Patient-Centric Secure-and-Privacy-Preserving Service-Oriented Architecture for Health Information Integration and Exchange

Mahmoud Awad and Larry Kerschberg,

Center for Health Information Technology, George Mason University, http://hit.gmu.edu

Abstract. In this paper, we propose a secure and privacy-preserving Service Oriented Architecture (SOA) for health information integration and exchange in which patients are "part owners" of their medical records, have complete ownership of their integrated health information and decide when and how data is modified or exchanged between healthcare providers or insurance companies. This architecture is different from integrated Personal Health Record (PHR) such as Google Health and Microsoft HealthVault in that electronic health records are not stored in online databases but instead are aggregated on-demand using web service requests. Web service providers working on behalf of the patients do not keep copies of the complete EHR but instead provide a pass-through service, and would require PKI-based security certificates to initiate health information exchange.

Keywords: Privacy Ontology, Electronic Health Record, Service Oriented Architecture, Health Information Exchange, HER, SOA, HIE.

1 Introduction

Patient health records (in electronic or paper form) such as medications, lab results and family history are owned by the healthcare establishment that requested or created such records. Even though patients can request copies of their medical records, the process of getting such records is neither streamlined nor convenient. Photocopies of large medical files are costly and in most cases unreadable, and, in the case of electronic systems, these records are usually in proprietary format that are hard to integrate with each other. As more healthcare providers switch to Electronic Health Records (EHR), most of these issues will be overcome but the security, privacy and ownership of these medical records remain hard-pressed issues.

The Health Insurance Portability and Accountability Act (HIPAA), which was enacted in 1996, includes provisions that govern certain privacy aspects related to patients health records. These provisions apply to healthcare providers such as hospitals, physicians and laboratories, but do not apply to companies that aggregate these health records in electronic format such as Google Health, Microsoft HealthVault and Indivo. Most people consider the state of their health to be very

confidential and, therefore, security and privacy concerns may drive people away from such integrated systems in spite of all the strict online privacy policies established by Google and Microsoft. People would rather deal with a healthcare entity that is covered under an enforceable federal law than deal with unenforceable privacy policies established by corporations that have objectives that overshadow and eclipse the confidentiality of an individual's lab results or family medical history.

In this paper, we propose a secure and privacy-preserving Service Oriented Architecture (SOA) for health information integration and exchange. The proposed architecture is different from integrated EHR systems such as Google Health and Microsoft HealtVault in that electronic health records are not stored in online databases but instead are aggregated on demand using web service requests. All health information exchanges have to be approved by the patient and would require one-time use secure tokens for authentication, privacy policies to control data elements exchanged and fine-grained security policies to control data element values exchanged. As a proof of concept, we developed a prototype showing how privacy and security policies are created and how they are applied as part of an EHR exchange.

2 Proposed Architecture

In our proposed architecture, shown in Figure 1, the patient is represented by an application server that communicates with healthcare providers using a set of web services. This application server contains a set of privacy policies and security policies that govern all data exchange requests, and does not have the capability to store the patient's complete health record.

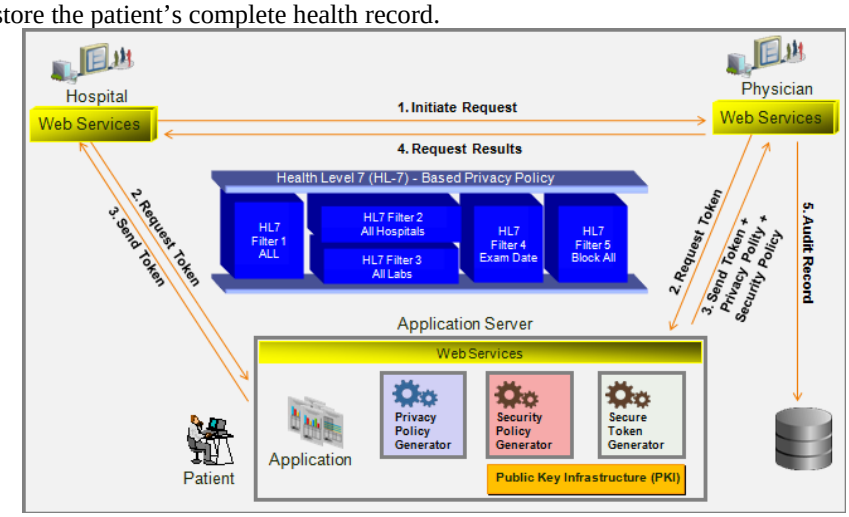

Fig. 1. Patient-Centric Secure System Architecture.

