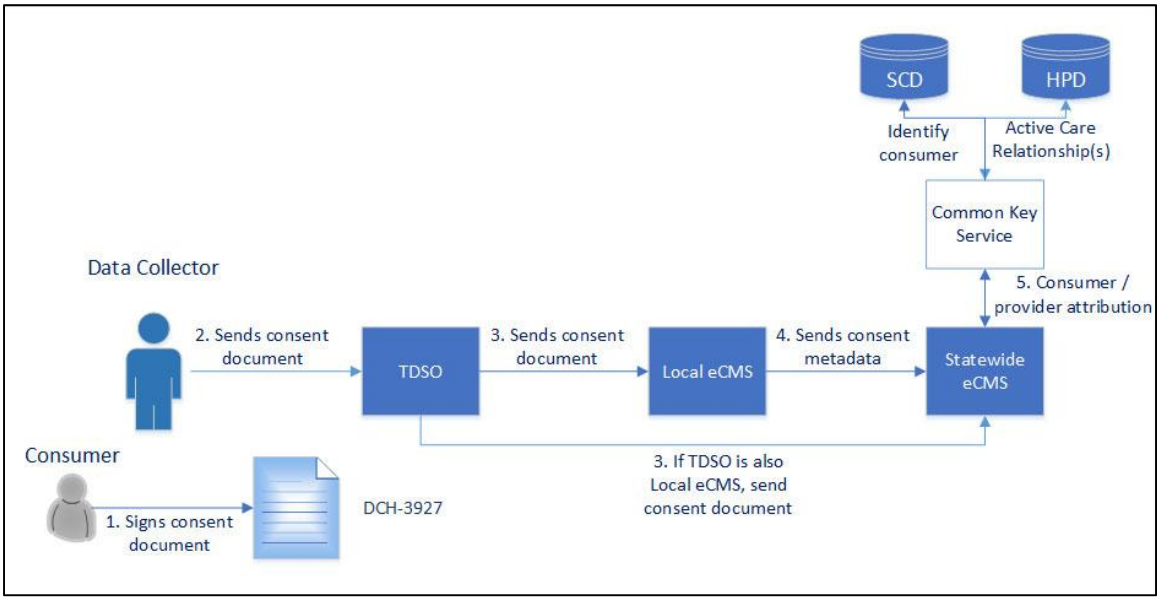

Figure 1. Send Consent Data Flow Example

This is the most frequent transaction for data collectors. A data collector obtains a consumer's consent document (on paper or in an electronic form) and creates a computable representation of that consent form as a consent document (as a scanned .pdf if on a paper form).

Upon receipt of a consent document the local eCMS validates and stores the consent document. The local eCMS stores the consent document in its repository and sends the metadata it derives from the document to the statewide eCMS. Figure 1 and the steps listed below depict the scenario for the Send Consent Registration process.

1. A consumer is referred to a specialist by his Primary Care Provider (PCP) during a visit. The consumer signs a DCH-3927 (consent document) in order to permit his Specially Protected information (SPI) to be shared with the specialist to whom he is being referred
2. The PCP sends an electronic, structured, representation of the consent document to a TDSO by way of their EHR
3. The TDSO sends (forwards) the electronic consent document to local eCMS
4. Local eCMS parses and stores the electronic consent document and sends relevant metadata to the statewide eCMS
5. The statewide eCMS uses the Common Key Service (CKS) as part of the identity matching, and updates the SCD and Health Directory with the metadata it receives from local eCMS

