Leveraging the Cloud for Electronic Health Record Access

by Brian Coats, MS, and Subrata Acharya, PhD

Abstract

Healthcare providers are under increasing pressure to enable widespread access to their electronic health record (EHR) systems for the patients they serve; the meaningful use incentive programs are perhaps the most significant driver encouraging this access. Elsewhere, the cloud has become extremely efficient and successful at establishing digital identities for individuals and making them interoperable across heterogeneous systems. As the healthcare industry contemplates providing patients access to their EHRs, the solution should leverage existing cloud investment, not duplicate it. Through an analysis of industry standards and similar work being performed in other industries, a trust framework has been derived for exchanging identity information. This research lays out a comprehensive structure that healthcare providers can easily use to integrate their EHRs with the cloud for identity validation, while meeting compliance guidelines for security and privacy. Further, this research has been implemented at a large regional hospital, yielding immediate and tangible improvements.

Keywords: identity assurance; OpenID; portable identity; identity management; federated authentication

Introduction

Many healthcare providers are finding themselves poorly positioned to enable the types of distributed access that electronic health record (EHR) systems are supposed to facilitate. The regulations and programs that are driving EHR adoption, including the Health Insurance Portability and Accountability Act (HIPAA) and the incentives for meaningful use of EHRs, provide almost zero guidance on how to address these 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 to their EHR systems by their patients from the cloud.

Background and Significance

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, has been heralded as providing the healthcare community a "transformational opportunity to break through the barriers to progress."[1] As part of the HITECH Act, the Department of Health and Human Services established the meaningful use program, which authorizes incentive payments to healthcare providers that use certified EHR technology to accomplish specific objectives in care delivery. A number of the objectives for meaningful use require

healthcare providers to provide patients access to their health records. The recent stage 2 objectives specifically mandate that hospitals grant patients access to view, download, and transmit their health information online within 36 hours of discharge; eligible professionals (EPs) have to do this within four business days. Unfortunately, little to no guidance is given for how this should be accomplished. Similarly, the healthcare information technology industry has long discussed the issue and challenges of providing patient access to health records,[2–4] with very little in the way of solutions.

At the core of establishing access is the reliable validation of the identity of a user accessing the protected health information (PHI). The healthcare industry has traditionally followed the approach of each provider creating its own silos of data stores and corresponding security frameworks to access the data. The long-established model for authentication of all electronic systems, including EHR systems, is that the credentials used to validate identity are stored within the application being accessed, as depicted in Figure 1. The establishment, issuance, and maintenance of digital identities and corresponding credentials create a usability barrier for patients as well as an efficiency barrier for healthcare providers. Usability of EHR systems starts with being able to log in. If patients are forced to contact each of their healthcare providers for unique credentials, logging in becomes significantly harder and more confusing than if the patients can log in using credentials they are already familiar with. Similarly, having a healthcare provider create and maintain the technical and support systems to issue credentials is unnecessary and therefore inefficient compared to using a preexisting infrastructure that has very little additional 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 to adopt technical and organizational solutions that are scalable and that easily interoperate throughout the entire healthcare industry and beyond.

Methods

Creating a Portable Access Model

When an entity creates electronic identities and configures applications to leverage those identities, three fundamental issues need to be addressed: Who does the digital identity belong to? How do individuals prove their identity? What should the user be allowed to access or do in the relevant application? These three issues are more technically referred to as identity management, authentication, and authorization. Identity management consists of the underlying processes and systems that establish and keep track of who an individual is and that allow other systems to relate a digital identity to an actual person. *Authentication* and *authorization* are many times incorrectly used interchangeably or combined as a single issue called "access," but they refer to two very distinct steps. Authentication is how individuals prove who they are. On the other hand, authorization addresses what privileges each 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.

Authorization decisions must inherently be made at the application level, but authentication can almost always be externalized from the resource being accessed. The authentication event has three subcomponents: the user with possession of a credential; the identity provider, an authentication system that can validate said credentials; and the service provider, the application that recognizes the identity. As Figure 1 shows, traditional systems have the credential repository or identity provider built into the application itself. 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. Therefore, as healthcare providers address electronic access to their EHR systems, the challenge of authentication can be 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 a single EHR system can be configured to use any number of

authentication systems, as depicted in Figure 2. In this model, the authentication event can be performed by any trusted identity provider. The ideal identity providers are commercial vendors that have existing business relationships with individuals. Some of the most prominent candidates are Verizon, Comcast, AT&T, Google, Yahoo, and Microsoft. 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 and password creation and maintenance effort. The existing identity providers in the cloud invest billions of dollars cumulatively every year on usability. Many of their usability efforts are centered on making their services easy to use and prominently 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. In fact, as discussed in the Results section below, password resets are one of the largest technical support issues for organizations. This framework outsources this support issue by allowing healthcare providers to simply leverage the cloud's existing investment instead of trying to duplicate it. Further, these cloud identity providers enable entities to leverage their services for absolutely no cost beyond the person-hours required to configure the integration.

