USE CASE SPECIFICATION

Version 2.0

Single Sign-On

Version History

Version #	Date	Author(s)	Reason for Change
1.0	12/19/2019	Use Case Team - HealthTech	New
2.0	02/07/2020	Use Case Team - HealthTech	Added two new fields as requested by client, changed colors background to approved color scheme

Single Sign-On/Direct Query for Healthcare Provider, Healthcare Organizations, and Payors

HIE Use Case Summary

Current access to electronic healthcare information often consists of logging into multiple networks, portals, and/or databases. The user must manage several unique login identifications (ID) and passwords for each data source that is needed during the course of normal work. This creates inefficiencies in productivity and password fatigue. Managing multiple login credentials may lead the user to forget passwords thereby activating an auto-lockout feature of data sources after multiple failed attempts. This can also create security risks by the users writing down passwords, keeping passwords simple, or using the same easy to memorize password for multiple environments. Not only is the productivity of the user compromised potentially diminishing valuable patient care time, but the information technology (IT) team can be inundated with unnecessary password reset requests if the above occurs.

Single sign-on (SSO) can solve issues encountered with accessing multiple data sources providing a mechanism by which a user can be authenticated in one place and use those credentials to seamlessly and securely access other applications such as Big Sky Care Connect (BSCC), Montana's health information exchange (HIE). SSO is a user authentication service that allows a user to apply the same set of credentials to access multiple applications. The user has access to all applications to which they have been granted rights. In healthcare, SSO requires a solid "trust framework" where identities are thoroughly verified before allowing the user to have access across multiple systems. SSO is one of the ways to support a zero-trust security strategy enabling secure and unified access across all application types. When using data sources containing protected health information (PHI), federal laws and regulations must also be considered.

Direct Query provides a service by which BSCC HIE can be integrated into disparate applications, such as electronic health record (EHR) systems keeping the user in their "home" environment without the need for switching from one system to another. Querying BSCC HIE for vital health information at the point of care can be incorporated into the routine workflow of providers and payors.

Both SSO and Direct Query are technologies commonly used by HIEs to enhance the ease of use and speed of accessing HIEs by provider organizations. Direct Query involves embedding the HIE portal into the provider's EHR system permitting the EHR to query the HIE on its own, so the information contained in the HIE is always present in the providers EHR allowing them to never have to leave their primary application.

SSO allows the provider to press a single button (sometimes this can be automated) which sends both the provider's sign-on credentials and patient context to the HIE and automates the sign-on and query functionality of the HIE. There are advantages and disadvantages to each technology and EHR capability considerations; and therefore, provider organizations will want to explore each before deciding which to implement. In both cases HIEs across the country have shown that often

the use of the HIE is almost totally dependent on providers having one of these two technologies. They essentially have duplicate financial and business considerations.

User Story

Clinic: Dr. Smith, a family practice clinic provider, is frustrated with the multiple applications he must log into to perform his daily tasks and struggles to remember the different user IDs and passwords for each environment that he accesses. He feels that having only one user ID and password would make his work process easier and would give him more time to provide patient care. SSO/Direct query available through BSCC HIE offers Dr. Smith an easy and secure way to access external data sources while remaining in his clinic's EHR. SSO gives Dr. Smith the ability to access relevant patient data from prior healthcare visits, medication lists, PDMP, lab results, images, etc. with one click to BSCC HIE for a 360° view at the point of care. For example, Dr. Smith would log into his EHR and click on BSCC HIE link allowing access to an individual patient's health record via the HIE portal with the correct clinical data immediately displayed.

Direct query allows Dr. Smith to easily integrate HIE queries into his daily workflow. Care coordination is improved with quick and easy access to existing treatment plans shared among the collective care providers. By accessing the trusted secure BSCC HIE, Dr. Smith has a holistic view of the patient he is treating and has regained valuable patient care time with one click access to data sources which can help improve patient outcomes.

Hospital: In a hospital setting, medical professionals log on to and log off from workstations each time they use them to avoid the disclosure of information to unauthorized individuals, ensuring the integrity and accuracy of patient information. Different users in the hospital system are granted role-based privileges and security access to the patient health record. Providers must remember many of passwords to access various applications needed to accomplish their daily work. This can lead to the sharing of passwords or writing down passwords. Sometimes a user may be required to manually log out of a workstation in order to be granted access to another.

