Implementation of a single sign-on system between practice, research and learning systems

Saptarshi Purkayastha[1]; Judy W. Gichoya[2]; Siva Abhishek Addepally[1]

[1] Department of BioHealth Informatics, Indiana University Purdue University, Indianapolis;
[2] Department of Radiology and Imaging Sciences, Indiana University School of Medicine, Indianapolis

Keywords

Integrated information systems, electronic health records, educational needs, single sign-on, Security Assertion Markup Language, SAML, Central Authentication System, CAS

Summary

Background: Multiple specialized electronic medical systems are utilized in the health enterprise. Each of these systems has their own user management, authentication and authorization process, which makes it a complex web for navigation and use without a coherent process workflow. Users often have to remember multiple passwords, login/logout between systems that disrupt their clinical workflow. Challenges exist in managing permissions for various cadres of health care providers.
Objectives: This case report describes our experience of implementing a single sign-on system, used between an electronic medical records system and a learning management system at a large academic institution with an informatics department responsible for student education and a medical school affiliated with a hospital system caring for patients and conducting research.
Methods: At our institution, we use OpenMRS for research registry tracking of interventional radiology patients as well as to provide access to medical records to students studying health informatics. To provide authentication across different users of the system with different permissions, we developed a Central Authentication Service (CAS) module for OpenMRS, released under the Mozilla Public License and deployed it for single sign-on across the academic enterprise. The module has been in implementation since August 2015 to present, and we assessed usability of the registry and education system before and after implementation of the CAS module. 54 students and 3 researchers were interviewed.
Results: The module authenticates users with appropriate privileges in the medical records system, providing secure access with minimal disruption to their workflow. No passwords requests were sent and users reported ease of use, with streamlined workflow.
Conclusions: The project demonstrates that enterprise-wide single sign-on systems should be used in healthcare to reduce complexity like "password hell", improve usability and user navigation. We plan to extend this to work with other systems used in the health care enterprise.

Correspondence to:
Saptarshi Purkayastha, PhD
Assistant Professor, Department of BioHealth Informatics
School of Informatics and Computing, Indiana University Purdue University Indianapolis
719 Indiana Avenue, WK 119, Indianapolis, IN 46202.
Email: saptpurk@iupui.edu
Phone: 317–274–0439

Appl Clin Inform 2017; 8: 306–312
https://doi.org/10.4338/ACI-2016-10-CR-0171
received: October 14, 2016
accepted: January 14, 2017
published: March 29, 2017
Citation: Purkayastha S, Gichoya JW, Addepally SA. Implementation of a single sign-on system between practice, research and learning systems. Appl Clin Inform 2017; 8: 306–312
https://doi.org/10.4338/ACI-2016-10-CR-0171

1. Background

Increased complexity of health care delivery and rising medical costs have led to regulatory changes in recent years including incentivizing health care providers to adopt electronic medical systems like computerized order entry systems, e-prescribing and clinical decision support [1]. This has increased digitization in the health system resulting in multiple new challenges including the lack of harmonization between multiple systems in the health care enterprise that disrupts clinical workflows [2, 3]. The result is fragmented systems that have been reported as barriers to adoption and use of electronic medical systems [4, 5].

A single patient visit generates multiple data points captured in multiple systems. Moreover, health care delivery is reliant on many ancillary systems including pharmacy dispensing software for medication management and dictation software for generating radiology reports. Each of these systems has separate user management, authentication and authorization procedures, increasing the complexity to manage user profiles and privileges across a health care enterprise with hundreds of users.

D'Costa-Alphonso et al. demonstrated that user identification requirements result in 12 passwords required for every healthcare worker to maintain the integrity of digital healthcare data [6]. Users also have to remember the username and passwords for each system as well as deal with session timeout occurrences. This complexity is considered a necessary evil by users and is referred to by many as "password hell" [7]. Moreover, in work environments where clinical service and research is part of expected responsibilities, additional user accounts are required for accessing the research systems like REDCap™, clinical trial registries and student learning management systems. Students in health informatics programs often have to deal with health data in a separate silo from assignments as the course work does not integrate electronic health record system information with the course assignments [8].

In an attempt to improve the balance between security and urgency of health care service delivery, health care providers have developed numerous workarounds to improve computer access [9]. These include use of Styrofoam cups to reduce session logouts, sharing logged in session as 'professional courtesy' and writing passwords on sticky notes attached to medical devices [ibid].

