Use Case Summary

NAME OF UC:

SINGLE SIGN ON FOR HEALTHCARE PROVIDERS AND PATIENTS

Sponsor(s): Michigan Department of Health and Human Services

Date: 02-03-16

The purpose of this Use Case Summary is to allow Sponsors, Participants, and other readers to understand the purpose of the Use Case (UC), the value proposition the UC represents, and what the Use Case does, requires, and how the UC operates at a high level. The summary is intended to help the HIE and HIT Community understand where this UC fits within the overall roadmap for statewide sharing of health information.

This UC Summary has several sections allowing readers to understand the impact of this UC in the following areas: health outcomes, regulation, cost and revenue, implementation challenges, vendor community, and support.

Executive Summary

In this section provide a brief (3-5 sentence) summary of the UC's function and purpose. Also include a brief description of the importance and highlight the expected positive impact from implementation of this UC.

Currently the task of electronically accessing health information often means logging into multiple, disconnected networks, portals or databases, meaning users must maintain and remember unique login IDs and passwords for each data source. This creates obvious productivity-draining issues resulting from forgotten login information, recovering and resetting passwords, and auto-lockout after multiple failed login attempts. There are also security risks inherent in users writing down passwords or keeping them simple or identical to ease memorization. The issues multiply with each additional login and password combination that a user must maintain, creating additional security risks and potentially taking health professionals' valuable time away from patient care.

Popular Internet companies have enabled users to employ one login ID and password to access multiple web sites. For example, a Google login ID and password now also accesses Facebook, YouTube, LinkedIn and a growing list of web sites that enable shared 'identities.' This ability to 'share' one identity across multiple networks, web sites or software applications is popularly called Single Sign-On or SSO. It gained immediate acceptance as users enjoyed the freedom from remembering so many unique login/password combinations.

Single Sign-On applied to health information can similarly solve issues inherent in having to access multiple data sources, but when using data sources that provide access to Protected Health Information (PHI) we must additionally consider federal laws and regulations regarding who may access a person's PHI. Specifically, on the public Internet there is no standard way to verify someone's identity, so in the world of health information SSO, a shared login ID and password should only be provided to someone whose identity has been thoroughly verified.

Advanced Executive Summary:

Enabling SSO in healthcare requires a very solid 'trust framework' where identities are thoroughly verified before allowing use of that identity across multiple systems. Previously in healthcare no such trust framework has existed. This SSO Use Case provides a trust framework based and identity authentication technologies that allow trusted identities to be easily shared, distributed, maintained, exchanged and used across multiple healthcare systems, organizations, and services to enable widespread, secure Single Sign-On.

This SSO Use Case increases security by simplifying user access and reducing the overall number of identities a participant must manage. The goal is to establish a single trusted identity and set of attributes that can be used by an individual or service between trusted data sharing organizations.

This Use Case allows organizations to use either trusted identities of their own provision or MiLogin trusted identities from the State of Michigan. This allows users to use Single Sign-On (SSO) across multiple healthcare services. As a result, users within the organization can maintain a single login ID and password (i.e. a trusted identity) which can access all services available through the Identity Exchange Platform based on the permissions given to them by the organization.

For example, a user could log in to their native electronic health record system (EHR), and then (without needing another login/password) directly access a Prescription Drug Monitoring Program (such as the Michigan Automated Prescription System) to determine if a patient's use of controlled substances falls within acceptable limits. In Michigan this simple capability to directly access a prescription monitoring program without extra login credentials has been projected to potentially save millions of dollars per year for pharmacists and physicians.

The Identity Exchange Hub allows service providers to obtain trusted identities at various National Institute of Standards and Technology (NIST) Levels of Assurance (LOA) ranging from 1 to 4, which allows trusted identities to be verified, authenticated and have SSO with various healthcare systems and services. The Identity Exchange Platform utilizes the State of Michigan's MiLogin as its trusted identity provider and to access service providers behind State firewalls such as myHealthPortal – the Medicaid member portal - and service providers outside State firewalls such as a Registry for Advance Directives, the Gift of Life Registry for organ donors, Health Information Service Providers (HISPs) providing Direct Secure Messaging (DSM), Electronic Health Records (EHR), Personal Health Records (PHR), the statewide Health Provider Directory (HPD) and the statewide Consumer Directory.

This Single Sign-On Use Case enables organizations outside the State of Michigan's firewalls to trust MiLogin credentials. Different Levels of Assurance can be utilized to grant authorization based on a user's role within the organizations with which they are affiliated. The Identity Exchange Hub service supports optional use of approved biometric or multifactor authentication services for NIST LOA 3 trusted identities.

