Use Case Summary

Use Case Name:	Single Sign-On
Sponsor:	Michigan Department of Health and Human Services
Date:	March 20, 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.

Currently the task of electronically accessing health information often means logging into multiple, disconnected networks, portals, or databases. This means that users (physicians, nurses, pharmacists, etc.) must maintain and remember unique login IDs and passwords for each data source they use.

These multiple safeguards create obvious productivity-draining issues, including forgotten login information, passwords that need to be recovered and reset, or auto-lockout after multiple failed login attempts. Also, there are 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 a health professional's valuable time away from caring for patients.

Purpose of Use Case: The Single Sign-On use case increases security by simplifying a user's access and reducing the overall number of identities a participant must manage. The primary 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.

Overview

This overview goes into more details about the use case.

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 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.” It gained immediate acceptance as patrons 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. When using data sources that provide access to protected health information (PHI), there needs to be additional consideration regarding 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. Therefore, a shared login ID and password should only be provided to someone whose identity has been thoroughly verified.

Enabling single sign-on 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 existed. This use case provides a trust framework based on identity authentication technologies that allow trusted identities to be easily shared, distributed, maintained, exchanged and used across multiple healthcare systems, organizations, and services.

This use case allows organizations to use either trusted identities of their own provision or MILogin trusted identities from the State of Michigan. As a result, users 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 permissions given to them by other participating organizations.

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 Single Sign-On use case enables organizations outside state firewalls to trust state credentials. Different Levels of Assurance can be utilized to grant authorization based on a user's role and privileges to access different kinds of information from participating organizations.

Diagram

This diagram shows the information flow for this use case.

The Single-Sign-On use case leverages a body of technology and legal trust called Federated Identity Management (FIdM). FIdM consists of policies, practices and protocols as illustrated in the diagram below and defined as follows:

- **Policies:** The legal and trust framework which establishes trust, including a trusted data-sharing organization agreement, use case summary, use case exhibit, and use case implementation guide.
- **Practices:** 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:** 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.

Policies, practices and protocols are the three major components of the Single Sign-On use case. They allow organizations and services (such as health systems, health plans, health information exchanges, Direct HISPs, Identity Providers, the Statewide Consumer Directory, the statewide HPD, advance directives registries, personal health records, patient portals, and other healthcare organizations to share trusted identities with each other.

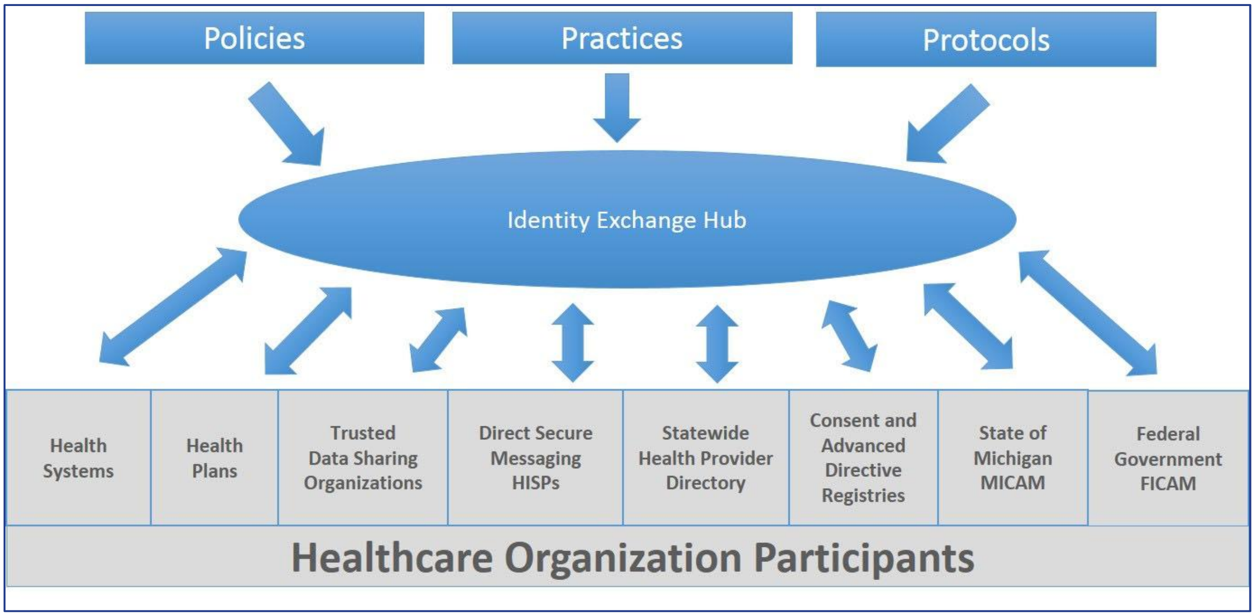
Policies
Practices
Protocols
Identity Exchange Hub
Health Systems
Health Plans
Trusted Data Sharing Organizations
Direct Secure Messaging HISPs
Statewide Health Provider Directory
Consent and Advanced Directive Registries
State of Michigan MICAM
Federal Government FICAM
Healthcare Organization Participants