In the health care domain, the HL7 Context Management Specification (CCOW) [10] and the Enterprise User Authentication (EUA) [11] provide standards for user management across the enterprise. Yet, implementing these profiles in EHR systems often means implementing another central system such as Kerberos for EUA or multi-component, complex, user-interface level integration like CCOW that need strict changes in integration points and do not work on only data sharing [12]. Enterprises in other domains have implemented single sign-on (SSO) systems that can integrate diverse systems and improve user-experience [13–14], accessibility [15], and security [16, 17]. There are different types of single-sign on systems. Systems like OAuth [18] and OpenID [19] provide shared authentication to users while others provide authentication and authorization. Past user management research systems describe the term Reduced sign-on (RSO) to highlight the problem in implementing SSO where authentication or authorization is reduced and user logs are missed [20]. RSO prompts the user to enter another set of verification when they try to access critical applications, for example by requesting a hardware token number or asking a challenge question. While others have highlighted that SSO systems create a single point of failure, SSO makes it easier to contain user management in one place, instead of securing multiple locations. This is referred to as reducing the "attack surface", by having to manage fewer places of vulnerability [21].

2. Objectives

This case report describes our experience in integrating electronic medical systems with an SSO system that is already widely deployed and used at a large academic institution participating in training health informatics students, providing health care services across five hospitals and conducting research. Each student, staff or faculty is assigned a unique username powered by a SSO protocol and system, known as Central Authentication Service (CAS). We investigated the feasibility of utilizing this SSO system to support shared user access between a research database aggregating clinical in-

formation longitudinally from multiple systems in the health enterprise including EHR, RIS and PACS and a learning management system (LMS).

3. Methods

To evaluate the feasibility of SSO for shared user access, we selected two use cases. Both cases utilize OpenMRS, an open source, flexible medical records platform. OpenMRS is used in healthcare sites located in over 40 countries to manage health care provided to over 5.1 million patients [22]. At our institution, we used an instance of OpenMRS as a clinical data repository for patients who are treated with Yttrium-90 radio embolization (RE) at the radiology department, as shown in ▶Figure 1. The RE disease registry system combines clinical data from various practice systems including EHR, PACS and LIS that have separate authentication systems. A second OpenMRS instance is deployed in the informatics department as an EHR system that imports data from 7 community health centers in Indiana. This instance is used by health informatics researchers and students in the health informatics program. Course work such as lecture slides, assignments, quizzes are created in Canvas, a learning management system (LMS) used in multiple universities. The EHR system and LMS are separate systems and previously required students to have a different login accounts to access data for assignments, classwork, lab work or homework.

To integrate the SSO functionality, we developed the CASAuth module for OpenMRS which was deployed in both instances. The module is released under Mozilla Public License and is available at https://github.com/iupui-soic/openmrs-module-casauth/. Along with the authentication service provided by CAS, we also use the widely adopted SAML 2.0 standard in the module to share course details and user role (whether the user is student, instructor or teaching assistant) between the two systems.

We implemented user authorization using Shibboleth over the Security Assertions Markup Language (SAML) 2.0 protocol in the second instance because we wanted user role information when showing EHR data into the LMS. The CASAuth module registers a unique application key with CAS server. Once a user attempts to login to an OpenMRS resource that requires authentication (patient records, problem lists or any other data from the EHR), the user session is checked for validity. If the session is valid, the user's browser is redirected and provided the resource. If the session has expired, user is redirected to the CAS login screen, with our application key, as shown in ▶Figure 2.

This key is used to verify that the request is coming from a known application. This results in generating a jsessionid variable that is passed along to the CAS server's authentication page. The user fills in the SSO username and password, and on correct authentication, a SAML token (eduPersonPrincipalName (ePPN) in the form of a Universal Resource Name) along with the username is passed onto OpenMRS. OpenMRS uses this to authenticate the user with the appropriate privileges, since the SAML token contains user role information. We also get the assignment information passed as a session variable, when accessing data through the LMS. This allows OpenMRS to restrict data that is applicable for the current assignment using the row-per patient reporting module. This data is transferred from the EHR to the LMS, because we use the SAML token to identify the user's current session properties such as user role, scoped affiliation such as assignment details.