The server representing the patient consists of the following components:

1. Database contains fine-grained historical audit trail of all data exchange requests among healthcare providers, which includes additions, modifications and deletions of health record structure or data. The patient's medical history can be reconstructed using this audit trail but only the patient has privileges to initiate such request.

2. Privacy Policy Generator (PPG) generates privacy policies by defining which data structure elements are allowed to be exchanged between healthcare entities. The policy itself is represented using HL7 CDA syntax and acts as a filter between a web service and its data store. Privacy policies can be generated manually or via templates such as Continuity of Care Record (CCR) which is an HL7 constraint.

3. Security Policy Generator (SPG) generates security policies that restrict records retrieved by a database in response to an EHR query. These security policies enforce fine-grained access and are modeled similar to relational database fine-grained security access control. In order to generate new security policies or modify existing policies, the SPG receives a request from the PPG with a privacy policy identifier, a healthcare provider identifier and the data elements that need to be secured by the new security policy.

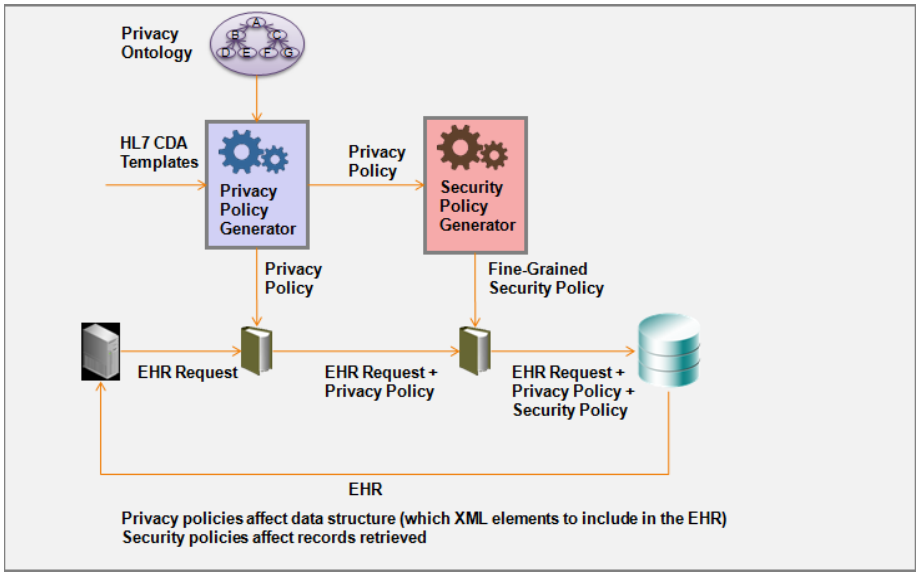

Fig. 2. Privacy and Security Policy Generators.

The architecture offers a clear separation between privacy policies and security policies in order to provide better flexibility in producing and applying the filters and

predicates produced by the PPG and SPG respectively. Privacy filters are applied first to restrict data elements in an XML response (or columns in case of relational tables), then security policies are applied to limit the data element values. Implementation details depend on the architecture of the medical record system implemented internally at the healthcare providers or health insurance companies. Systems that use relational database can use fine-grained access control to implement security policies and systems that use XML databases can use XML schemas to validate the XML document produced.

1. Secure Token Generator (STG), Requests for EHR exchange are initiated but not executed until secure tokens are generated by the STG. The tokens are generated using PKI and use a random number to ensure they are used only once.

2. Privacy Ontology; helps the PPG determine relationships among healthcare providers and between EHR data elements and provides a mapping between the healthcare providers and EHR data elements. Default privacy policy templates are generated using this privacy ontology. An example of relationships between healthcare providers is all the hospitals and medical practices that use Quest Diagnostics as their diagnostic laboratory testing facility. This knowledge simplifies the process of generating security policies that would allow lab results to be exchanged between these medical facilities and Quest Diagnostics. Also, knowing that the patient's primary family physician is a registered practitioner at particular hospital helps establish the level of trust in data exchanges between the physician and various offices within the hospital.