When properly implemented, SSO maintains the security of all applications for which it is being used, tracks and logs access to PHI, and delivers fast access to critical information. SSO offers a secure means of proper user authentication, application access, and enables proper privacy controls. A provider can access patient records, prescription information, and other medical data using one-time authentication.

Payor: A payor needs to access additional data from a medical encounter in support of a claim that was submitted for a patient. SSO and direct query enables this payor to quickly and securely access clinical and administrative data located in BSCC HIE via a single access point using the login credentials required for their native health information technology (HIT) system.

This user will be able to securely access richer clinical data through the seamless integration of BSCC HIE queries into their workflow saving time and resources which may result in reduced or eliminated time spent obtaining information directly from a provider, saving them time as well. Being able to efficiently incorporate clinical and claims data will assist this payor in identifying gaps in care, profiling patients, and producing population health analytics.

Key Actors

Those who will be using the application or system; can be human or technology. Key actors include but are not limited to:

- Medical and non-medical staff serving at hospitals, clinics, long-term health facilities, public health departments, and patient centered medical homes, as well as case managers, care managers, pharmacies, Emergency Medical Services (EMS), home care, hospice, Department of Correction (DOC), payors/health plans, state/federal agencies, public health registries.

- EHR and HIE systems must communicate using an Identity proofing methodology to accomplish the match between systems.

Stakeholder

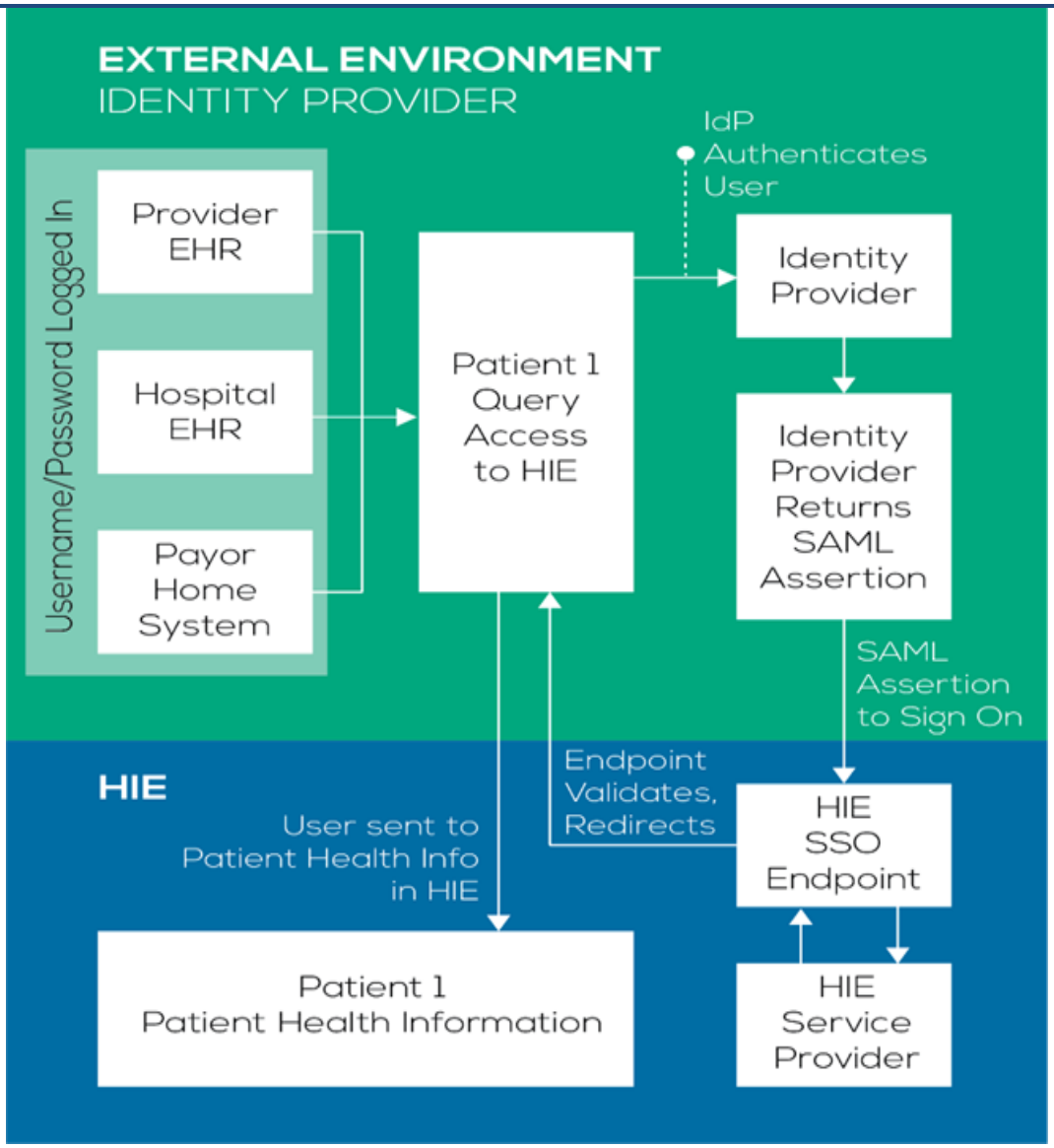
Those who have an interest in the success of the use case. Stakeholders include but are not limited to:

- Key actors listed above.

- BSCC, Montana Medical Association (MMA), Department of Public Health and Human Services (DPHHS), Montana Board of Nursing, Montana Hospital Association (MHA), as well as compliance teams representing providers, and legal teams representing providers.

Function/Purpose

SSO is a session and user authentication service that permits a user to use one set of login credentials such as name and password to access multiple applications thereby mitigating the burden of managing various usernames and passwords. SSO grants a user access to all applications to which they have been credentialed and eliminates future password prompts from every disparate application needing to be accessed. SSO establishes a single trusted identity and set of attributes that can be used by an individual or service between trusted data sharing organizations.



Value Proposition

Implementing SSO will result in significant savings to a healthcare organization through the reduction of time wasted in password resets and navigating between disparate systems with multiple log-ins. This could reduce the number of clicks the end-user makes as this brings information in from a variety of sources into a central record serving to increase use for the HIE and other registries. This will result in increased productivity as well as a better overall user experience.

Calculating an exact savings is difficult, however by looking at the time to reset one password per quarter for one user, a conservative estimate can be made. If the average healthcare professional costs in Montana range between $13/hour per office/medical support staff and $89/hour per provider, and a typical password reset takes 30 minutes depending upon help desk availability, then the savings range is between $6.50 to $44.50 times the number of healthcare support staff

and providers. Following that calculation, if there are 100 office/medical support staff within an organization that are required to reset their password per quarter, the savings to the organization is $650 per quarter or $2,600 per year. The savings realized for 100 healthcare providers is roughly $4450 per quarter or $17,800 per year.

Financial and Business Considerations

Financial consideration

Both SSO and Direct Query will require an investment per provider for those providers included in the Phase One and Phase Two milestones as defined in our InterSystems contract, the HIE side is included in our current pricing from InterSystems. On the provider side for these organizations, many of these organizations may have the ability to configure their own internal systems without assistance from the vendor; however, for budget purposes BSCC should plan for an investment per organization with the EHR vendor ultimately performing the work for the provider organization. This should, of course, be negotiated in bulk with the individual EHR vendors at the time the initial interfaces are negotiated.

- **Phase One:**

  The costs for InterSystems costs for this phase (3 hospitals and 2 clinic organizations) is included in the SOW. The anticipated provider costs for this phase range from $11,500 to $16,100 per connection for SSO or direct query respectively. Total cost for this phase is anticipated to be range between $57,500 and $80,500.

- **Phase Two:**

  The costs for InterSystems costs for this phase (9 hospitals and 2 clinic organizations) is included in the SOW. The anticipated provider costs range from $11,500 to $16,100 per connection for SSO or direct query respectively. Total cost for this phase is anticipated to be between $103,500 and $144,900.

