Bridging Electronic Health Record Access to the Cloud

Brian Coats
Towson University
bscoats@umaryland.edu

Subrata Acharya
Towson University
sacharya@towson.edu

Abstract

Healthcare providers are faced with mounting pressure to facilitate pervasive access to their electronic health record systems for their patients; the Meaningful Use incentive programs perhaps the most significant driver. Meanwhile the Cloud has expended immense time and resources on the establishment of proficient, easy-to-use digital identities for individuals, while also allowing those identities to be portable across a myriad of disparate systems. This research proposes the success and proliferation of the Clouds' digital identities to be part of the solution to the healthcare industry's access issue. By analyzing industry standards and other ongoing identity related work in other industries, a trust model was produced to enable the exchange of identity information. As such, this research proposes a comprehensive framework for healthcare providers to follow to integrate their EHRs with the Cloud for provide identity validation, while ensuring compliance guidelines for security and privacy. To demonstrate the viability of this research, a number of pilots and concept projects have been implemented at a large regional hospital that have already produced immediate and tangible improvements.

1. Introduction

The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2010 has been touted as the “transformational opportunity to break through the barriers to progress"[1] for the healthcare industry. Out of HITECH, the Department of Health and Human Services created incentive programs which provide payments to healthcare providers that demonstrate 'Meaningful Use' of certified electronic health record (EHR) technology to accomplish specific objectives in care delivery. Providing patients access to their health records is among the many Meaningful Use objectives. The latest Stage 2 objectives specifically require that hospitals grant patients access to view, download, and transmit their health information online within 36 hours of discharge; Eligible Professionals (EP) must provide this within 4 business days. However, healthcare providers are given little to no guidance for how this access requirement should actually be accomplished, only that it must be completed.

When attempting to unravel this daunting task of providing access to EHRs, a key component is how users will validate their identity. In a traditional scenario, this issue would be addressed by each EHR system creating its own, unique data stores and corresponding security controls for accessing their respective data. Similarly, authentication of these systems including EHRs, involved using a credential stored locally within the system being accessed, as depicted in Figure 1. Therefore healthcare providers employing this traditional model must issue their users some credential, such as a username and password, that is stored within the healthcare provider's EHR system. Consequently, when the user attempts to access said EHR system they must enter the corresponding credential for that system. Further, if an individual interacts with multiple healthcare providers, they are required to have provider-specific credentials for each EHR system. The effort and complexity associated with the establishment, issuance, and maintenance of digital identities and corresponding credentials creates both a usability barrier for patients as well as an efficiency barrier for healthcare providers. At the most basic level, the usability of an EHR system by patients starts with being able to log in. Requiring patients to contact each of their healthcare providers to establish unique credentials is appreciably more cumbersome and confusing compared to using a familiar credential for all systems. Likewise, a healthcare provider creating and maintaining the technical and support systems to issue credentials becomes unnecessary. Therefore the traditional approach becomes inefficient compared to using a preexisting infrastructure that has very little associated cost and effort to utilize. For providers that are starting or have already begun to address identity access and management in their environments, it is critical that the technical and organizational solutions being adopted are scalable and able to easily interoperate throughout the entire healthcare industry and beyond.

This electronic identity situation has many healthcare providers finding themselves poorly positioned to enable the types of distributed access that EHR systems are supposed to facilitate. The regulations and programs that are driving EHR adoption, including HIPAA and Meaningful Use, provide virtually no direction on how to tackle these

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.367

enormous usability and efficiency challenges. This research proposes a prescriptive solution to this problem by creating a flexible, proven framework for healthcare providers to achieve pervasive electronic access of their EHR systems by their patients from the Cloud. Specifically, the key contributions of this research to the healthcare information technology industry are:

- The creation of an easily adaptable identity assurance framework for healthcare providers to follow to integrate Cloud access to their EHR systems,
- A comprehensive Identity Provider profile to evaluate Cloud vendors' identity assurance capacity,
- A simple registration utility that can be used to link EHR accounts to Cloud accounts, and
- Enhanced security and usability for a partnering regional healthcare provider.

The remainder of the paper is as follows: Section 2 presents the concepts of portable access between heterogeneous systems; Section 3 describes how trust in an external identity is achieved; Section 4 lays out the guidelines external Identity Providers must follow in order to integrate with an EHR; Section 5 discusses how the Cloud is actually integrated with an EHR; Section 6 describes how this research is already being used in real-world applications; Section 7 discusses future directions of this and other similar research; and finally Section 8 summarizes the goals of this research and its importance to the advancement of information security in healthcare.

2. Creating a Portable Access Model

There are 3 fundamental issues that need to be addressed when establishing digital identities and configuring applications to leverage those identities:

- Who does the digital identity belong to?
- How does the individual prove their identity?
- What should the user be allowed to access or do in the relevant application?

These issues are more technically referred to as identity management (IdM), authentication, and authorization. IdM is the underlying processes and systems that establishes and keeps track of who an individual is and allows other systems to relate a digital identity to an actual person. It is critical to recognize that an individual possess any number of identifiers that make up their digital identity. The IdM system correlates and tracks those identifiers across all systems. Authentication and authorization are many times incorrectly used interchangeably or combined as a single issue called ‘access’ but they are 2 very distinct steps. Authentication is how an individual proves who they are. On the other hand, authorization addresses what privileges that individual should have, such as being able to view or modify data in an application. The distinction is critical when considering a portable access model.