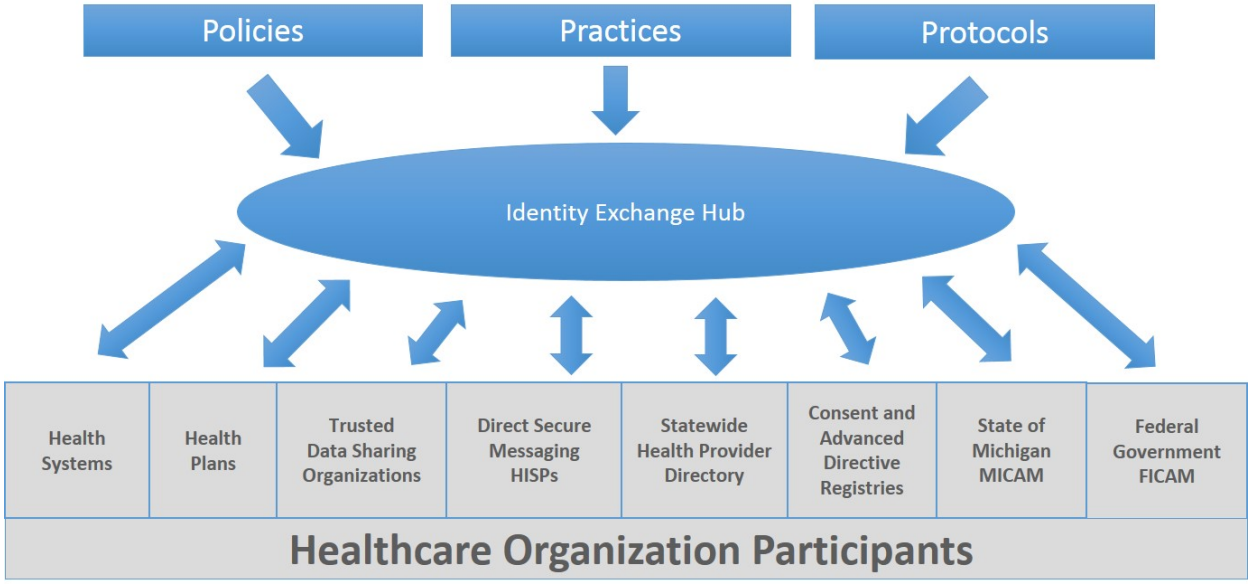
Diagram

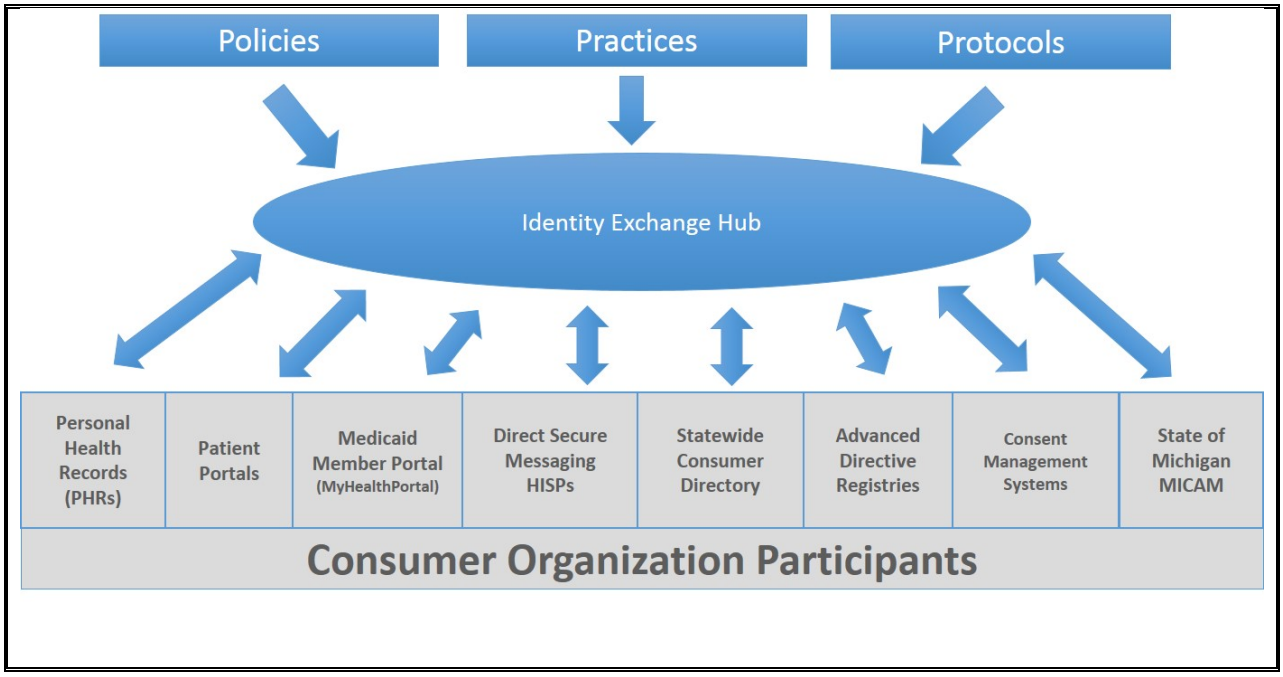
In this section, provide a diagram of the information flow for this UC. The diagram should include the major senders and receivers involved and types of information being shared.