Beyond the Phase One and Phase Two milestones, the entire estimated costs will need to be budgeted for each additional large provider organization using this technology. This technology will usually be implemented only in very large provider organizations, but an attempt should be made with smaller EHR vendors to also implement as many as possible. All hospital and mainstream ambulatory clinics should be targeted for implementation.

- **Future Connections:**

  The costs for future connections will include an InterSystems cost ranging from $10,000 per SSO interface to $14,000 per direct query. In addition, yearly maintenance fees of $1,500 to $2,100 respectively, per connection. When including provider costs, it is

anticipated to range from $23,000 to $32,200 per connection for SSO or direct query respectively.

- **HealthTech Solutions Anticipated Costs:**

  Outreach and Onboarding:

  Costs associated with SSO would be included in the onboarding and outreach costs as with any other provider connections. In addition, SSO would be part of a number of connections that would be made for a provider resulting in minimal additional work by the onboarding and outreach team. Since these costs are included in the contract for HealthTech onboarding and outreach, no additional cost breakout is included.

Funding sources: Funding for SSO/Direct Query has been budgeted in the 90/10 monies available through CMS.

End-user fees: As with the initial interface, there may be additional ongoing charges from the EHR vendors for maintenance of these technologies on an annual basis which should be identified at the time of negotiations with the EHR vendor.

Tie back to value proposition: Password resets, per the stated value proposition, are virtually eliminated with the implementation of this technology. It should be noted; however, that the implementation of these technologies can be the difference between providers using and not using the HIE or using it very little. Providers are reluctant to leave their EHR systems to search and/or access other systems for information. Since these technologies automate the access of the HIE, studies have shown a remarkable uptake in HIE access by providers in every organization connected to the HIE.

Business Considerations

- **Interface and access Technology negotiations**: BSCC (HealthTech) should be prepared to quickly and earnestly negotiate with the EHR vendors to procure the best pricing along with a guarantee that all implementations of the vendor's EHR solution in the state are included in a single price, over a set period of time that allows completion of all work by September 30, 2021.

- **Staffing requirements:** BSCC (HealthTech) has initial staff assigned to help negotiate and coordinate the onboarding activities needed for this technology with the various vendors. If need be, HealthTech will either add or repurpose staff as needed to ensure connectivity of as many provider organizations as possible before September 30, 2021. Work can continue after this date; however, more guidance will be needed from CMS to determine the funding availability for the HIE and its providers.
- **Workflow redesign:** When the outreach team returns to provider organizations for HIE training, some assistance will be given to the provider organizations to assist them with workflow integration and practice operations. By nature, these technologies make this work much easier for both BSCC and the provider.

Upstream/Downstream Dependencies

SSO/Direct Query use case requires the development of a trusted framework that identifies the technology, stakeholders, entities, and health care organizations impacted by the implementation of an SSO or Direct Query solution. It is necessary to identify the dependencies that will potentially impact SSO/Direct Query, both upstream and downstream.

Stakeholder

- **Upstream** – Stakeholders will be identified. Once stakeholders are identified, information will be gathered including the healthcare organizations they seek to access.
- **Downstream** – Infrastructure will need to be established that will support end-users, participants, entities, and others, to include establishing access and providing help in the future.

End-User Level

- **Upstream** – Create access including credentials and roles for end-users.
- **Downstream** – Establish a user's role and grant authorization to those healthcare organizations and systems for which they are affiliated.

Healthcare Organizations/Payors

- **Upstream** – Identify either entity or participant's role – identity provider or service provider, or both.
- **Downstream** – Ensure the entities are accessible to all end-users who are approved to access the organization or system.

Technical

- **Upstream** – Identify standards, supporting infrastructure, and technology options to support SSO or Direct Query across multiple organizations, end-users, platforms, and healthcare organization participants. Create networks within SSO, develop connections to those networks, and create organization access.
- **Downstream** – Ensure entities are informed of requirements to participate in SSO, applications, platforms, networks, and organizations.

Regulation

- **Upstream** – The review and analysis of federal and state laws that may impact SSO has been accomplished and described in the Legal/Policy Consideration section.
- **Downstream** – Establish procedures to ensure end-users are only accessing systems and applications they are approved to access. Establish security measures to lock down an end-user when possible violations are detected.