The SSO implementation has been used for over 12 months and we obtained detailed feedback from the users using a structured, open-ended questionnaire at the end of the course. The response rate was about 70%, with a mean response length of 883 words, divided across 10 questions (▶Supplement 1). The deep analysis for that has not been presented in this case report due to space constraints. For the radiology instance, we interviewed 3 researchers who used the repository. For the education instance, we requested feedback from all 86 users, who were enrolled in two courses that use the integrated EHR-LMS during this period, of whom 36 graduate and 18 undergraduate students, one instructor and two teaching assistants (TA) provided feedback. In the next section, we report on the lessons learnt in implementing an SSO that is appropriate for practice, research and learning systems in medicine.

4. Results

4.1 Integrating SSO for clinical registry

SSO use in our clinical registry simplifies user management across multiple roles. In the clinical data repository, we have data entry personnel, faculty supervisors, residents, and other cadres of health care providers. Using SSO we are able to assign different roles to users. No user accounts have required any password reset for the duration of the registry use in last 12 months that the repository has been running. Connecting to the CAS system was a critical component of passing security audits including HIPAA (Health Insurance Portability and Accountability Act) specified by the IT management team who maintain the health system infrastructure at our institution.

Standard practice in our institution is to run periodic security checks by the IT department. To enable system analysis, the security analysts needed a user created that matches their testing account specifications. We were able to bypass this by utilizing the CAS SSO login that had implied permissions and roles desired by the security team, thus saving us time on testing and modification of user roles to support such testing.

We continuously recruit more users into the system for various roles. The SSO allows us to standardize the onboarding process that requires minimal user account setup. In the past, we needed more paper work for account access to each system and specifications of user roles. Now the central system manages the account roles.

To support multisite data entry, we rely on VPN provided by various groups in our department. The IT administrators use SSO accounts to add users to the group required to use the clinical registry system without a need to track new users and manage password changes in a secondary system.

4.2 Integrating SSO for learning

Students in the health informatics program answered the feedback questionnaire showing that the coursework was more relevant from use of real patient data during learning, compared to only previously having to imagine how EHR systems work. The data sharing agreement with 7 CHCs mandate that we could use their data only for learning and not research purposes. We are also not allowed to share full data with anyone or dump data outside the EHR. Thus, we could not directly create accounts and provide full access to the EHR to students. The SSO integration enabled easy sharing of real patient data in a secured and controlled way through the integration between the EHR system and LMS. No passwords had to be reset during 12 months of use. TAs and instructors reported ease of grading, since they can view the data used by the student in an iframe within the LMS, which actually shares the same browser session between the LMS and the EHR.

5. Discussion

This case study is one of the first reports to look at integration of practice, research and learning systems with a single sign-on system. Our institution serves 5 different hospitals, each with its own health systems and support department. Health care providers of various cadres (nurses, physician assistants, residents, medical students and staff doctors) are shared across these 5 hospitals with periodic rotations in different clinical units that have implemented different electronic systems. Each system has its own user management. The single common account is the institution wide CAS login system.

Gartner et al reported that 30% of helpdesk calls were password related with an average cost of $32 for each reset password. An average user requires 4 password resets yearly [23]. Password managers that use a single master password to remember all other passwords, have been proposed as a solution to "password hell", yet these don't mitigate the disruption of workflow [24]. The user still has to authenticate for each new application. Local password managers don't work across machines and web based ones have a number of security issues that can be exploited [25]. From our experience using SSO for user management, we believe that enterprise SSO use can result in healthcare savings along with improved usability and security. Prior literature has described that clinicians

require an average 6.4 passwords per day to access patient data. Using SSO for clinicians can save 9.51 minutes per day per clinician [26]. Moreover, a previous study assessing the use of SSO on roaming computers in the emergency department improved productivity, ensured HIPAA compliance, improved user satisfaction, and, minimized errors, and disruption of critical work [26]. Our findings are similar, but also expand that multiple configurations in SSO system integration can be used for learning, practice and research systems in healthcare.

6. Conclusions

The project demonstrates that enterprise-wide single sign-on systems should be used in health systems, as it improves usability, security and workflow across disparate systems. We will extend this to work with PACS, labs and other systems.