This Single-Sign-On Use Case leverages a body of technology and legal trust called Federated Identity Management (FIdM) which consists of **Policies, Practices and Protocols** as illustrated in the diagram below and defined as follows:

- **Policies** refer to the legal and trust framework which establishes trust, including a Trusted Data Sharing Organization Agreement (TDSOA), Use Case Summaries (UCS), Use Case Agreements (UCA) and Use Case Implementation Guides (UCIG).
- **Practices** refer to the technical implementations needed to create and connect networks allowing shared (federated) identities and Single Sign-On, as well as the workflows to create, issue and use shared (federated) trusted identities only to persons whose identities have been thoroughly verified.
- **Protocols** include the identity verification requirements (NIST 800-63-2 Levels of Assurance) and security obligations of the Federated Organizations (NIST 800 framework). Protocols also include technologies and standards used for federated identity as well as the Identity Exchange Platform.

These **Policies, Practices and Protocols** are the three major components of the Single Sign-On Use Case, allowing organizations and services such as Health Systems, Health Plans, Health Information Exchanges, Direct HISPs, Identity Providers like the State's MiLogin, and the Statewide Consumer Directory, the Statewide Health Provider Directory (HPD), Advance Directives Registries, Personal Health Records, Patient Portals, and other healthcare systems to share trusted identities with each other.




Policies
Practices
Protocols
Identity Exchange Hub
Personal Health Records (PHRs)
Patient Portals
Medicaid Member Portal (MyHealthPortal)
Direct Secure Messaging HISPs
Statewide Consumer Directory
Advanced Directive Registries
Consent Management Systems
State of Michigan MICAM
Consumer Organization Participants

Regulation

In this section, describe whether this UC is being developed in response to a federal regulation, state legislation or state level administrative rule or directive. Please reference the precise regulation, legislation, or administrative act such as Public Law 111-152 (Affordable Care Act), Public Law 111-5; Section 4104 (Meaningful Use), 42 CFR 2 (substance information), MCL § 333.5431 (Newborn Screening), PA 129 (standard consent form), etc.

Additionally, provide information if this UC will allow Eligible Professionals/Providers (EP) or Eligible Hospitals (EH) to meet an attestation requirement for Meaningful Use.

Legislation/Administrative Rule/Directive

☐ Yes
☒ No
☐ Unknown

Name or number of legislation, rule, directive, or public act:

Meaningful Use:

☐ Yes
☒ No
☐ Unknown

Cost and Revenue

In this section provide an estimate of the investment of time and money needed or currently secured for this UC. Be sure to address items such as payer incentives, provider incentives, revenues generated (e.g. SSA transaction payments) or cost savings that could be realized (i.e. reduction of administrative burden).

As information is known or available, provide information on the resources and infrastructure needed to move this UC into production.

Costs to Implement:

Costs to develop the SSO Use Case and the supporting infrastructure of the Identity Exchange Hub, MICAM, and MiLogin are borne through a combination of Health Information Technology (HIT) Advanced Planning Document (APD) funding from the Centers for Medicare and Medicaid Services (CMS) and General Funds from the State of Michigan. From FY13-FY15 costs for this Use Case totaled [insert FY13-FY15 actuals]. FY16-17 costs for this Use Case are estimated at [give FY16-17 budget total for IEH] and are funded by CMS. The investment of time to develop this Use Case is XXX FTEs from FY13-FY17. Additional costs for this Use Case presently include the cost of identities from the State of Michigan via MICAM/MiLogin. At a future point the State of Michigan may determine that it is more cost-effective to leverage the credentials and identity proofing conducted at other major health care institutions in the state. By accepting the identity proofing and identities from other trusted entities, the burden on the State may be lessened, saving money and potentially creating additional efficiencies.

Costs to Adopt:

Because of the rapid global success of SSO between popular web sites and based on feedback from providers and patients involved in early pilot efforts, it does not appear that payer or provider incentives

will be necessary – instead, it is anticipated that popular user demand will lead to rapid adoption of this SSO Use Case in healthcare when it is ready.