Technology System Components and Services Utilization

Security Assertion Markup Language (SAML) is a standard for providing SSO to users. The arrangement, called a "federation", involves logging users into participating applications based on their credentials in their home context. SAML allows for the federation server or servers to

exchange tokens from local environments for ones that function consistently with standards-based applications. The local security environment serves as an identity provider to the federation server. At logon, the user receives a standard SAML token that will identify the user to all participating applications which serve as service providers.

SAML transactions use encrypted Extensible Markup Language (XML) for secure, standardized communications between the identity provider and service providers. SAML is the link between the authentication of a user's identity and the authorization to use a service.

Most organizations already know the identity of users because they are logged in to their Active Directory domain. It makes sense to use this information to log users in to other applications, such as web-based applications.

A user is logged into a system that acts as an identity provider. The user wants to log in to a remote application, such as a support or accounting application (the service provider). The following happens:

- The user accesses the remote application using a link on an intranet or a bookmark.
- The application identifies the user's origin and redirects the user back to the identity provider, asking for authentication. This is the authentication request.
- The user either has an existing active browser session with the identity provider or establishes one by logging into the identity provider.
- The identity provider builds the authentication response in the form of an XML-document containing the user's username or email address, signs the response using an X.509 certificate, and posts this information to the service provider.
- The service provider, which already knows the identity provider and has a certificate fingerprint, retrieves the authentication response and validates it using the certificate fingerprint.
- The identity of the user is established, and the user is provided with application access.

Configuration/Interfaces Required

- Service providers (participating applications such as the HIE portal, PDMP etc.), must be configured to support SSO via SAML token.
- Identity providers must be onboarded to the Federation server(s), which could be operated by the HIE, State or other vendors.

External Dependencies

- EHR vendor's technology capabilities to implement SSO/Direct Query.
- EHR vendor's capabilities to adhere to the same technology standards as required by BSCC HIE vendor for SSO/Direct Query implementation.
- Hospital, clinic, or payor's IT resources availability including EHR vendor.

Legal/Policy Considerations

Executive order No. 14-2019

- The state of Montana's **Executive order No.14-2019** established BSCC as Montana's state designated HIE entity. This order authorizes innovations that drive an evolution of primary care such as enabling SSO/Direct Query through BSCC to support integrated care delivery.

21st Century Cures Act (Section 4001, 4003& 4004)

- Section 4001(a) (Reduction in burden) – establishes a goal with respect to the reduction of regulatory and administrative burdens relating to the use of EHRs. Supports SSO because it focuses on reducing administrative burden to the use of Health IT and EHRs. SSO is meant to reduce username and password management in the use of BSCC, an individual provider's EHR, and PDMP.

- Section 4003 (Interoperability) with respect to health information technology means such technology that will (1) enable the secure exchange of electronic health information with, and use of electronic health information from, other health IT without special effort on the part of the user; (2) allow for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable state or federal law; and (3) does not constitute information blocking. SSO is meant to allow credentialed access to trusted and secure applications containing health information.

- Section 4004 (Information blocking) may include practices that restrict authorized access, exchange, or use including transitions between certified health information technologies; implement health IT in ways that would restrict the access, exchange or use of electronic health information to include transitioning between health IT systems. SSO provides a mechanism by which a user can be authenticated in one place and use those credentials to securely access other applications to which they are authorized to access.

HITECH Act

- The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 provides Health and Human Services (HHS) with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic HIE. The HITECH act supports the establishment of BSCC and its various functionalities such as SSO to improve efficiency in the use of the disparate HIT systems.

HIPAA (Pub.L.104–191, 110 Stat. 1936, enacted August 21, 1996, Title II)

- The HIPAA Privacy Rule describes what information is protected and how protected information can be used and disclosed. The HIPAA Security Rule describes who is covered by the HIPAA privacy protections and what safeguards must be in place to ensure appropriate protection of electronic protected health information. SSO will ensure that login information of providers is secured, prevent shared login details, and ensure that patient information can only be accessed by individuals who are authorized to have access to PHI.