Connecting the Cloud

Two fundamental aspects define assurance of trust in an identity: (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. The proposed framework involves creating identity assurance profiles, summarized in Table 1, with varying trust or levels of assurance (LOAs) that map directly to the National Institute of Standards and Technology (NIST) electronic authentication specifications.[5] The Centers for Medicare and Medicaid Services (CMS) has issued its own specific requirements dealing with electronic authentication and LOAs when accessing PHI covered by HIPAA.[6] CMS has determined that the equivalent of NIST LOA level 2 identity assurance is needed for individuals accessing their own PHI and the equivalent of level 3 is necessary for individuals accessing PHI about someone else.

The identity assurance profiles provide all parties a known set of rules by which to operate. However, in addition to the profiles, it is critical that organizations adopt an established Internet standard to facilitate the sharing and exchanging of identity information. Numerous options are available, and while any of these technologies can provide a similar solution, this research purports that OpenID is the most suitable identity standard available. Thus, 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. In addition to Google and Yahoo, its other corporate members include companies such as Microsoft, PayPal, Symantec, and Verizon, creating an foundation with significant market share in the digital identity space. More than a billion OpenID-enabled accounts exist and are being used by more than 50,000 websites.[7] With the adoption of a standard that is already in use by so many individuals and sites, the barriers for entry and user acceptance are significantly lower than with other alternatives.

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 identity provider and the degree of trust extended to how the data were 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. From this page, the patient would choose to register 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 the patient to enter a few pieces of known identifiable information. (See Figure 4.) The information entered on this page allows users 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 the identity has been established. (See Figure 5.) The patient will then choose a cloud account to link to the confirmed identity. Once the patient has selected an OpenID provider (a cloud account), the patient is directed to that cloud service's authentication page and is prompted to enter those credentials. (See Figure 6.) Once the credentials have been verified by the OpenID provider, a data release consent page will be presented to the patient. (See Figure 7.) 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. (See Figure 8.)

This simplistic approach is used extensively within the cloud today by many merchants and web services, presenting options such as "Register with Google" or "Register with Facebook." Healthcare providers would essentially be using a similar registration process by letting their patients attach a cloud credential to their identity in the 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 "Sign in via the Cloud" link, similar to that shown in Figure 3. After a patient clicks the link, the patient would be directed to choose a cloud account (an OpenID provider), as shown in Figure 9. Once an OpenID provider is selected, the patient is 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 into the EHR application. (See Figure 10.)

Using this model, different patients could use a cloud account of their choice from any one of the various OpenID providers to gain access to the same EHR system. This approach affords healthcare providers flexibility in the authentication to their system such that patients will be able to sign in with credentials that they use on a daily basis to access many other electronic resources in their personal lives. Further, for all healthcare providers that implement this solution, common patients of those providers could use the same set of credentials to access their EHRs 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.

Results

To demonstrate the viability of the proposed framework, partnerships were established with two regional hospitals. Each of these hospitals interacts with a significant number of patients each year, and both are faced with the daunting and costly challenge of providing these patients access to their EHRs in a timely fashion. Hospital 1 has more than 800 licensed beds and more than 350,000 combined inpatient and outpatient admissions every year, while Hospital 2 has more than 400 beds and more than 400,000 patient admissions each year. With hundreds of thousands of patients each year, the effort required to provide patients with electronic access to their health records is significant. In fact, Hospital 2 has not provided any patient access to date because the necessary resources have been deemed so high. Hospital 1, which is providing patient access, reported that the information technology (IT) help desk fielded almost 37,000 calls in 2012, shown in Figure 11, related specifically to patient authentication issues. Authentication issues included questions about a patient's username, password, and secret question and answer or PIN for resetting a forgotten password, as well as other general inquiries.

Both of the hospitals were 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 Hospital 2. Hospital 1 has implemented a full pilot project using the framework to integrate OpenID access into its radiology scheduling application as well as one of its 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 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 of its patients. The healthcare provider's IT help desk has estimated almost a 60% reduction in the number of tickets related to authentication issues for the pilot applications since instituting OpenID access. If this trend continues and if OpenID is integrated across all systems that patients access electronically, the healthcare provider could potentially see a reduction of more than 22,000 tickets annually. The person-hours associated with this reduction in help desk tickets is significant and provides an extremely compelling reason to move forward. In fact, because of 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 and follow-up care, and dissemination of patient discharge instructions. 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 its environment. Building upon the early successes with this research framework, Hospital 1 is positioned to continue to grow its cloud integration to the point of truly achieving patient access for all health information electronically.