3. Applications are used to: a) Monitor data exchange requests and help the users decide whether to approve or reject a request; b) Produce privacy policies and security policies; c) Query an individual component of the EHR or produce a complete EHR by issuing EHR integration web service requests to all the registered healthcare providers; and d) Review and correct individual components of the EHR by issuing correction requests to the system holding the affected record.

ThePrivacy Ontology is an important component of our architecture and a subject of active research. We are motivated by the HL7 Security and Privacy Ontology (See: http://wiki.hl7.org/index.php?title=Security_and_Privacy_Ontology). The ontology was developed using their methology and use cases dealing with access control based on category of action, of object, of structural role, of functional role, and on multiple role values. Additional use cases deal with facilitating an automatic decision function and the design of an access control system.

The HL7 Security and Privacy Ontology is specified in the Web Ontology Language (OWL) and is implemented in the Protege Ontology Editor from Stanford University. We are presently investigating how to incorporate patient-centric privacy and security authorization constructs into the Privacy Ontology so as to strike a balance between patient privacy, the secure exchange of health information, and mechanisms to ensure the chain-of-custody of electronic health records.

3 Application Prototype

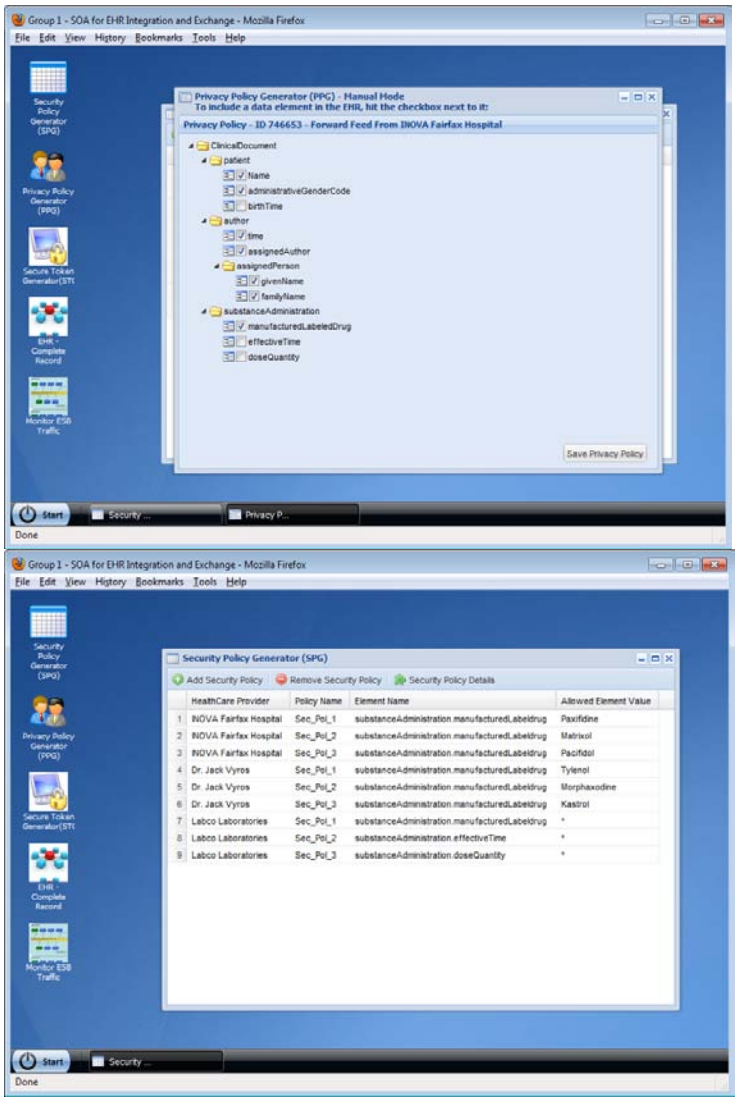

Fig. 3. Application Prototype.

