Use Case Summary

Use Case Name:	Electronic Consent Management Service (eCMS)
Sponsor:	Michigan Department of Health and Human Services, Michigan Health and Hospital Association
Date:	September 30, 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.

While the sharing of physical health information has been widely successful throughout Michigan, behavioral health is not being shared in a meaningful way. This is, in large part, due to federal and state laws and regulations, which place additional protections on certain pieces of health information called specially protected information (SPI). The most common protection attached with SPI is a requirement that consumer consent be obtained before any information is shared. A common example of SPI is information that comes from a 42 CFR Part 2 Facility, which handles substance use disorder information.

The case for requiring consumer consent is not trivial, and it is the direct result of discrimination of healthcare consumers in the past; however, it has resulted in confusion when patients do not know when they should be filling out consent forms and how to share their information with relevant individuals when they wish to do so.

Additionally, even when patients are aware that a consent form must be filled out, there are many inefficiencies with the current paper-based consent landscape. Patients can find themselves filling out multiple forms for different areas of specially protected information, they often need to fill out a new consent form at each new provider they see, and it is very difficult for patients to keep track of their consent preferences in a centralized location to make sure they are up to date.

The ultimate result of a patient being unaware that a consent form is needed or being unable to navigate the complexity of a paper-based system, is that specially protected information ultimately remains in a silo and is not shared as a part of that patient's history with pertinent providers.

This becomes particularly problematic in behavioral health situations where members of a patient's active care team will need timely information on that patient to appropriately ensure care is being coordinated during a health event. While Admissions, Discharge, and Transfer (ADT) notifications serve this need in the physical health space, behavioral health ADTs have not been possible due to the consent piece that is not required of physical health information.

ADT notifications are valuable because they can inform all members of a patient's care team—from specialists to doctors to health plans—about a patient's health events, strengthening connections between patients and their support systems and helping healthcare providers work together.

For these notifications to be sent with all pertinent information, the inefficiencies in the consent landscape must be solved by forming a solution that allows consent to be obtained in a convenient way, in one centralized location, in real time.

Purpose of Use Case: The Electronic Consent Management Service (eCMS) use case allows behavioral health providers to participate in the statewide exchange of health information via ADT notifications by creating a two-part solution, which would allow providers to electronically check consent and would subsequently allow for a consent check by a Health Information Network (HIN) before ADT messages containing specially protected information (SPI) are sent.

Overview

This overview goes into more details about the use case.

Electronic Consent Management Service (eCMS) is a service that allows healthcare consumers to manage their consent preferences electronically, better allowing them to control their own health information. The eCMS would consist of many components, which would work together to function properly.

The eCMS Module

The first component of eCMS would be an easily embeddable module, which would allow consent to be obtained electronically. The eCMS module could be embedded into any existing provider portal or consumer portal to prevent consumers from logging onto multiples portals to coordinate care.

For providers who do not have existing provider or consumer portals, MiHIN could provide a solution. The eCMS module could be housed on MiHIN's existing MIDIGATE platform for providers who do not have existing portals. The Consumer Portal could be offered by MiHIN as an additional service for entities that would like to implement this use case, but, do not have their own, existing consumer portals. However, once operational, the consumer portal would be managed by the providers.

To clarify, a provider portal is a portal that is housed at the provider office. Consumers can interact with the provider portal when they are in-person for a visit. Provider portals are usually offered by providers themselves or office representatives. Consumer portals, conversely, are webpages that consumers can log into in the comfort of their own home or on a mobile application.

The ability to fill out an electronic consent form is substantial because it solves many of the inefficiencies associated with the paper-based system. It allows consumers to avoid filling out multiple paper forms at the provider office, it allows them coordinate their consent preferences across multiple providers, and it allows for them to view all their preferences in one sole location.

Note: The eCMS Module leverages the Active Care Relationship Service® (ACRS), Health Provider Directory (HPD), and Common Key Service® (CKS).

Statewide eCMS System

The Statewide eCMS system will house the original consent form and all consent preferences when saved in the eCMS module. The statewide eCMS system is managed by Michigan Health Information Network (MiHIN).