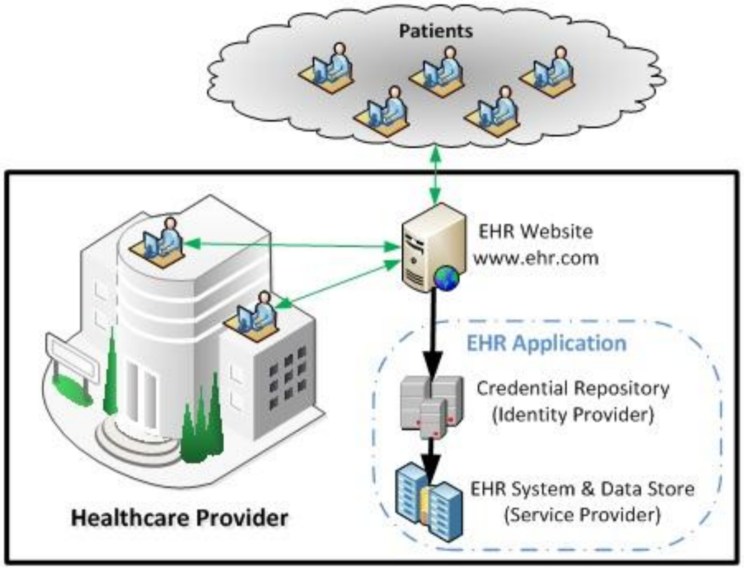


Figure 1. Traditional EHR Access Model

Authorization decisions must inherently be made at the application level but authentication can almost always be externalized from the resource being accessed. Examining the authentication event closer, there are 3 sub-components: the user, known as the Subject, with possession of a credential; an authentication system that can validate said credentials, known as the Identity Provider (IdP); and the application that recognizes the identity, known as the Service Provider (SP). As Figure 1 shows, traditional systems have the credential repository or IdP built into the application itself. This model creates a dependency that in order to access that application the corresponding internal credential must be used. A key objective of this research is to break this dependency. More simply, this research proposes that EHR applications need to be able to use other identity stores to validate credentials, beyond those stored in the local EHR database. Fortunately, this basic functionality is supported by all the major commercial offerings in some fashion and the real effort lies in getting EHR systems to work effectively and appropriately with external systems. Therefore as healthcare providers address electronic access to their EHR systems, the challenge of authentication can be essentially outsourced to other vendors and organizations that have already made significant investments in this arena.

Leveraging the ability to separate the authentication process from the EHR application, this research proposes a framework by which authentication of a single EHR system can not only be configured to a single external authentication system but in fact to use any number of authentication systems. In this model, the authentication event can be performed by any trusted Identity Provider. The basic function of an IdP is to be an authoritative source for establishing and maintaining both identities and credentials. An IdP could be a commercial vendor such as Verizon, Comcast, or AT&T that has a business relationship with individuals. Similarly, an IdP could be a company such as Google, Yahoo!, Microsoft, or MySpace, that offers free services but also tracks relevant identity information. It is important to point out that while all of these IdPs can authenticate an individual, it is critical that the identity management system at the local healthcare provider have the ability to map the external IdP's identifier to a user in the local system. For example, many of the free IdPs use an email address as the core identifier for users in their systems. An EHR system is likely to use something entirely different such as a Social Security number, Patient Number, or similar style identifier. Therefore the healthcare provider's IdM system needs to know how to map that external identifier to the internal identifier. It is also important to acknowledge that not all Identity Providers have the same security requirements for establishing identities and credentials. Consequently, not all Identity Providers can be extended the same amount of implicit trust that the user has proved their identity. In fact, it is this concept of varying trust or levels of assurance (LOA) that is central to regulating external credentials appropriately for EHR access.

When examining trust in an identity, there are 2 fundamental aspects that define assurance: 1) the degree of confidence in the vetting process for establishing the identity and matching credential, and 2) the degree of confidence that the user of the credential is the owner of the credential. The higher the level of confidence in both of these areas, the higher the level of assurance a system can have when using the associated credential. Depending on the needs or requirements of the system to be accessed, the appropriate LOA can be required of the credentials being used. The proposed framework involves creating identity assurance profiles with varying LOA that map directly to the National Institute of Standards and Technology's (NIST) e-Authentication specifications.

3. Defining Trust in an Identity

In 2003, the Federal Government's Office of Management and Budget (OMB) released memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*. This document laid out four distinct levels of assurance related to electronic identities used for electronic transactions. These levels are[2]:

- ❖ Level 1: Little or no confidence in the asserted identity's validity.
- ❖ Level 2: Some confidence in the asserted identity's validity.
- ❖ Level 3: High confidence in the asserted identity's validity.
- ❖ Level 4: Very high confidence in the asserted identity's validity.

OMB mandated that NIST establish technical standards for the implementation of each level of assurance. NIST subsequently created the *Electronic Authentication Guideline*[2] which now acts as the regulatory standard for all electronic authentication within resources of federal agencies. In 2008 the Federal Identity, Credential, and Access Management (ICAM) subcommittee of the General Services Administration Office of Government-wide Policy was established to improve electronic access to government resources[3]. These improvements included internal access, access with other government partners and agencies, external business partners, and with the American population at large. Consequently, one of the specific tasks ICAM performs is the evaluation of identity authentication models for possible adoption or integration by the Federal Government. Hence the guidelines laid out by both ICAM and NIST serve as the obvious benchmark that other industries could use to establish their own e-authentication requirements and provide the foundation for new trust frameworks.