Revoking Consent

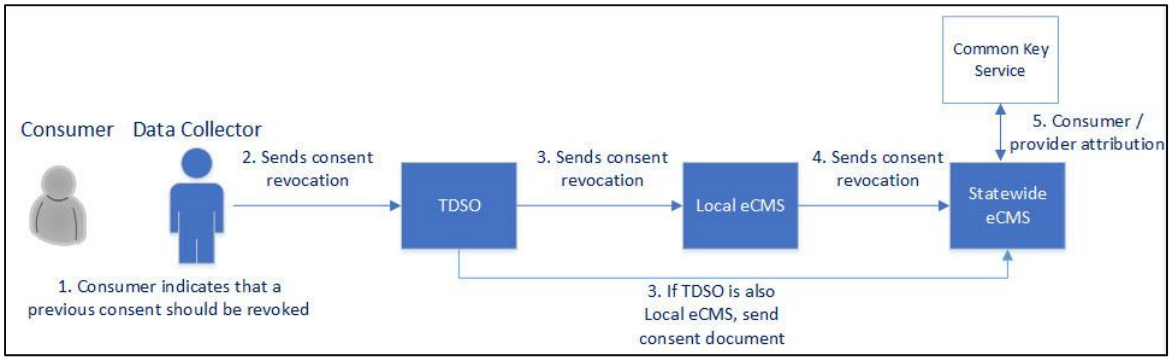

Figure 2. Revoke Consent Data Flow Example

A consumer may revoke (cancel) the consent document before its expiration data. Figure 2 and the steps listed below depict a scenario for the Send Consent Revocation process:

1. A consumer decides to revoke his previously signed consent document, which previously authorized sharing SPI with a PCP
2. The consumer's new PCP creates his Consent Revocation document and sends it to a TDSO
3. The TDSO sends the Consent Revocation to a local eCMS
4. Upon receiving a Consent Revocation, the local eCMS stores the consent document in its repository and sends updated metadata indicating the revocation to the statewide eCMS
5. The statewide eCMS uses the Common Key Service as part of the identity matching, marks the existing consent metadata registration as revoked

If the consumer wishes to continue sharing his SPI with other providers, the consumer's new PCP must obtain an updated and signed Consent Form and submit his new consent document to a TDSO. The TDSO then takes the same steps as if the consumer was beginning the Consent Registration.

Find/Send Active Consent

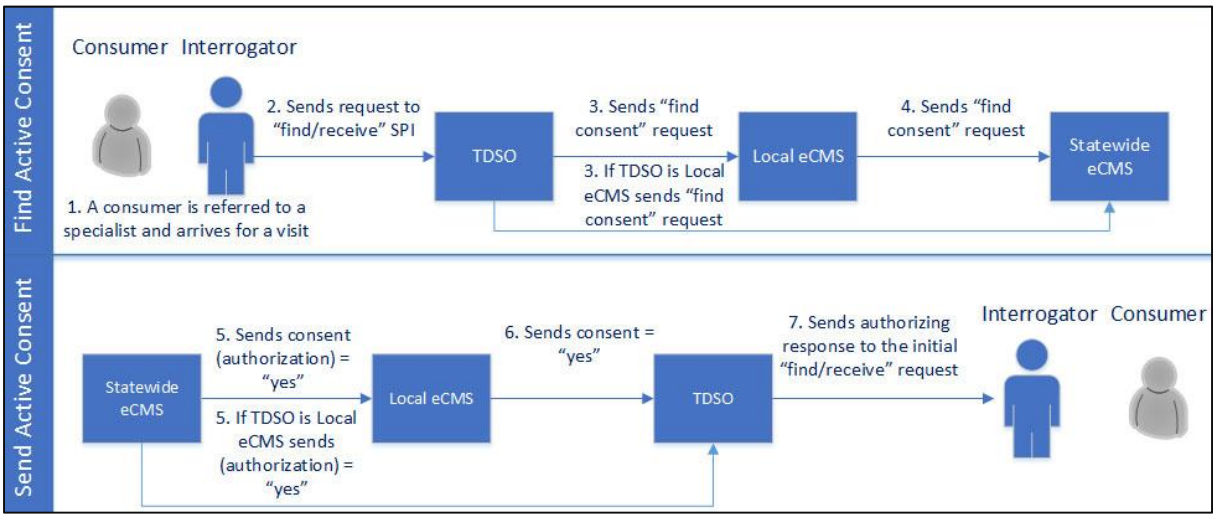

Figure 3. Request Consent Status Data Flow Example 1

An interrogator may check to see if consent is on file by sending a Find Active Consent request to the local eCMS. The local eCMS sends a response to the interrogator, completing the Find/Send Active Consent Process.