Privacy Tags

For consent to be checked before a message with SPI is sent, MiHIN must have a way of knowing that a message contains SPI. The easiest way to accomplish this, without altering the integrity of the message itself, is by attaching an HL7 Security Label or "Privacy Tag" to the message.

Privacy tags are specially tailored codes that can be inserted into pre-existing fields on a message. For example, in an ADT message, a privacy tag could be inserted into the *Message Content* field of the message, which is a field not currently utilized.

Using HL7 Security Labels as a privacy tag allows for scalability because these labels are internationally recognized and nationally referenced in important initiatives such as the Trusted Exchange Framework and Common Agreement (TEFCA). They also allow for granularity so they can be tailored to prompt consent checks for different consent forms housed in the statewide eCMS.

When MiHIN sees a privacy tag, they would be alerted that the message does have SPI and would subsequently run the message through the statewide eCMS system to ensure the appropriate consent was on file before routing a message. More information on this situation is highlighted in the Diagram below.

Persona Story

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

Sarah Gets Treatment for Abdominal Pain

Sarah is a Michigan resident where non-specially protected health information is sent to a patient's care team as governed by HIPAA for reasons of Payment, Treatment and Healthcare Operations through the MiHIN Network. Sarah's active care team is determined based on physician-provided active patient lists.

Sarah regularly attends an opioid treatment facility. Sarah's SUD information, which is protected by 42 CFR Part 2, is distributed through the MiHIN network to only those members of Sarah's care team who are listed on her existing active Michigan MDHHS-5515 Consent to Share Behavioral Health Information for Care Coordination Purposes consent form.

Due to abdominal pain, Sarah sought treatment from a new provider: Dr. McCoy. Dr. McCoy added Sarah to her patient list, which updated ACRS. Because Dr. McCoy was not listed on Sarah's consent form, Dr. McCoy's electronic health system was not allowed to send or receive any health information protected by 42 CFR Part 2.

Later, Sarah visited her eConsent portal and gave consent for Dr. McCoy to send and receive health information that is protected by 42 CFR Part 2, including medication information that is also protected by 42 CRF Part 2. Dr. McCoy's electronic health system was now allowed to send and receive SUD information, which has been appropriately tagged.

Additionally, in the future, whenever an ADT message is created, even one from a Part 2 facility which may have specially protected information on addiction treatment, Dr. McCoy will receive that information and be able to appropriately coordinate Sarah's care.

She will also have to ability to draw connections between Sarah's SUD history and future medical conditions because she has a comprehensive view of Sarah's medical history.

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

Diagram

This diagram shows the information flow for this use case.

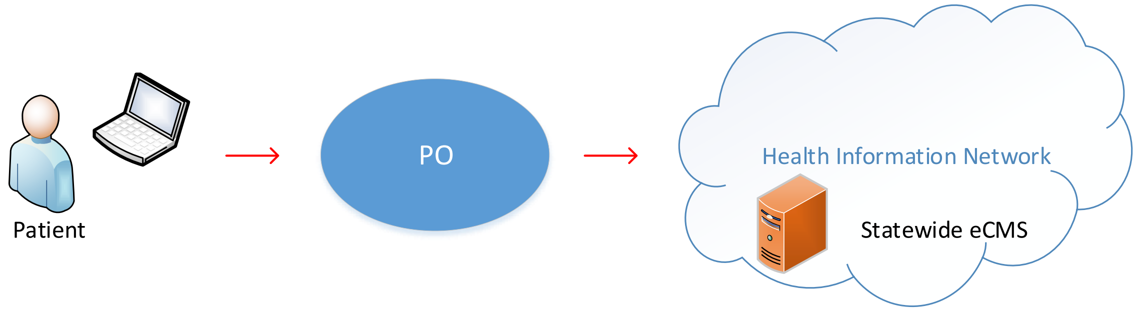


Figure 1: Collecting Consent for Consumer

1. Consumer fills out MDHHS 5515 on eCMS module at provider office.
2. When the Consumer hits save, the Consent Form and all consent preferences are stored in the Statewide eCMS.