The Centers for Medicare & Medicaid Services (CMS) has issued specific requirements dealing with e-authentication and levels of assurance when accessing protected health information (PHI) covered by the Health Insurance Portability and Accountability Act (HIPAA)[4]. CMS has determined the equivalent of NIST LOA Level 2 identity assurance is needed for accessing your own PHI and Level 3 for accessing PHI about someone else. This means potential IdPs for EHR systems would need to ensure an identity assurance equivalent to Level 2 or 3 depending on the type of access. This research lays out identity assurance profiles for Levels 1-3 that satisfy the NIST guidelines so Identity Providers can guarantee which LOA each of their credentials can reliably assert. An implicit trust can then be achieved with all recognized IdPs that assert a particular LOA credential since all IdPs would be using the same standardized identity assurance profiles. These arrangements would culminate in a many-to-many relationship between EHR systems and Identity Providers. Furthermore, if Cloud Identity Providers participated in this scheme, patients could leverage their existing Cloud credentials to access their medical information as shown in Figure 2. This results in patients being able to use the same, familiar Cloud credential to access EHR systems at different healthcare providers. As mentioned, the authentication event is just one of 3 aspects of access that need to be addressed but it represents a key user interaction point in the process. By taking advantage of existing Cloud credentials, healthcare providers can not only provide their patients with a familiar user experience but also effectively offload the username/password creation and maintenance effort. Password resets have traditionally been one of the largest technical support issues for organizations. This framework outsources this support issue to the Cloud.

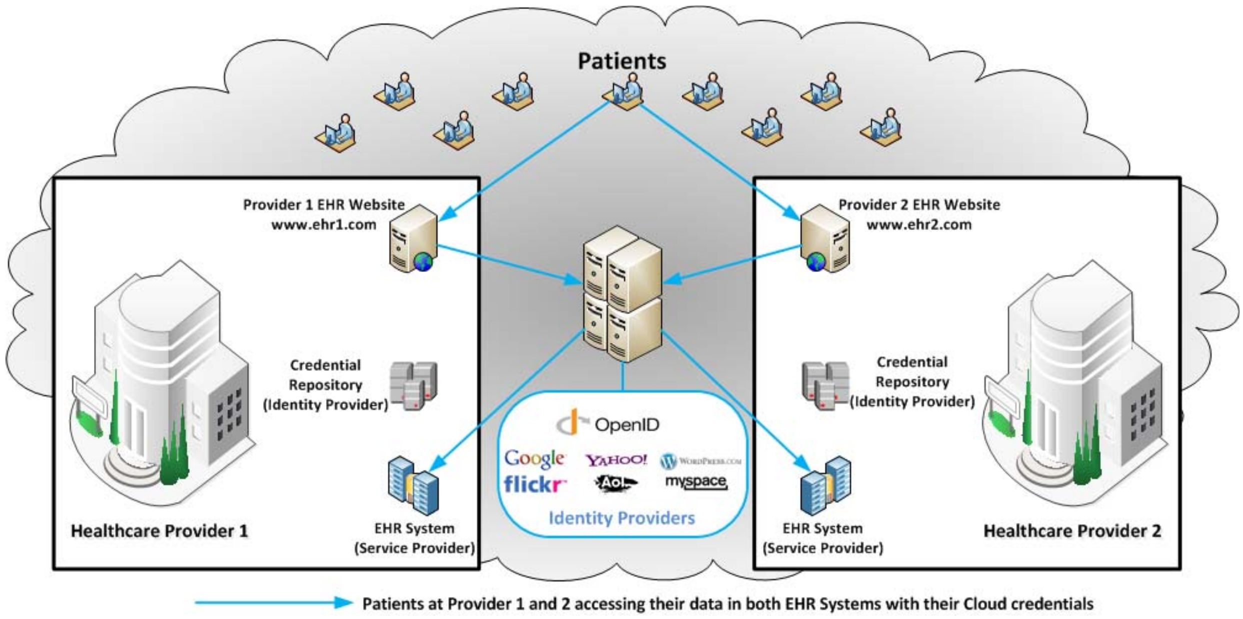


Figure 2. Federated EHR Access Model using the Cloud

While the concept of Identity Providers and Service Providers operating within a common identity assurance framework is extremely compelling, there clearly needs to be some level of governance to ensure its practical viability. This governance body would be responsible for establishing a certification process by which potential member healthcare providers could verify they are able to interoperate with Identity Providers while ensuring the security and privacy of the sensitive data they possess. The certification process for IdPs would be tiered to accommodate different criteria depending on the LOA of the credentials the IdP holds. The criteria for certification of each LOA profile are summarized in Table 1. With common profiles to follow, effectively any organization could participate as an Identity Provider including public organizations, private companies, or even healthcare providers themselves.

4. Criteria for Identity Profiles

Many of the criteria apply to all the LOA profiles used by Identity Providers. The higher the LOA of the identity to be asserted, the more scrutiny that must be given to how the identity was established, how the credentials issued, how the user asserts their identity, and the general integrity of the business practices of the IdP.