7. Multiple Choice Questions:

1. Which of the following single-sign on protocol was integrated with the electronic health record system and the radiology clinical registry to manage user authentication?
A Learning Management System
B Central Authentication Service
C Virtual Private Network
D Open Medical Records System

The option B. Central Authentication Service (CAS) is the correct answer because it is a protocol used for sharing authentication between multiple systems. When a user tries to access a resources requiring authentication, they are redirected to the CAS login page and after successful login, the CAS system sends a service ticket back to the resource which validates that the user has been authenticated and can be provided with the requested resource.
2. Based on the paper's implementation, what is used to transfer role information between the learning management system (LMS) and the electronic health record system?
A Health Insurance Portability and Accountability Act
B Central Authentication Service
C HL7 Context Management Specification
D Security Assertions Markup Language (SAML) token

The option D. SAML token is the correct answer because it is an XML file, technically also called SAML Assertion, which is transferred from an identity provider (CAS server) to the service provider (LMS and EHR). This XML document contains user role information, along with other user details.

Clinical Relevance Statement

Use of SSO, can improve savings in healthcare IT implementations, improve usability for clinicians and reduce security problems. This means focus can be put on patient safety by avoiding workflow disruptions and security breaches.

Conflicts of interest

The authors declare that they have no conflicts of interest in the research.

Protection of Human and Animal Subjects

The study was performed in compliance with the World Medical Association Declaration of Helsinki on Ethical Principles for Medical Research Involving Human Subjects, and was reviewed by Indiana University Institutional Review Board (Protocol #1612648308).

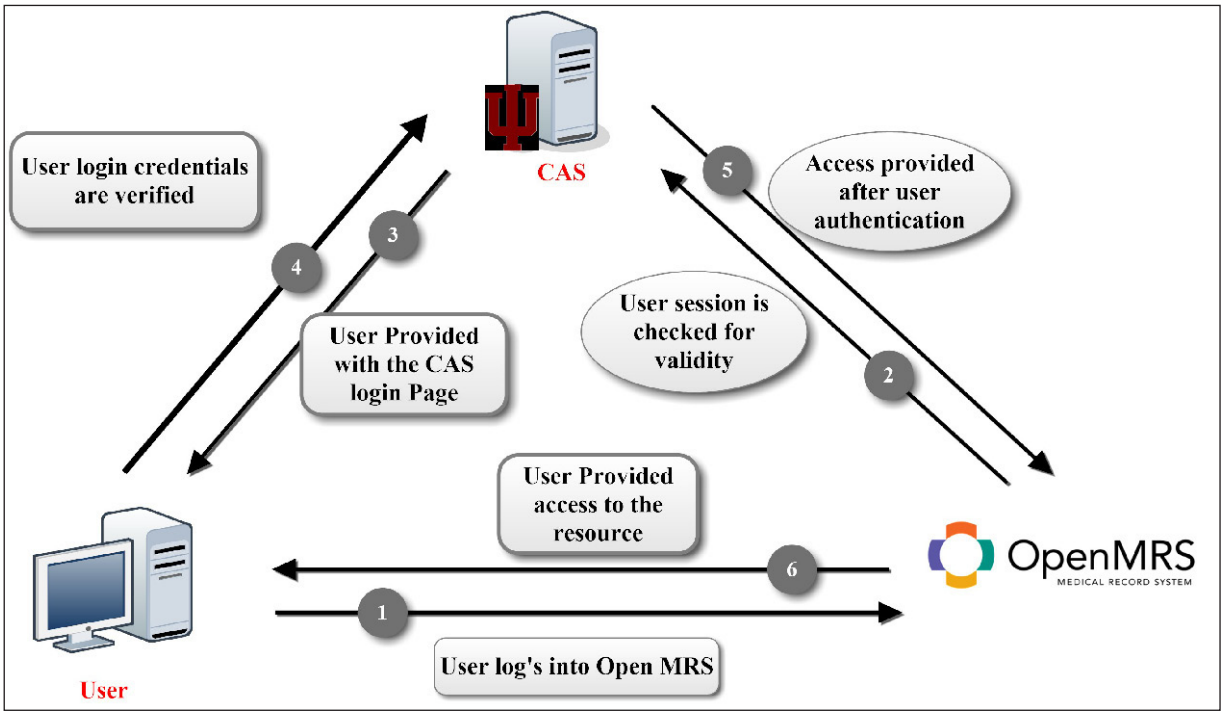

Fig. 1 CAS-only workflow used in Radiology Department for the radioembolization registry