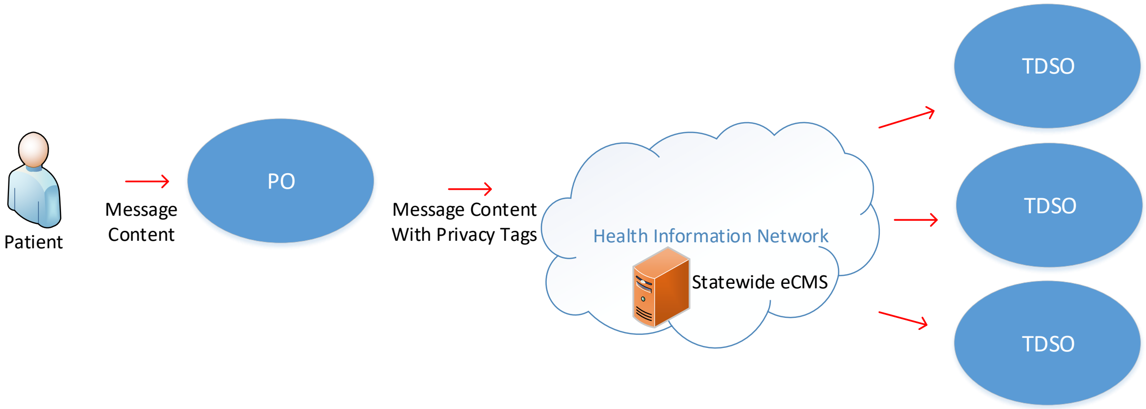


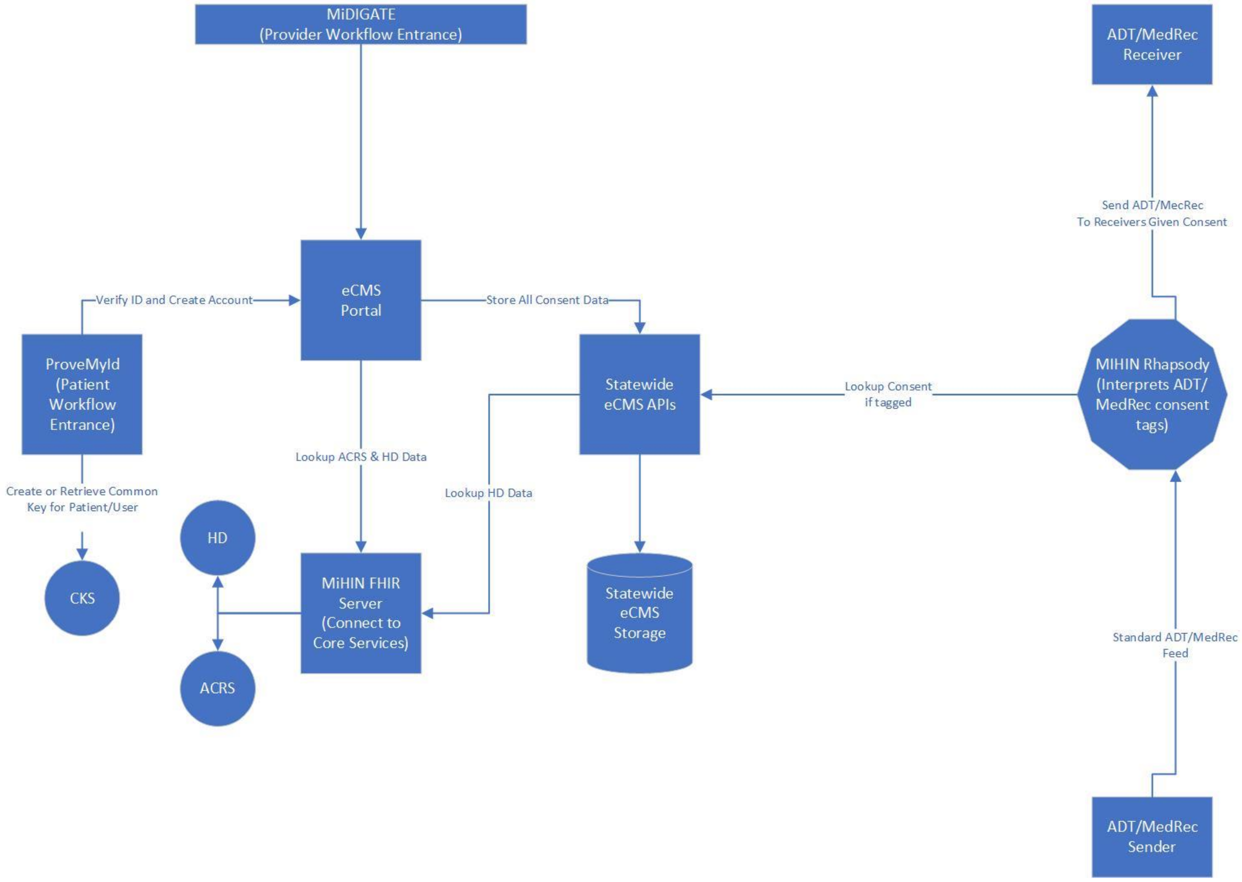
Figure 2: ADT Message with SPI Sent from 42 CFR Part 2 Facility