The General Requirements category covers the basic guidelines each IdP must meet or follow if they are to obtain certification for any level of assurance. It is necessary for the IdPs to demonstrate they are a legitimate entity and should indeed be recognized as an authoritative source of identity for other organizations. Further, IdPs must establish they can provide appropriate levels of liability for their actions. Lastly, IdPs must ensure they have documented policies and procedures and their practices are consistent with those documents.

The Infrastructure Guidelines category establishes guidelines for the Identity Provider's IT environment. All IdPs must ensure adequate software security by keeping all relevant software up to date and patched. This includes software used for: transactions of identities, credentials, and assertions; the authentication process; credential issuance and maintenance; and identity data storage. IdPs must be able to similarly demonstrate appropriate physical and network security exists at their respective locations where identity data is stored.

Table 1. Criteria for Identity Provider LOA Profiles

Category	Criteria	LOA 1	LOA 2	LOA 3
A. Organizational Requirements	1. Certification	♦	♦	♦
	2. Legal Status	♦	♦	♦
	3. Liability Provisions	♦	♦	♦
	4. Policies and Practices	♦	♦	♦
B. Infrastructure Guidelines	1. Software Security		♦	♦
	2. Physical Security		♦	♦
	3. Network Security		♦	♦
C. Identity Creation and Proofing	1. Identity Establishment		♦	♦
	2. Identity Proofing		♦	♦
	Existing Relationship		♦	♦
	In-Person Proofing		♦	♦
	Remote Proofing		♦	♦
	3. Record Retention		♦	♦
D. Identity Management Practices	1. LOA Classification per Identity	♦	♦	♦
	2. Consistent Data Definitions	♦	♦	♦
	3. Informed Consent	♦	♦	♦
E. Credential Management	1. Subject Interactions		♦	♦
	2. Revocation		♦	♦
	3. Reissuance		♦	♦
	4. Record Retention		♦	♦
F. Authentication Guidelines	1. Unique Identifier	♦	♦	♦
	2. Minimum Entropy of Authentication Secret	14 bits	20 bits	64 bits
	3. Protection of Authentication Secrets	♦	♦	♦
	4. Assertion Security	♦	♦	♦
	5. Multi-Factor Authentication			♦
G. Risk Mitigation	1. Acceptable Use Policies	♦	♦	♦
	2. Business Continuity		♦	♦
	3. Attack Resistant	♦	♦	♦
	4. Single Sign-on (SSO)	♦	♦	♦
	5. Credential Sharing Resistant	♦	♦	♦

The next category deals with how identities are created, vetted, and proofed. For IdPs asserting LOA 2 or 3 identities, processes must exist to verify the data they collect is based on public records or government-issued IDs. As this data will be the basis for which the digital identity will be established, it is critical that it is vetted before it is used for transactions outside of the Identity Provider. Once the identity has been registered, the IdP must perform identity proofing by ensuring that the collected information reflects an actual person, that the information can uniquely distinguish a single individual within the IdP's system, and that the person requesting the registration matches the identity being registered. The last part of this category covers the requirements for record retention of the registration process and how the identity was vetted and proofed.

The Identity Management section deals with how the Identity Provider defines, asserts, and releases identity information. The IdP must classify each digital identity it holds to a specific LOA and ensure there is no chance for identities to inadvertently have their LOA elevated. Each IdP will also need to conform to a standard set of data definitions for the identity data that will be shared with EHR systems to ensure interoperability. Before releasing data to an EHR system, the IdP must present the user with the specific data that will be released, allow the user to consent to the release, and then record the consent for non-repudiation. Informed consent has been an ever growing issue with transactions on the Internet and it is a critical component of any trust framework.

The Credential Management category deals with how credentials are used in transactions. IdPs are required to ensure users reassert their identity for each transaction in some fashion. Additionally, IdPs will ensure any credentials that are no longer valid for any reason will be revoked immediately. If a credential is ever reissued, the user must reestablish their identity by providing information from prior transactions such as by using pre-registered questions with responses not easily determined by anyone other than the user. The final aspect of this category is the requirement for IdPs to maintain a record of all credential management activities including issuance, revocation, expiration, and reissuance for a period not less than 180 days beyond the age of the credential. This level of documentation is needed for IdPs to sufficiently establish non-repudiation for the user's activities.

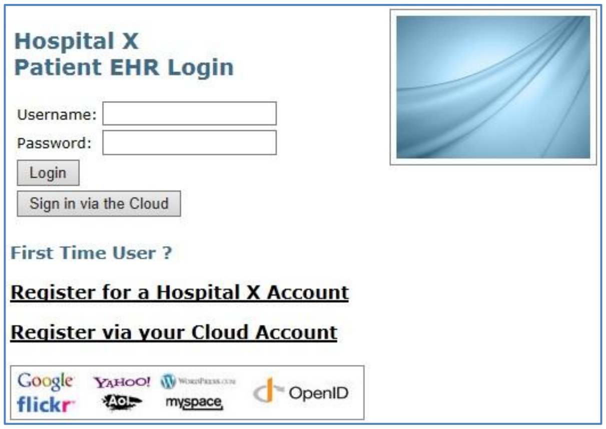
The Authentication Guidelines section stipulates how the authentication process must work on the IdP for the different levels of assurance. First and foremost, IdPs have to ensure all credentials they issue are unique and only correspond to a single individual. While a user could possibly have multiple credentials to validate themselves with, no set of credentials can be held by more than one user. Depending on the LOA, the authentication secret - commonly a password - needs to meet a certain degree of entropy or resistance to guessing. Entropy is achieved by making the authentication secret have adequate complexity parameters, limit the age and reuse of the secret, and limit the number of invalid attempts before the credential is disabled. For LOA 1, the minimum entropy for the authentication secret is 14 bits or 1 in 16,384 (2^{14}) chance of being guessed. For LOA 2, the minimum entropy is 20 bits and LOA 3 is 64 bits. The higher the LOA, the higher the resistance to guessing is required. It is a requirement for all LOA's that IdP's store the authentication secrets using industry-standard encryption algorithm to provide adequate protection while at rest. Similarly, IdPs must guarantee all communications between the user and the IdP are also encrypted. Lastly, IdPs that assert LOA 3 identities must utilize a form of multi-factor authentication while validating the user.