Discussion

The pilots at Hospital 1 have demonstrated that the framework proposed by this research addresses the identity management crisis from both the healthcare provider and patient perspectives. Numerous organizations and foundations are likewise working in the space related to portable digital identities. Considerable work is being done in the higher education community by Internet2 and the InCommon federation to enable individuals at universities to access other universities' resources 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 the Federal Identity, Credential, and Access Management (FICAM) program has approved for LOA level 1–2 access for federal resources.[8] 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.[9, 10] Verizon has recently developed a software as a service (SaaS) offering to perform external authentication, similar to that proposed by this research, specifically for healthcare organizations.[11] This research demonstrates specifically how a federated authentication model can be replicated using an open-source style architecture to leverage credentials held by a larger population of patients while significantly lowering costs to the healthcare provider.

A number of other mature technologies and protocols allow for a federated authentication model similar to OpenID. Security Assertion Markup Language (SAML), perhaps OpenID's most prominent 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)[12] and Microsoft's Active Directory Federation Services (ADFS),[13] that effectively accomplish the same basic federated approach. As many organizations adopt one solution or the other, considerable work is being done to bridge the technologies, expanding the possibilities of interoperability even further.[14] Likewise, initiatives for almost all the major SSO solutions to interoperate in all conceivable directions are underway. Therefore, the particular solution an industry or entity embraces is less important than the fact that it moves quickly and surely to make the necessary organizational and technical choices to participate in these technologies.

Clearly all of this work is moving in the same direction, with industries and technologies converging to form a larger interoperable community. The White House has solidified this trend with the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative. NSTIC has been tasked with creating an "Identity Ecosystem" of interoperable technology standards and policies to be used across all sectors to provide increased, security and privacy and, most importantly, ease of use for individuals.[15] In conjunction with the meaningful use objectives, this national strategy only further cements the need for the healthcare industry to restructure its approach to identity access and management from a centralized to a distributed model.

Conclusion

Ubiquitous access is no longer a fantastical dream; it is a reality and is quickly becoming an expectation by our connected society. The meaningful use objectives continue to push healthcare providers to allow 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 not only to satisfy immediate needs but to prepare for the future. 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 between the healthcare industry and the cloud identity space can be bridged, and interoperability with industries across the spectrum can be achieved.

Brian Coats, MS, is a doctoral candidate in the Department of Computer and Information Sciences at Towson University in Towson, MD.

Subrata Acharya, PhD, is an assistant professor in the Department of Computer and Information Sciences at Towson University in Towson, MD.

Notes

1. Blumenthal, D., and M. Tavenner. "The 'Meaningful Use' Regulation for Electronic Health Records." *New England Journal of Medicine* 363 (2010): 501–4. doi:10.1056/NEJMp1006114.
2. Middleton, B., W. Hammond, P. Brennan, and G. Cooper. "Accelerating U.S. EHR Adoption: How to Get There from Here." *Journal of the American Medical Informatics Association* 12 (2005): 13–19. doi:10.1197/jamia.M1669.
3. Hassol, A., J. Walker, D. Kidder, K. Rokita, D. Young, S. Pierdon, D. Deitz, S. Kuck, and E. Ortiz. "Patient Experiences and Attitudes about Access to a Patient Electronic Health Care Record and Linked Web Messaging." *Journal of the American Medical Informatics Association* 11 (2004): 505–13. doi:10.1197/jamia.M1593.
4. Beard, L., R. Schein, D. Morra, K. Wilson, and J. Keelan. "The Challenges in Making Electronic Health Records Accessible to Patients." *Journal of the American Medical Informatics Association* 19 (2012): 116–20. doi:10.1136/amiajnl-2011-000261.
5. US Department of Commerce, National Institute of Standards and Technology. *Electronic Authentication Guide (Rev. 1)*. 2011. http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf (accessed December 4, 2011).
6. US Department of Health and Human Services, Centers for Medicare and Medicaid Services. *CMS System Security and e-Authentication Assurance Levels by Information Type*. 2011. http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/System-Security-Levels-by-Information-Type.pdf (accessed November 12, 2012).
7. OpenID Foundation. "What Is OpenID?" 2012. Available at http://openid.net/get-an-openid/what-is-openid/ (accessed November 5, 2012).
8. Internet2. InCommon. "What Is the Assurance Program?" 2012. Available at http://www.incommon.org/assurance/ (accessed November 5, 2012).
9. US General Services Administration, Office of Governmentwide Policy. "OpenID 2.0 Profile." 2009. http://www.idmanagement.gov/documents/ICAM_OpenID20Profile.pdf (accessed November 5, 2012).
10. Open Identity Exchange. "About Open Identity Exchange." 2012. Available at http://openidentityexchange.org/about (accessed November 7, 2012).
11. EMR, EHR & HIT News. "Verizon Gives Health Care Identity Services a Booster Shot." 2011. Available at http://www.emrandehrnews.com/2011/09/10/verizon-gives-health-care-identity-services-a-booster-shot/ (accessed August 1, 2013).
12. Jasig. "CAS [Central Authentication Service]." 2012. Available at http://www.jasig.org/cas (accessed December 19, 2012).
13. Microsoft. "Windows Server: Active Directory Federation Services." 2012. Available at http://technet.microsoft.com/en-us/windowsserver/dd448613 (accessed December 19, 2012).
14. Internet2. "Social and Organizational Identities Discussion Space." 2012. Available at https://spaces.internet2.edu/display/socialid/Home (accessed December 20, 2012).
15. US Department of Commerce, National Institute of Standards and Technology. "About NSTIC." 2012. http://www.nist.gov/nstic/about-nstic.html (accessed November 14, 2012).