Patient Protection and Affordable Care Act (42 U.S.C § 18001 (2010)

- The Affordable Care Act (ACA) of 2010 establishes comprehensive health care insurance reforms that aim to increase access to health care, improve quality and lower

health care costs, and provide new consumer protections. The ACA supports technological innovations that promote integration of health IT systems that promote patient care and improved health outcomes. SSO will allow the seamless access to a patient's clinical data through BSCC HIE to assist the health care plan's case managers to identify gaps in care, prior authorizations, referral approval and population health analytics.

Assumptions

- During the development of the SSO use case, all projections are for planning and estimate purposes only.
- During the development of the SSO use case, all projections/estimates do not consider undefined business scoping elements that may be found throughout the project life cycle due to stakeholder requests, business and vendor requirements, vendor negotiations, dependencies, durations, and any lag times which may result from the actual planning and implementation process.
- Most, if not all providers, will use SSO and/or Direct Query capabilities.
- Enterprises belong to one or more Cross-Enterprise Document Sharing (XDS) Affinity Domains. An XDS Affinity Domain is a group of healthcare enterprises that have agreed to work together using a common set of policies and share a common infrastructure.
- Document concept in XDS is not limited to textual information.
- XDS is document content neutral, any type of clinical information without regard to content and representation is supported.
- Vendor costs are based on knowledge as of February 7, 2020 and may increase or decrease depending upon final contract negotiated with vendors.
- Vendor costs have not anticipated increased costs that may occur in the future.
- Costs do not include the outreach costs which are included in the outreach/onboarding contract.
- Use case work and management is continual throughout the project. These activities will transfer to BSCC permanent staff as they are hired and trained. These are part of the operational HIE process.
- HealthTech Solutions is on a time and materials contract which states that costs to not to exceed that which is identified in the contract.
- Constraints, inclusions, and exclusions are based on current knowledge as of February 7, 2020 and may change.
- Policy, legal, and regulatory as well as technical standards for interoperability changes may take place on both the state and federal level.
- Ongoing monthly interface fees are being negotiated as part of the initial HIE statement of work (SOW).
- Vendor costs identified do include monthly fees and are being negotiated in the initial HIE SOW.

Key Performance Indicator/Metrics of Use Case

The following are some examples of metrics that can be measured and related to achieving basic federation of identities allowing users to access systems or information at other organizations:

- Number of organizations that have signed agreements and are trusted entities participating in the SSO Use Case.
- Percent change in the trusted entities participating (growth/loss).
- Successful exchange of user credentials and authentication across multiple trusted entities.
- Percentage of users that access HIE with SSO/Direct Query access versus the percent of users that access HIE without SSO/Direct query access.
- Active participation by multiple health plans and other healthcare service providers
- Metric pertaining to automatic account creation:
    - Successful automatic account creation by one or more trusted entities (i.e., user can log in to all SSO enabled accounts they have authorization to access).

Alternative Paths

Traditional SSOs are layered on top of on-premises identity management platforms such as Active Directory. The on-premises identity management infrastructure is useful, but the trend is in favor of cloud alternatives. This requires a growing number of add-ons as more IT resources shift to the cloud.

A next generation SSO provider that connects to more than just web applications may be an alternative path to consider. This type of SSO provider authenticates user access to virtually any IT resource such as systems, applications, networks, and file servers all with minimal infrastructure on-premises. Sales Force and JumpCloud Directory as a Service are examples of the next generation true SSO provider. These securely connect authenticated users to systems, applications, files, and networks. Web application SSO is a core feature of this hosted directory service and has the ability to authenticate access to almost any IT resource.

Another alternative path is do nothing. Not implementing SSO would continue to require all providers and end-users to access the HIE portal through a web application, each with its own unique user ID and password. Doing nothing could lead to:

- Limited access and utilization of the data in BSCC HIE.
- Continued frustration by end-users logging out of home system to log into and access other systems throughout their process of daily work.
- Continued increase of costs relating to IT support for password resets.
- Continued security risk derived from sharing passwords and/or writing down ID and passwords.

This project is funded in whole or in part under a Contract with the Montana Department of Public Health and Human Services. The statements herein do not necessarily reflect the opinion of the Department.