Risk mitigation is the final category of the profile. Each IdP must have acceptable use policies that their users are periodically informed of and the users' agreement to said policies is recorded. Additionally, IdPs must take steps to ensure business continuity by minimizing the chance of system failures. In the event there was a failure, IdPs must guarantee the failure wouldn't cause an inaccurate identity assertion being sent to an EHR system. IdPs must also be able to ensure that their authentication systems are resistant to various attacks including replay and eavesdropping. If IdPs use any type of single sign-on (SSO) technologies, they must utilize industry-standard techniques and encryption must be used to ensure their integrity. The final risk mitigation requirement is the IdP must demonstrate measures have been taken to resist credential sharing, either accidental or intentional.

5. Connecting the Cloud

The identity assurance profiles provide all parties a known set of rules by which to operate. However, beyond the profiles it is critical that organizations adopt an established internet standard to facilitate the sharing and exchanging of identity information. While there are more than a few options available, the prominent standards that have emerged are: 1) OpenID, 2) Security Assertion Markup Language (SAML), 3) OAuth, and 4) WS-Trust. While any and all of these technologies can provide a similar solution, this research purports that OpenID is the most suitable identity standard available. As such, the OpenID identity standard has been incorporated into this framework to provide the foundation for identity creation and credential distribution. OpenID consists of the most common Identity Providers available on the Internet including Google, Yahoo!, Flickr, MySpace, and AOL. Its corporate members add companies such as Microsoft, PayPal, Symantec, and Verizon to create an organization with significant market share in the digital identity space. Over a billion OpenID enabled accounts exist and are being used by more than 50,000 websites today[5]. By choosing a standard that is already in use by so many individuals and sites, the barriers for entry and user acceptance are significantly lower than other alternatives. The Federal Government has recognized OpenID as an important standard with which to interoperate. ICAM has approved an OpenID profile that is certified for LOA 1 authentication for Federal Government resources[6]. The creation of a profile for LOA 2 and LOA 3 for use with the government is well underway; further signifying the wide adoption of the standard by the public and private sectors.

While the OpenID standard facilitates the authentication event, organizations must also address how the OpenID identity is connected or mapped to the organization's record of that identity. The mapping process can have user involvement or not, depending on the data held by the external IdP and the degree of trust extended to how the data was vetted as belonging to the user. A base solution offered by the framework is a user-driven registration process as shown in Figures 3 through 8. This process begins at the healthcare provider's EHR login page or patient portal.


Hospital X
Patient EHR Login

Username:
Password:

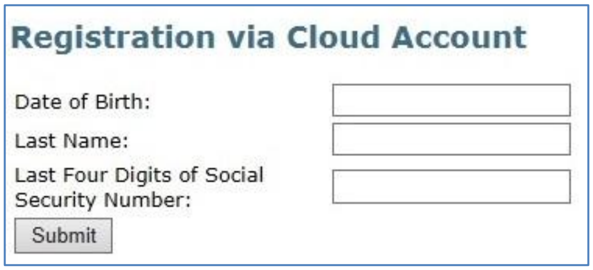
First Time User ?

Register for a Hospital X Account

Register via your Cloud Account

Figure 3. Example Patient Portal

From this page, the patient would choose to register themselves with the EHR site by clicking the "Register via your Cloud Account" link. The patient would be directed to a simple registration page, hosted by the healthcare provider, that would initially ask them to enter a few pieces of known identifiable information as depicted in Figure 4.


Registration via Cloud Account

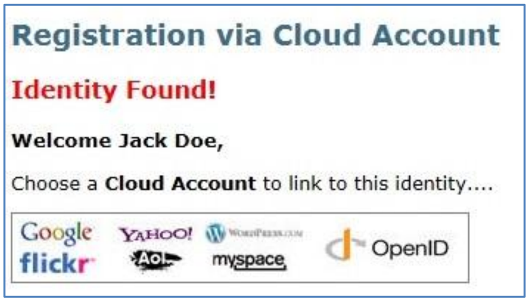
Date of Birth:

Last Name:

Last Four Digits of Social Security Number:

Figure 4. Registration via the Cloud - Step 1

The information entered on this page allows the user to uniquely identify themselves to the healthcare provider while providing a degree of confidence that it is indeed the patient registering on the site. Once the healthcare provider has verified the information against its records, the site will notify the patient that their identity has been established.