Table 1

Criteria for Identity Provider Level of Assurance (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. Multifactor Authentication			♦
G. Risk Mitigation	1. Acceptable Use Policies	♦	♦	♦
	2. Business Continuity		♦	♦
	3. Attack Resistant	♦	♦	♦
	4. Single Sign-on (SSO)	♦	♦	♦
	5. Credential Sharing Resistant	♦	♦	♦

Figure 1

Traditional Electronic Health Record (EHR) Access Model

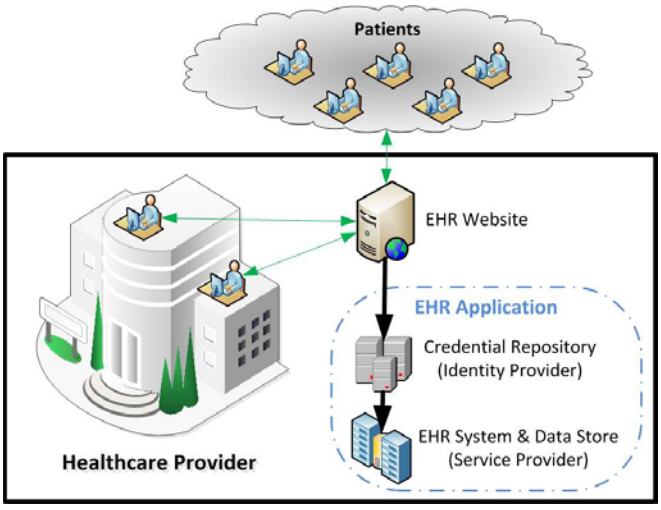

Figure 2

Federated Electronic Health Record (EHR) Access Model Using the Cloud

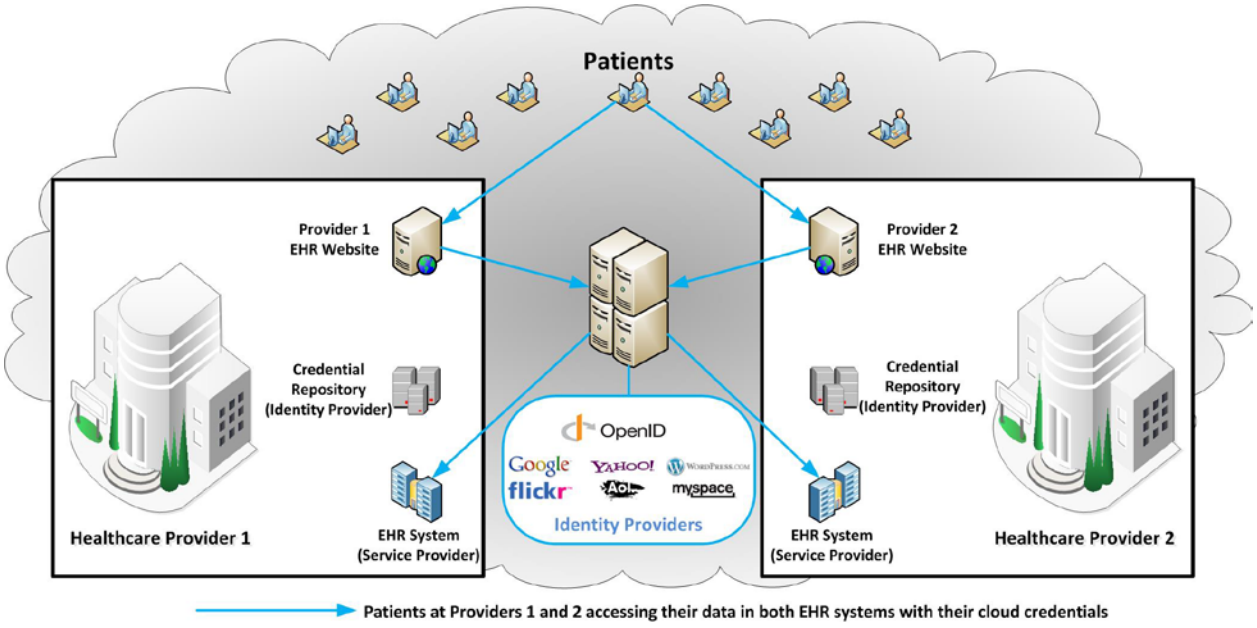