Figure 1. Healthcare Organization Participants Single Sign-On

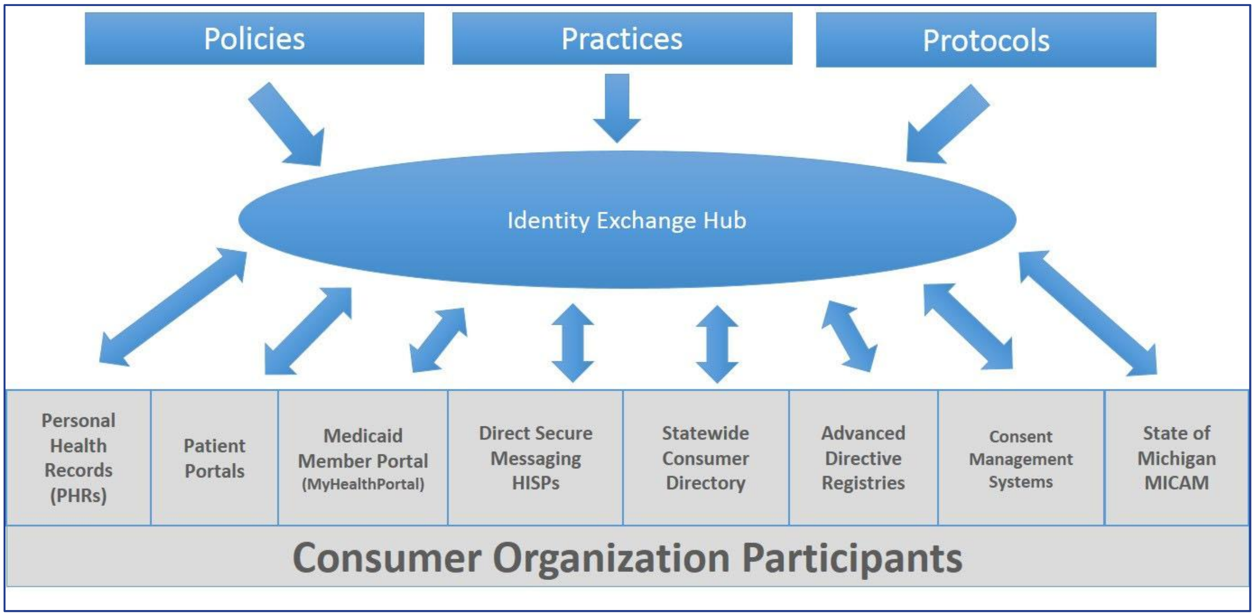
Policies
Practices
Protocols
Identity Exchange Hub
Personal Health Records (PHRs)
Patient Portals
Medicaid Member Portal (MyHealthPortal)
Direct Secure Messaging HISPs
Statewide Consumer Directory
Advanced Directive Registries
Consent Management Systems
State of Michigan MICAM
Consumer Organization Participants

Figure 2. Consumer Organization Participants Single Sign-On

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

Meaningful Use:

☐ Yes
☒ No
☐ Unknown

Cost and Revenue

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

Costs to Implement

The costs to develop the Single Sign-On use case and the supporting infrastructure of the Identity Exchange Hub, Michigan Identity Credentialing and Access Management (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 fiscal year 2013 to 2015 costs for this use case totaled [insert FY13-FY15 actuals]
- The estimated costs for this use case for fiscal year 2016 through 2017 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 fiscal years 2013 through 2017

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 single sign-on between popular Websites 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 a rapid adoption of this use case in healthcare when it is ready.

Cost Savings

This use case will drive significant but difficult-to-estimate cost savings through a 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, and an average password reset takes 30 minutes, the savings is $150 times the number of healthcare professionals. Therefore, for 100,000 professionals, 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 the Single Sign-On 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.

Implementation Challenges

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

Technical implementation challenges depend upon the technical capability level of the various 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:

- Federated identities and single sign-on practices
- SAML 2.0 and OAuth/OpenID
- User-managed access
- REST/RESTful application programming interfaces

- Service provider roles and identity provider roles
- Identity proofing requirements for users

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

Vendor Community Preparedness

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

Vendor preparedness is varied in the healthcare industry, from organizations that are fully supportive of required technologies to those that have single sign-on 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 single sign-on. 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.

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

When evaluating the concerns and oppositions to the Single Sign-On 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

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

- Michigan Department of Health and Human Services (using funds secured from CMS and the State of Michigan)

Metrics of Use Case

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

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

- Number of trusted data sharing organizations (TDSOs)s participating in the Single Sign-On 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's 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 single sign-on-enabled accounts that they have authorization to access)

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.

In collaboration with the State of Michigan, the Michigan Health Information Network Shared Services has created an IEH service that shares trusted identities across organizations. This IEH service permits Medicaid to expand its MICAM MILogin single sign-on 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 single sign-on.