Registration via Cloud Account

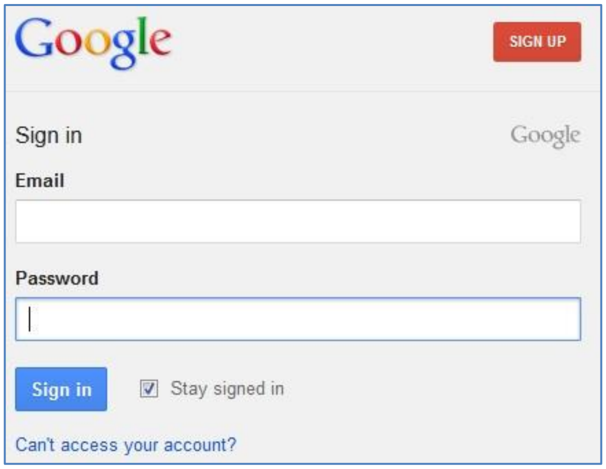
Identity Found!

Welcome Jack Doe,

Choose a **Cloud Account** to link to this identity....

Figure 5. Registration via the Cloud - Step 2

The patient will then choose a Cloud Account of their choice to link to the confirmed identity. Once the patient has selected an OpenID provider (a Cloud Account), they are directed to that Cloud service's authentication page and prompted to enter those credentials.



Sign in

Email

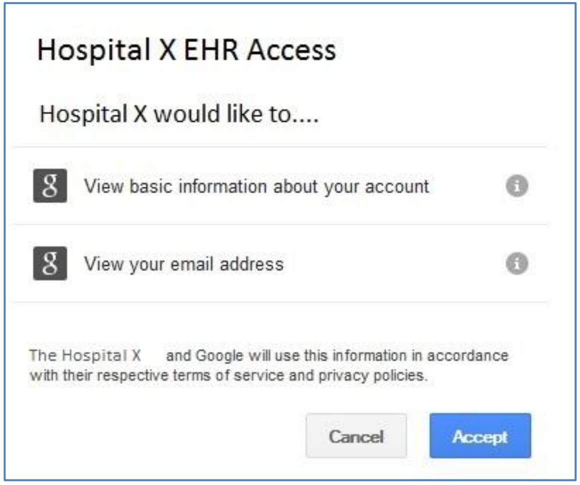
Password

☑ Stay signed in

Can't access your account?

Figure 6. Registration via the Cloud - Step 3

Once the credentials have been verified by the OpenID provider, a data release consent page will be presented to the patient.


Hospital X EHR Access

Hospital X would like to....

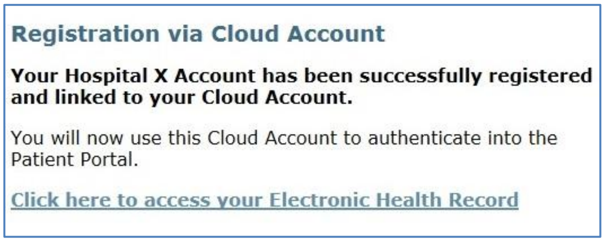
View basic information about your account

View your email address

The Hospital X and Google will use this information in accordance with their respective terms of service and privacy policies.

Figure 7. Registration via the Cloud - Step 4

This page will describe which specific pieces of information the healthcare provider is requesting from the Cloud account. Once the patient has consented to the release of the information, the mapping is complete.



Registration via Cloud Account

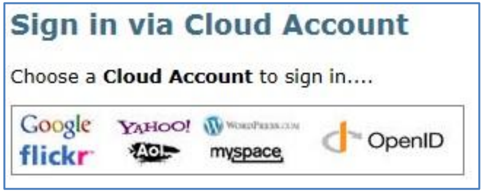
Your Hospital X Account has been successfully registered and linked to your Cloud Account.

You will now use this Cloud Account to authenticate into the Patient Portal.

Click here to access your Electronic Health Record

Figure 8. Registration via the Cloud - Step 5

This simplistic approach is used extensively within the Cloud today by many merchants and web resources, presenting options such as 'Register with Google' or ‘Register with Facebook’. Healthcare providers would essentially be doing a similar type registration process by letting their patients attach a Cloud credential to their identity in the provider's EHR. With the Cloud credential mapped to an EHR identity, patients could then log into the EHR application using that credential. The patient portal or EHR authentication page would simply have a link to “Sign in via the Cloud”, similar to Figure 3. After a patient clicks the link they would be directed to then choose a Cloud Account (an OpenID provider), similar to Figure 9.

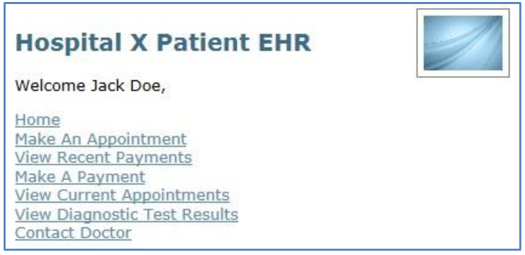


Sign in via Cloud Account

Choose a **Cloud Account** to sign in....

Figure 9. Authentication via the Cloud

Once the OpenID provider was selected, the patient would be presented with the respective OpenID provider’s authentication screen, as seen in Figure 6, the same screen presented by the OpenID provider as part of the registration process. After successful authentication, the patient would be redirected back directly into the EHR application.