Cost Savings:
This Use Case will drive significant but difficult-to-estimate cost savings through reduction of administrative burden and elimination of wasted time, yielding increased productivity for participants. If the average healthcare professional has to reset one password per quarter and the average professional costs $75/hour full loaded, and an average password reset takes 30 minutes, the savings is $150 times the number of healthcare professionals – in Michigan, if 100,000, the savings could be coarsely estimated as $15,000,000 per year.

Revenues
In the future, there may be participation fees for this Use Case. Additionally, there may be fees per trusted identity. Costs to participate in this SSO Use Case may vary based on each participating organization's federation maturity level. Some organizations start from scratch when creating SAML 2.0 and OAuth-aware systems and require greater integration costs than other organizations that have existing capabilities and require less integration work, costing less. The cost/revenue model for this Use Case has not yet been developed.

Implementation Challenges

In this section, as information is known or available, describe challenges that may be faced to implement this UC. Be sure to address whether the UC leverages existing infrastructure, policies and procedures, ease of technical implementation, or impacts current workflows (short term and long term).

Technical implementation challenges depend upon the technical capability level of the participants.

The technologies needed to support this Use Case are mature and are based on existing standards, such as SAML 2.0. Organizations implementing this Use Case need to be familiar with the following technologies and concepts:

a. Federated identities and single sign-on practices
b. SAML 2.0 and OAuth/OpenID
c. User-Managed Access (UMA)
d. REST/RESTful Application Programming Interfaces (APIs)
e. Service Provider Roles and Identity Provider Roles
f. Identity proofing requirements for users

Participants in this Use Case will need to plan and establish workflows to support implementation of federated identities and single sign-on functionality.

Vendor Community Preparedness

In this section, address the vendor community preparedness to readily participate in the implementation of this UC. Speak to whether this UC will utilize current or future technical capabilities of the vendor products. If this UC requires new functionality at the vendor level provide information as known to the timeliness of when product updates may be available and any potential costs to the HIE community.

Vendor preparedness is varied in the industry from organizations that are fully supportive of required technologies, to those that have SSO capabilities on a future road map, to organizations that have not made any move in this arena. In the identity management space, most leading EHR vendors either already are supporting or will be capable of supporting the implementation requirements of shared identities and SSO. By participating in the Single Sign-On Use Case, an organization can be either an identity provider, a service provider, or both. Among the service providers and their applications, systems, and services there are greater variance in identity management capabilities. For example, EHR platforms have limited support for identity management; however, third party applications can fill this role until native support is released by the EHR vendors, if they choose to develop their own.

Support Information

In this section, provide known information on the support for this UC.

Support can come from multiple levels (Governor, Federal or State Legislative, MI HIT Commission, Michigan State Departments, CMS/ONC/CDC, MiHIN Board, Qualified Organizations, Payer Community, Interest Group [ex: MSMS, MHA], or Citizen support).

Please note any concerns or oppositions with the Use Case.

Political Support:

☒Governor
☐Michigan Legislature
☐HIT Commission
☒MDHHS or other SOM Department
☐CMS/ONC
☐CDC
☒MiHIN Board
Other:

Concerns/Oppositions:

When evaluating the concerns and oppositions to the SSO Use Case, it is important to note that this Use Case does not support the sharing of health data but rather the sharing of keys to access the health data. The following concerns have been identified:

- Requires trust beyond reproach;
- Requires strict policies and procedures and strong legal agreements;
- Requires extreme oversight of account creation

Sponsor(s) of Use Case

Who are the major sponsors of the use case?

MDHHS is sponsoring the project using funds secured from CMS and the State of Michigan.
MiHIN is coordinating the project.

Metrics of Use Case

In this section, define metrics for the Use Case to be successful.

The following are some metrics related to achieving basic federation of identities allowing users to access systems or information at other organizations:

- Number of TDSOs participating in the SSO Use Case
- Percent change in TDSOs participating (growth/loss)
- Successful exchange of user credentials and authentication across multiple TDSOs
- Active participation by multiple health plans and other healthcare service providers such as the Peace of Mind Registry (Advance Directives), Gift of Life Registry (Organ donors), the Statewide Consumer Directory, and other service providers as they become available
- Successful integration with the State of Michigan's MILOGIN identity provider

Metric pertaining to automatic account creation:

- Successful automatic account creation by one or more TDSOs (i.e., user can log in to all SSO enabled accounts they have authorization to access)

Other Information

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

In collaboration with the State of Michigan, the Michigan Health Information Network Shared Services (MiHIN) has created an Identity Exchange Hub service (IEH) that shares trusted identities across organizations. This IEH service permits Medicaid to expand its Michigan Identity Credentialing and Access Management (MICAM) MiLogin Single Sign-On (SSO) services portal, allowing access to numerous State data sources and enabling MiHIN's IEH service to share MiLogin identities with other Medicaid-related organizations for SSO.