1. A consumer is referred to a specialist for symptoms of anxiety
2. The specialist wants to pre-check the consumer's healthcare history and sends a Find Active Consent request to the associated TDSO
3. The TDSO sends the Find Active Consent request to a local eCMS
4. The local eCMS sends the Find Active Consent request to the statewide eCMS
5. The statewide eCMS determines that consent is provided for the specialist and replies with a "consent in place" message to the local eCMS
6. The local eCMS sends the authorizing message to the specialist's TDSO
7. The TDSO sends the authorization to the consumer's specialist so that the specialist's request to receive the consumer's SPI can be fulfilled

Find/Send Consent Document

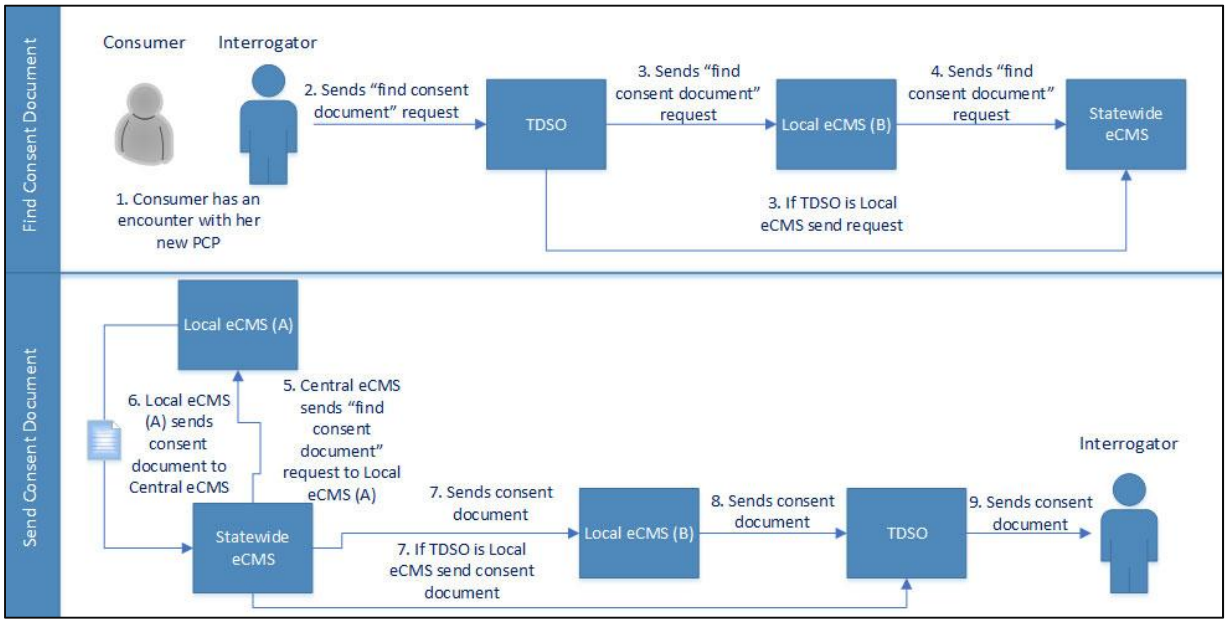

Figure 4. Request Consent Status Data Flow Example 2

The Find/Send Consent Document Use Case allows the interrogator to request a consent document(s) by providing a consent document handle. Most interrogator will be restricted to only obtain the current consent document while a limited set of interrogators such as auditors may be allowed access to current and past consent documents.

1. A consumer decides to change PCPs and arrives for her first visit with her new provider
2. The new PCP attempts to obtain the consumer's most recent consent document by sending a request to their TDSO
3. The TDSO sends (forwards) the request to local eCMS
4. The local eCMS sends (forwards) the request to the statewide eCMS
5. The statewide eCMS receives the query from eCMS and checks its registry to determine which local eCMS is storing the consumer's active (most recent) consent document. Having determined that the consumer's active consent document is stored in eCMS, the statewide eCMS sends a request to retrieve it
6. Local eCMS sends a redacted consent document to the statewide eCMS sends a request to retrieve it
7. The statewide eCMS sends the redacted consent document to local eCMS
8. Local eCMS sends the redacted consent document to the PCP's TDSO
9. The TDSO sends the redacted consent document to the PCP in response to the initial query

Please note: SCD will only return a value of "consent in place for named recipient" or "consent not in place for named recipient." It will not disclose if a prior consent has expired or been revoked.

Regulation

This section describes whether this use case is being developed in response to a federal regulation, state legislation or state level administrative rule or directive.