4 Discussion

Any comprehensive solution for EHR integration and exchange has to be technologically feasible but also politically acceptable. Healthcare providers will

always claim ownership of all medical records in their possession, and as long they are HIPAA-compliant, we have to assume that they have developed adequate internal security and privacy policies to protect these medical records. Our proposed solution only requires a web services layer around existing systems while giving patients an active role in the EHR exchange instead of the current practice of providing their healthcare providers with a blank authorization to exchange their EHR with anybody. Also, fully centralized EHR integration solutions are prone to privacy and security lapses and disruptive hacker attacks such as Denial Of Service (DOS). Fully distributed solutions, on the other hand, are prone to data loss if they do not offer proper data redundancy and backup strategies. Our proposed solution maintains the existing distributed network of systems represented by the healthcare providers but offers a secure method for data integration on demand.

5 Conclusion

In this paper, we propose a secure and privacy-preserving SOA for health information integration and exchange in which patients are "part owners" of their medical records, have complete ownership of their integrated health information and decide when and how data is modified or exchanged between healthcare providers or insurance companies. This architecture is different from integrated Electronic Health Record (EHR) such as Google Health and Microsoft HealtVault in that electronic health records are not stored in online databases but instead are aggregated on demand using web service requests. Web service providers working on behalf of the patients do not keep copies of the complete EHR but instead provide a pass-through service, and would require PKI-based security certificates to initiate health information exchange.

References

1. Vagelis Hristidis, Peter J. Clarke, Nagarajan Prabakar, Yi Deng, Jeffrey A. White, Redmond P. Burke: A Flexible Approach For Electronic Medical Records Exchange. In: Proceedings of the international workshop on Healthcare information and knowledge management, Conference on Information and Knowledge Management, Arlington, Virginia, USA, Pages: 33 – 40. (2006)
2. Au, R.; Croll, P.: Consumer-Centric And Privacy-Preserving Identity Management For Distributed E-Health Systems. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences, vol., no., pp.234-234, 7-10. (2008)
3. Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu: Hippocratic Databases. In: Proceedings of the 28th international conference on Very Large Data Bases, Hong Kong, China, Pages: 143 – 154.(2002)
4. Deepthi Rajeev, Catherine J Staes, R Scott Evans, Susan Mottice, Robert Rolfs, Matthew H Samore, Jon Whitney, Richard Kurzban, Stanley M Huff, 2010. Development Of An Electronic Public Health Case Report Using HL7 V2.5 To Meet Public Health Needs. In: The Journal of the American Medical Informatics Association, JAMIA; 17:34-41.

5. Song Han, Geoff Skinner, Vidyasagar Potdar, Elizabeth Chang: A Framework Of Authentication And Authorization For E-Health Services. In: Proceedings of the 3rd ACM workshop on Secure web services. (2006)
6. Janos L. Mathe, Sean Duncavage, Jan Werner, Bradley A. Malin, Akos Ledeczi, Janos Sztipanovits: Towards The Security And Privacy Analysis Of Patient Portals. ACM SIGBED Review, Volume 4 , Issue 2, Pages: 5 – 9. (2007)
7. Jing Jin, Gail-Joon Ahn, Hongxin Hu, Michael J. Covington, Xinwen Zhang: Patient-Centric Authorization Framework For Sharing Electronic Health Records. In Proceedings of the 14th ACM symposium on Access control models and technologies, Pages: 125-134. (2009)
8. Daglish, D.; Archer, N.: Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues. In: World Congress on Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS '09, vol., no., pp.110-120, 25-27. (2009)
9. Sloane, Elliot; Leroy, Gondy; And Sheetz, Steven: An Integrated Social Actor and Service Oriented Architecture (SOA) Approach for Improved Electronic Health Record (EHR) Privacy and Confidentiality in the US National Healthcare Information Network (NHIN). In Americas Conference on Information Systems (AMCIS), AMCIS 2007 Proceedings. Paper 366. (2007)
10. Ajit Appari And M. Eric Johnson: Information Security and Privacy in Healthcare: Current State of Research. In: International Journal of Internet and Enterprise Management. (2009)
11. Vicky Liu, Lauren May, William Caelli, Peter Croll: Strengthening Legal Compliance For Privacy In Electronic Health Information Systems: A Review And Analysis. In: Electronic Journal of Health Informatics, Vol 3(1): e3. (2008)
12. Taylor, K.L.; O'keefe, C.M.; Colton, J.; Baxter, R.; Sparks, R.; Srinivasan, U.; Cameron, M.A.; Lefort, L.: A Service Oriented Architecture For A Health Research Data Network. In: Proceedings. 16th International Conference on Scientific and Statistical Database Management, vol., no., pp. 443- 444, 21-23. (2004)