Figure 3

Example Patient Portal

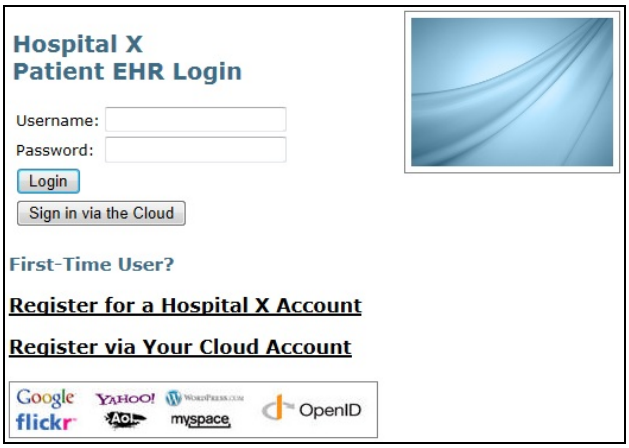

Figure 4

Registration via the Cloud—Step 1

Figure 5

Registration via the Cloud—Step 2

Figure 6

Registration via the Cloud—Step 3

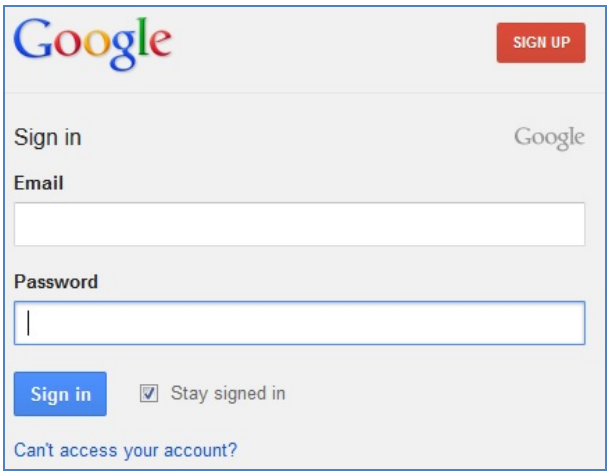

Figure 7

Registration via the Cloud—Step 4

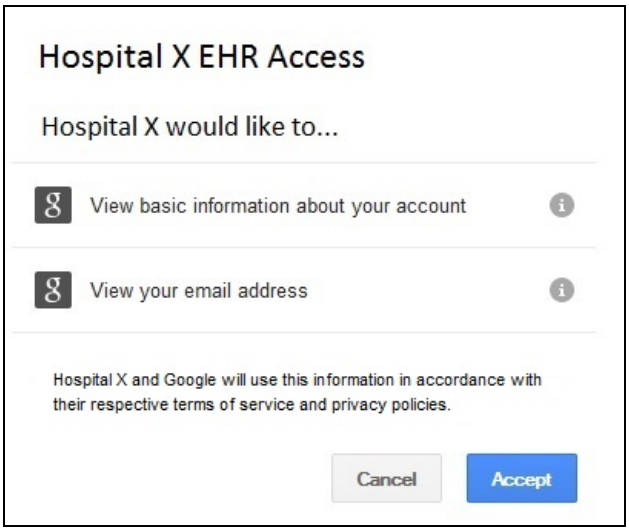

Figure 8

Registration via the Cloud—Step 5

Figure 9

Authentication via the Cloud

Figure 10

Sample Patient Electronic Health Record (EHR)

Figure 11

Annual Help Desk Tickets Related to Authentication