Legislation/Administrative Rule/Directive:

☒ Yes
☐ No
☐ Unknown

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- 42 CFR Part 2 (Code of Federal Regulations)
- Violence Against Women Act
- Family Violence Prevention and Services Act

HIPAA establishes a minimum of safeguards for protected health information. This federal law applies no matter how health information is shared, whether electronically, in writing, or verbally. In general, HIPAA allows protected health information to be shared for the purposes of treatment, payment, and health care operations (TPO). By signing a Notice of Privacy Practices acknowledgement with a healthcare provider or health system, a consumer is effectively acknowledging they understand that providers can share their physical health information among other providers and payers for TPO purposes as specified under HIPAA.

42 CFR Part 2 requires consumer consent for the disclosure and use of consumer records for alcohol and drug use, which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program.

Federal Guidance

- "Applying the Substance Abuse Confidentiality Regulations 42 C.F.R. Part 2 (Revised)" (2011), http://www.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs

Michigan Laws

- Michigan Mental Health Code: Public Act 258 of 1974, MCL 330.1001 et. seq.
- Michigan Public Act 129 OF 2014 - establishes statewide standard consent form for those involved in treatment

Multiple state and federal laws govern confidentiality of health information limiting how healthcare providers, payers and others can share health information.

Other health information is much more restricted by state and federal law. 42 CFR Part 2 requires consumer consent for the disclosure and use of consumer records for alcohol and drug use, which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program. The Michigan Mental Health Code (MCL 330.1748) also requires consent prior to the disclosure of a recipient's mental health records. For 42 CFR Part 2 and the Michigan Mental Health Code, providers must obtain consent to share mental health and substance use disorder records, unless the disclosure falls within one of the enumerated exemptions to consent, such as a medical emergency (called "break the glass").

In accordance with Public Act 129 of 2014, MDHHS released a statewide standard consent form on January 1, 2015. Michigan's standard consent form is designed to meet the requirements of 42 CFR Part 2 and Michigan's Mental Health Code for care coordination purposes.

Meaningful Use

☒ Yes
☐ No
☐ Unknown

This use case does not singularly meet any requirements of Meaningful Use; however, this use case may help facilitate exchange of information, which can assist in meeting Meaningful Use requirements.

Cost and Revenue

This section provides an estimate of the investment of time and money needed or currently secured for this use case.

Costs

There are two costs associated with this use case.

- The cost of implementing this use case, which requires the use of new and existing infrastructure and is estimated to be in the high six figures. New infrastructure required for this use case includes deploying a shared electronic consent management service (eCMS) that records "metadata" from all other eCMS instances statewide, the cost for which is still being determined.
  - This shared eCMS must be integrated with SCD. The cost for integration and testing with the SCD is included in the estimate for this use case.

- The other potential cost for this use case is that of not implementing it. This cost is estimated to be millions of dollars in annual waste due to difficulties and delays storing, managing, coordinating, and communicating behavioral health information, as well as potential damages from improperly communicated consumer information.
  - Implementing this use case can also reduce the annual costs of maintaining and supporting multiple disconnected repositories of consumer consent forms, which is estimated to be millions of dollars per year.
  - Implementing this use case will accelerate the adoption of a statewide standard consent form (both paper and electronic) which also leads to immense cost reductions, particularly in areas such as diversions and related legal and judicial costs.

The return-on investment for successfully implementing and adopting this use case is good – a high six-figure investment for a potential high nine-figure return.

Revenues

The cost savings and workflow efficiencies achieved by enabling healthcare providers to more easily store, manage, locate and access consumer consent information should prompt stakeholders to subscribe to this service. The pricing model will likely vary by participating organization, and may be similar to a data plan offered by a wireless carrier. This could include a base fee for a certain number of data-sharing transactions with additional per-transaction fees for notifications beyond that baseline on a monthly basis. Storage of consumer consent information (meta-data) may also be offered as a fee-based service.

Stakeholders who may wish to participate in the electronic exchange of consumer consent forms include but are not limited to:

- Providers
- Prepaid inpatient health plans (PIHPs)
- Community mental health agencies
- Hospitals
- Specialists
- Home health care / Long-term and post-acute care / Skilled nursing facilities
- Rehabilitation centers
- Payers
- Pharmacies
- Health plans / payers
- Accountable care organizations or health homes

This section will be updated when the full revenue model for this use case is finalized.

Implementation Challenges

This section describes the challenges that may be faced to implement this use case.