1. Patient is admitted to 42 CFR Part 2 facility
2. Admissions Discharge or Transfer (ADT) message with SPI is created
3. 42 CFR Part 2 Facility attached HL7 Security Label aka “privacy tag” to ADT
4. ADT is sent to MiHIN, who recognizes it has SPI due to privacy tag
5. Privacy tag prompts message to run ADT through statewide eCMS to check if consent is on file, if so the appropriate end points to route
6. Message is routed to end points with privacy tag attached to allow receiving individuals or organizations to know to limit use

Additional Scenarios:

While MiHIN is initiating this use case with ADT notifications, as the above diagram displays, additional scenarios for data flow will be available. For example, situations where a provider may need to query the Statewide eCMS system to check for consent to share with a particular provider may arise. This use case would be able to accommodate that situation, as opposed to an ongoing care coordination use case, but we will incorporate those models into the Use Case Summary as priorities are identified by MDHHS and Michigan Stakeholders.

Workflow



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

- 42 CFR Part 2

Promoting Interoperablity:

☒ Yes
☐ No
☐ Unknown

This use case supports Promoting Interoperability Stage 2 Transitions of Care measures (12) for eligible professionals.

Cost and Revenue

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

Implementation Challenges

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

Primary challenges to implement this use case potentially include:

- Inclusion of all relevant standardized privacy tags to electronic health messages required by psychiatric facilities and treatment centers.
- The creation of a statewide eCMS system
- Educational component of confusion privacy laws and regulations

Vendor Community Preparedness

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

Since MiHIN's ADT notification service and use case are already established, the technical capacity is in place to share ADT notifications based on a vendor's ability to create, send, receive and process them. Privacy tags require minimal effort and no cost to attach, but merely require training for organizations who will participate in the use case.

The vendors may not have the technical capabilities to house the eCMS module if they do not have existing provider or consumer portal to store the page. MiHIN could assist if this presents as a challenge with its existing Medical Information Direct Gateway (MIDIGATE) portal or the creation of a consumer portal.

The vendors, however, should be onboarded to the following use cases regardless of if they choose to use our portals or their own:

- Active Care Relationship Service®
- Health Provider Directory (HPD)
- Common Key Service®

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

Other: None

Concerns/Oppositions: None

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.

Metrics include:

- # of Organizations Sending Consent Form to Statewide eCMS
- # of Organizations Sending Tagged Messages to MiHIN
- # of Organizations Receiving Tagged Messages from MiHIN
- # of Specially Protected Facilities Sending Messages to MiHIN (E.g. Part 2 Facilities)

- # of Tagged Messages Received by MiHIN
- # of Tagged ADT Messages Received by MiHIN (Should be same as last for now)
- # of Tagged ADT Messages From Specially Protected Facilities (E.g. Part 2 Facilities)
- # of Tagged ADT Messages From Non-Specially Protected Facilities
- # of Tagged Messages That Cannot Be Routed to End Point

Other Information

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

Under MiHIN's existing legal trust framework, the information will not be shared with a health plan if a person directly pays for the service. However, an important caveat is that the individual must say up front that they plan to self-pay and the facility must include a self-pay code in the ADT Notification sent to MiHIN. Otherwise, the admission ADT Notification will go to the health plan.