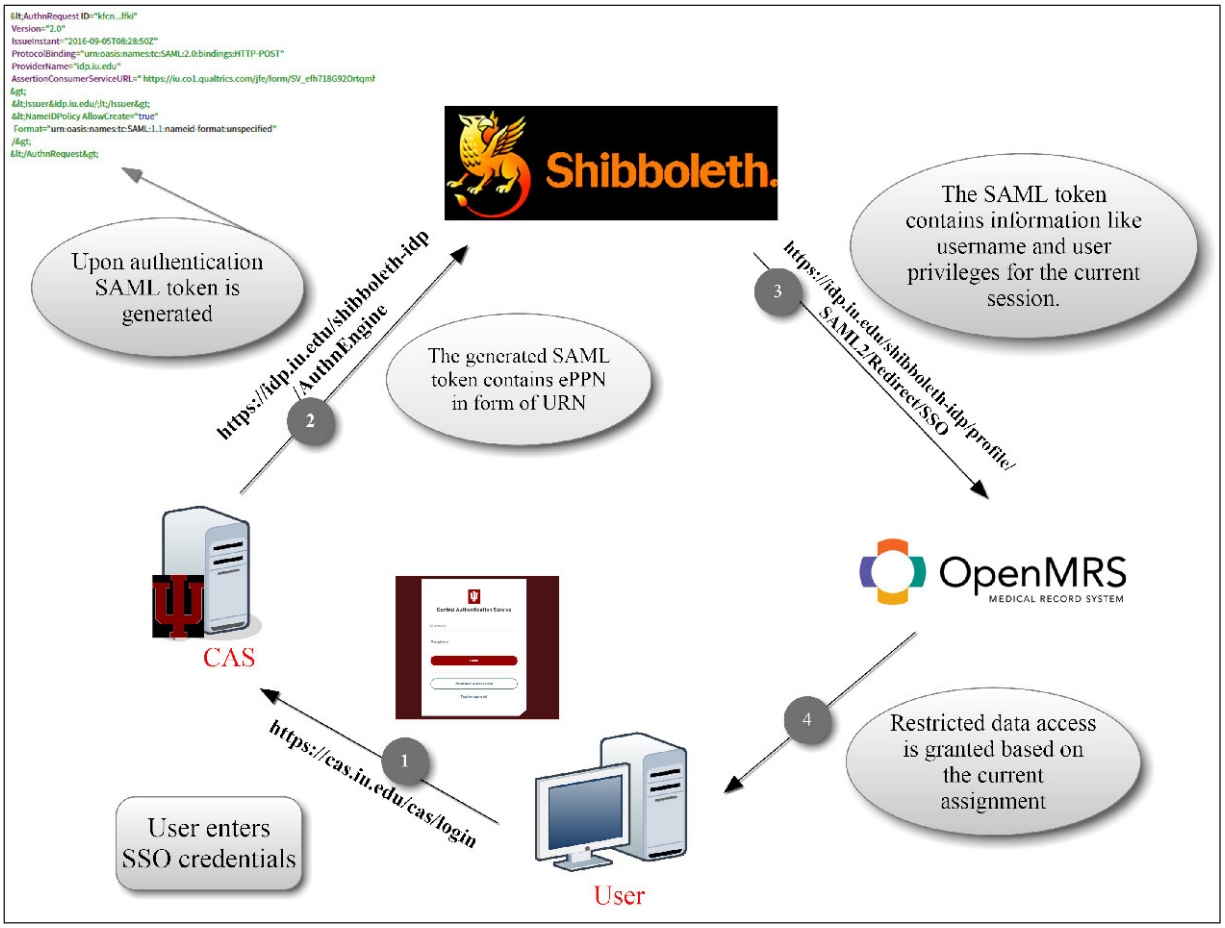

Fig. 2 CAS used with Shibboleth at Department of BioHealth Informatics

References

1. Meaningful Use Regulations | Policy Researchers & Implementers | HealthIT.gov [Internet]. [cited 2016 Dec 20]. Available from: https://www.healthit.gov/policy-researchers-implementers/meaningful-use-regulations
2. Niazkhani Z, Pirnejad H, Berg M, Aarts J. The impact of computerized provider order entry systems on inpatient clinical workflow: a literature review. J Am Med Inform Assoc JAMIA 2009; 16(4): 539–549.
3. Mazlan EM, Bath PA. Impact of health informatics implementation on clinical workflow: A review. In: Proceedings of the World Congress on Engineering and Computer Science. 2012.
4. Zheng K, Haftel HM, Hirschl RB, O'Reilly M, Hanauer DA. Quantifying the impact of health IT implementations on clinical workflow: a new methodological perspective. J Am Med Inform Assoc JAMIA 2010; 17(4): 454–461.
5. Jha AK, DesRoches CM, Campbell EG, Donelan K, Rao SR, Ferris TG, Shields A, Rosenbaum S, Blumenthal D. Use of Electronic Health Records in U.S. Hospitals. N Engl J Med 2009; 360(16): 1628–1638.
6. D'Costa-Alphonso M-M, Lane M. The Adoption of Single Sign-On and Multifactor Authentication in Organisations - A Critical Evaluation Using TOE Framework. Issues Informing Sci Inf Technol 2010; 7: 161.
7. Furnell S. Authenticating ourselves: will we ever escape the password? Netw Secur 2005; 2005(3): 8–13.
8. Borycki E, Kushniruk A, Armstrong B, Joe R, Otto T. Integrating Electronic Health Records Into Health Professional and Health Informatics Education: A Continuum of Approaches. Acta Inform Medica 2010; 18(1): 20.
9. Koppel R, Smith S, Blythe J, Kothari V. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? Stud Health Technol Inform 2015; 208: 215–220.
10. HL7 Standards Product Brief – HL7 Context Management Specification (CCOW), Version 1.6. [cited 2016 Dec 20]. Available from: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=1
11. Oreku GS, Li J. End User Authentication (EUA) Model and Password for Security. J Organ End User Comput 2009; 21(2): 28–43.
12. Mykkänen J, Porrasmaa J, Rannanheimo J, Korpela M. A process for specifying integration for multi-tier applications in healthcare. Int J Med Inf 2003; 70(2–3): 173–182.