While much of this use case utilizes existing MiHIN infrastructure, the establishment of a shared eCMS that coordinates other eCMS instances is a new infrastructure and will necessitate spending time and effort to properly scope project requirements, to find the right vendor for the project, and to implement an eCMS that is integrated with the rest of MiHIN's existing infrastructure. Implementation costs for this shared "metadata" eCMS are not fully defined and will need to be modified to accommodate vendor pricing and capabilities of the selected eCMS.

Other challenges include:

- Encouraging TDSOs to prioritize this use case to ensure they properly connect to the shared eCMS and to satellite eCMS solutions to receive and respond to requests for consent
- Educating healthcare providers on the new solution and encouraging them to use it
- Helping to define new workflows to support the electronic exchange of consumer consent information

Vendor Community Preparedness

This section addresses the vendor community preparedness to readily participate in the implementation of this use case.

One of Michigan's behavioral health technology vendors and at least one of Michigan's HIEs have implemented electronic consent management functionality that is in production, using an electronic version of the standard behavioral health consent form. These organizations are in the process of updating and modifying to align with the latest eCMS specification[5] and have expressed interest in utilizing a shared eCMS solution to support customers statewide. The eCMS specification is modeled after the "Query By Parameter (QBP)" specification standardized by the Centers for Disease Control (CDC). It was created for use in querying an Immunization Information Systems (IIS) such as the Michigan Care Improvement Registry (MCIR) for an immunization history and forecast.

[5] "An Electronic Consent Management…"

Since MiHIN's Immunization History-Forecast use case, which uses QBP, is anticipated to be a high-demand use case, organizations building or buying their own eCMS are likely to implement the QBP specification that the Immunization History-Forecast use case and eCMS share in common.

Other behavioral health solution vendors serving Michigan have conveyed intentions to participate in a statewide solution to improve data sharing needs of the behavioral health community while adhering to state and federal regulations and the eCMS specification.

PIHPs are dependent on their vendors' participation (e.g. PCE Systems, Streamline, NetSmart).

Some TDSOs, including qualified organizations (such as Washtenaw County Community Support and Treatment services), have deployed eCMS solutions for their customers to enable sharing behavioral health information.

Other qualified organizations, like Northern Physicians Organization (NPO), have developed their own consent and behavioral health information sharing solutions. There may be challenges to determining how the Consumer Consent Information use case can complement and augment these existing solutions, and whether existing solutions can conform to the eCMS protocol specification.

The transport of consent information may not be included as base functionality for some electronic health record vendors; however, if it is not a current functionality, it is likely to be on their future road map due to the above reasons

Support Information

This section provides known information on this support for this use case.

Political Support:

☒ Governor
☒ Michigan Legislature
☒ Health Information Technology Commission
☒ Michigan Department of Health and Human Services or other State of Michigan department
☐ CMS/ONC
☐ CDC
☒ MiHIN Board

Concerns/Oppositions: There are general concerns about implementing behavioral health information sharing in accordance with SAMHSA and 42 CFR Part 2. Specific concerns have been raised about whether each HIE, HIN, or other HIO in a network must be named as a "recipient" by a patient giving consent based on an FAQ published by SAMHSA (see FAQ link in the Regulation section of this document).

Sponsor(s) of Use Case

This section lists the sponsor(s) of the use case

- Michigan Department of Health and Human Services

Metrics of Use Case

This section defines the target metrics identified to track the success of the use case.

Connecting one or more TDSOs (each with a satellite eCMS) to the shared eCMS and SCD so that consent forms can be loaded (sent), found, revoked and received from another TDSO.

Metrics to measure the success of the use case can include:

- Number of TDSOs connected with a satellite eCMS to the shared eCMS and SCD
- Number of providers using this use case
- Number of consent "metadata" records sent to shared eCMS
- Number of consent "metadata" records queried by providers through shared eCMS

Other Information

This section is provided to give the sponsor(s) an opportunity to address any additional information with regard to this use case that may be pertinent to assessing its potential impact.

Consent for Minors

Some of the statutory and regulatory requirements that govern privacy and consent for the

sharing of health information for minors differ from the consent requirements for adults. The unique privacy and consent requirements for minors fall into two categories:

1. Designation of the age that a minor may consent to disclose health information
2. Restrictions and regulations on when a parent may access health information on a minor who has reached adulthood and/or the age of consent

These regulations and restrictions must be addressed in the Consumer Consent Information use case before sensitive health information for minors can be shared electronically.

The requirements for handling consent for minors are not yet fully reflected in this summary and must still be developed.