Hospital X Patient EHR

Welcome Jack Doe,

Home
Make An Appointment
View Recent Payments
Make A Payment
View Current Appointments
View Diagnostic Test Results
Contact Doctor

Figure 10. Sample Patient EHR

Using this model, different patients could be using their Cloud account of choice from any one of the different OpenID providers to gain access to the same EHR system. This approach affords healthcare providers a flexibility for authentication to their system such that patients will be able to use credentials they use on a daily basis, for access many other electronic resources in their personal life. Further, for all healthcare providers that implemented this solution, common patients of those providers could use the same set of credentials to access their EHR across all of those providers. This type of pervasive access to EHR systems across the industry is exactly the direction that the federal government and patients alike are starting to demand.

6. Research Implementation

In order to demonstrate the viability of the proposed framework, 2 regional hospitals were engaged. Each of these hospitals interact with a significant number of patients each year and are both faced with the daunting and costly challenge of providing them access to their electronic health records in a timely fashion. Hospital 1 has over 800 licensed beds and more than 350,000 patient admissions (combined inpatient and outpatient) every year, while Hospital 2 has over 400 beds and more than 400,000 patient admissions each year. With hundreds of thousands of patients each year, both hospitals are expending significant resources related to helping patients gain electronic access to their health records. The IT helpdesk at Hospital 1 reported fielding almost 37,000 calls per year related specifically to patient authentication issues. Authentication issues include questions about a patient's username, password, secret question and answer or pin for resetting a forgotten password, and other general inquiries. The breakdown of helpdesk tickets for each particular authentication issue is illustrated in Figure 11.

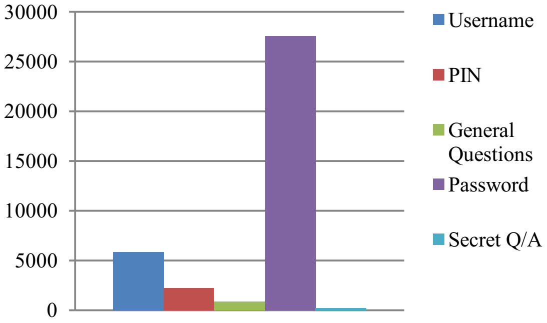


Figure 11. Annual Helpdesk Tickets Related to Authentication

Beyond authentication issues, each hospital's IT helpdesk were fielding thousands of calls related to how to establish their account with the hospital or the need to update their email address in the system. Cloud IdPs have a vested interest in keeping contact information such as name and email up to date. With this research's proposed integration, healthcare providers can easily extract this information from the Cloud periodically for all the patients that have registered their Cloud identities with the healthcare provider.

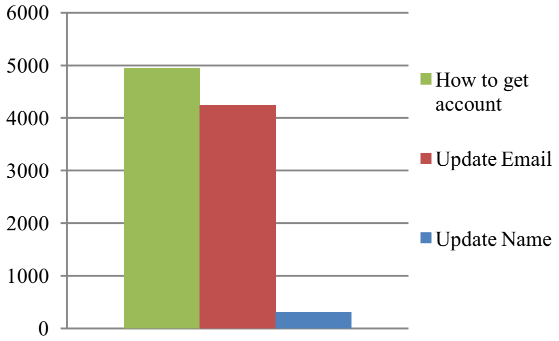


Figure 12. Annual Helpdesk Tickets Related to Contact Information

Each of the partner hospitals was looking to leverage existing, robust technologies to solve their patient access issues. Using the proposed framework, a series of pilots and concept projects were established with Hospital 1 and are currently under consideration by the Hospital 2. In addition to patient access to EHR data, Hospital 1 was able to successfully use their credential repository to federate with a number of National Institutes of Health (NIH) resources including PubMed, the Clinical Translational Sciences Award (CTSA) Management System, and the database of Genotypes and Phenotypes (dbGaP) using the same basic federated authentication framework. Additionally, the hospital implemented a full pilot project using this framework and the LOA 2 profile to integrate OpenID access to their radiology scheduling application as well as one of their diagnostic testing applications. Once the pilot was up and running, it allowed patients to use their Cloud credentials to schedule, modify, and view radiology and diagnostic testing appointments and results. This particular pilot has been significantly beneficial for the Hospital 1 and its patients alike. The Cloud access model requires very little user support overhead compared to the hospital supporting a system that issues, maintains, and revokes credentials for all their patients. The healthcare provider's IT helpdesk has estimated almost a 60% reduction in the number of tickets related to authentication issues for the pilot applications since instituting OpenID integration. Based on this trend and if OpenID was integrated across all systems that patient access electronically, the healthcare provider could potentially see a reduction of upwards of 22,000 tickets annually. The man-hours associated to this reduction in helpdesk tickets is quite significant and therefore a very compelling reason to move forward. In fact, due to the tremendous success of these pilots, other integrations are already being considered and planned by Hospital 1 to include nearly all scheduling applications (physician practices, diagnostic, imaging), patient reminders for preventive/follow-up care, and patient discharge instructions dissemination. While not as far along as Hospital 1, Hospital 2 is actively performing use-case analyses to determine how best to integrate this research into their environment. Building upon the early successes with this research's framework, Hospital 1 is positioned to continue to grow their Cloud integration to the point of truly achieving patient access for all health information electronically.