13. Maliki TE, Seigneur JM. A Survey of User-centric Identity Management Technologies. In: The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007). 2007. p. 12–7.
14. Sun S-T, Beznosov K. The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems. In ACM; 2012. p. 378–390.
15. Halling TD, Douglas C. Hahn. Bringing interlibrary loan services under a single sign on umbrella. Libr Hi Tech 2013; 31(1): 76–86.
16. Birk P, Chao C-Y, Chung H, Mason C, Reddy K, Venkataramappa V, Riddlemoser D. System and method for secure network state management and single sign-on. US20050154887 A1, 2005 [cited 2016 Oct 14]. Available from: http://www.google.com/patents/US20050154887
17. Dhamija R, Dusseault L. The seven flaws of identity management: Usability and security challenges. IEEE Secur Priv 2008; 6(2): 24–29.
18. Hardt D. The OAuth 2.0 authorization framework. 2012 [cited 2016 Dec 20]; Available from: http://tools.ietf.org/html/rfc6749%3E
19. Recordon D, Reed D. OpenID 2.0: A Platform for User-centric Identity Management. In: Proceedings of the Second ACM Workshop on Digital Identity Management. New York, NY, USA: ACM; 2006 [cited 2016 Dec 20]. p. 11–16. (DIM '06). Available from: http://doi.acm.org/10.1145/1179529.1179532
20. Chinitz J. Single sign-on: Is it really possible? Inf Syst Secur 2000; 9(3): 1–14.
21. Manadhata PK, Wing JM. An Attack Surface Metric. IEEE Trans Softw Eng 2011; 37(3): 371–386.
22. OpenMRS Releases 2015 Annual Report | OpenMRS. [cited 2016 Aug 18]. Available from: http://openmrs.org/2016/02/openmrs-releases-2015-annual-report/
23. A Business Case for Single Sign On. Healthcare IT News. 2011 [cited 2016 Dec 20]. Available from: http://www.healthcareitnews.com/blog/business-case-single-sign
24. Sun S-T, Pospisil E, Muslukhov I, Dindar N, Hawkey K, Beznosov K. Investigating Users' Perspectives of Web Single Sign-On: Conceptual Gaps and Acceptance Model. ACM Trans Internet Technol 2013; 13(1): 2:1–2:35.
25. Li Z, He W, Akhawe D, Song D. The emperor's new password manager: Security analysis of web-based password managers. In: 23rd USENIX Security Symposium (USENIX Security 14). 2014. p. 465–479.
26. Hope P, Zhang X. Examining user satisfaction with single sign-on and computer application roaming within emergency departments. Health Informatics J 2015; 21(2): 107–119.