7. Future Directions

The pilots at Hospital 1 have been demonstrating the framework proposed by this research addresses the identity management crisis both from the healthcare provider and patient perspective. It is important to note that numerous organizations and foundations are similarly working in the identity space related to portable digital identities. Considerable work is being done in the higher education community by Internet2 and the InCommon federation to enable universities access to other universities' and governmental resources using a single digital identity housed at the home institution. InCommon has been working extensively with federating technologies for the last decade and by no accident has become the first trust framework ICAM has approved for LOA 1-2 access for federal resources[7]. In the private sector, the Open Identity Exchange (OIX) is working closely with ICAM to advance private trust frameworks and identity portability to access federal resources using OpenID[8].

It is important to note that there are a number of other mature technologies and protocols that allow for a federated authentication model similar to OpenID. Security Assertion Markup Language (SAML), perhaps OpenID's most prevalent alternative, is used heavily within the higher education community and throughout many federal government agencies. Many organizations have other Single Sign-on (SSO) technologies such as Jasig's Central Authentication Service (CAS)[9] and Microsoft's Active Directory Federation Services (ADFS)[10] that effectively accomplish the same basic federated approach. As many organizations adopt one solution or the other, considerable work is being done to establish bridges between the technologies to expand the possibilities of interoperability even farther. Social-to-SAML[11] is one such project that allows OpenID Identity Providers to authenticate users into resources of SAML Service Providers. Likewise, there are projects in varying stages for almost all the major SSO solutions to interoperate in all conceivable directions. Therefore it is not as critical which solution an industry or entity embraces as it is that they move quickly and surely to make the necessary organizational and technical choices to position themselves to participate.

Clearly all of this work is moving in the same direction with all industries and technologies converging to form a larger interoperable community. The White House has solidified this trend in their National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative. NSTIC is singularly tasked with creating an "Identity Ecosystem" of interoperable technology standards and policies to be used across all sectors to provide increased security and privacy, but most importantly ease of use for individuals[12]. This national strategy in conjunction with the Meaningful Use objectives only further cements the need for the healthcare industry to entirely restructure their approach for identity access and management from a centralized to a distributed model.

8. Conclusion

Ubiquitous access is no longer a fantastical dream; it is a reality and quickly becoming an expectation by our connected society. The Meaningful Use objectives continue to push healthcare providers to enable patients greater and easier access to their health information. As healthcare organizations attempt to determine the best course of action, it is critical that they adopt scalable and interoperable solutions to not only satisfy the immediate needs but prepare for the future.

Usability underpins this entire issue. While patient authentication is essentially just the first step in providing access, it can be a crippling area if not approached properly. This research lays out a solution for healthcare providers to get out of the 'username/password business'. The existing Identity Providers in the Cloud are investing billions of dollars cumulatively every year towards usability. Much of their usability efforts are centered on making their services easy to use and prevalently placed throughout the Internet. Basic authentication functionality such as looking up a username or resetting a password is fundamental to the Cloud and is constantly being refined and improved. Healthcare providers can simply leverage this incredible investment instead of trying to emulate and duplicate it. Further, these Cloud Identity Providers enable entities to leverage their services for absolutely no cost beyond the man-hours required to configure the integration.

This research builds on many of the lessons learned by other industries to provide a mature, feasible solution to an otherwise overwhelming problem. With OpenID at the heart of this framework, the gap from the healthcare industry to the Cloud identity space can be bridged and interoperability with industries across the spectrum can be achieved.

9. References

[1] Blumenthal, D., & Tavenner, M. (2010). The “Meaningful Use” Regulation for Electronic Health Records. *New England Journal of Medicine, 363*, 501-504. doi:10.1056/NEJMp1006114.

[2] United States. Department of Commerce. National Institute of Standards and Technology. (2011). “Electronic Authentication Guide (rev 1),” retrieved December 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.

[3] United States. General Services Administration. Office of Government-wide Policy. (2012). "Federal Identity, Credential, and Access Management," retrieved November 2012, http://www.idmanagement.gov/pages.cfm/page/ICAM.

[4] United States. Department of Health and Human Services. Centers for Medicare & Medicaid Services. (2011). " CMS System Security and e-Authentication Assurance Levels by Information Type," retrieved November 2012, http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/System-Security-Levels-by-Information-Type.pdf.

[5] OpenID Foundation. (2012). "What is OpenID?" retrieved November 2012, http://openid.net/get-an-openid/what-is-openid/.

[6] United States. General Services Administration. Office of Government-wide Policy. (2009). "OpenID 2.0 Profile," retrieved November 2012, http://www.idmanagement.gov/documents/ICAM_OpenID20Profile.pdf.

[7] Internet2. InCommon. (2012). "What is the Assurance Program?" retrieved November 2012, http://www.incommon.org/assurance/.

[8] Open Identity Exchange. (2012). "About Open Identity Exchange," retrieved November 2012, http://openidentityexchange.org/about.

[9] Jasig. (2012). "CAS," retrieved December 2012, http://www.jasig.org/cas.

[10] Microsoft. (2012). "Windows Server: Active Directory Federation Services," retrieved December 2012, http://technet.microsoft.com/en-us/windowsserver/dd448613.

[11] Internet2. (2012). "Social and Organizational Identities Discussion Space, " retrieved December 2012, https://spaces.internet2.edu/display/socialid/Home.

[12] United States. Department of Commerce. National Institute of Standards and Technology. (2012). "About NSTIC," last accessed November 2012, http://www.nist.gov/nstic/about-nstic.html.