Security of Electronic Health Records based on Web Services

Jaminda S. Wimalasiri, Pradeep Ray, and Concepción S. Wilson
School of Information Systems, Technology and Management,
University of New South Wales, Sydney, NSW2052, Australia

Abstract – The current healthcare environment has embraced Electronic Health Records (EHRs) as evidenced by the numerous standards both formal and proprietary that have arisen. However, the issues of security and privacy in this new landscape has not been adequately addressed. Legislation has attempted to ameliorate the situation by mandating a minimum level of protection for the healthcare consumer. However, the leading standards lack technical specificity that would ensure security and privacy in a modern distributed system of EHRs. The research presented in this paper presents a means to address some of these issues by using a service orientated architecture.

I. INTRODUCTION

In our previous paper [1] we argued the need for an architecture that would allow the seamless integration of these disparate medical records without restricting healthcare providers to a particular standard or format. We adopted the use of an 'Ontology driven Multi-Agent System' to recognize and align data items from various EHRs of differing standards and formats, creating an integrated and unified view of a patient's medical history. We did not address the security and privacy implications that are inherent in such a system. The sensitivity of PHI and the associated need for security and privacy of EHRs is well established and all of the standards with respect of EHRs have acknowledged and attempted to meet this requirement. However, as with providing a uniform standard for EHRs, the issues in providing a uniform standard for security and privacy, in terms of both implementation and policy, are non-trivial. Interaction between healthcare institutions will still need to be preceded by a contractual agreement (chain of trust agreement). This would limit the utopian vision of a healthcare landscape where applications can share data across organizational boundaries on an ad hoc basis yet still maintaining the security and privacy of the data transmitted. And finally, we addressed the fact that most breaches of security occur within an organization.

The problem of security and privacy is a huge multi-faceted area. This paper does not attempt to address every possible scenario that would result in a security incident. Rather, we address the specific issues of privacy. As demonstrated in [3], privacy is a huge area of concern, with over 75% of people concerned or very concerned about sharing their PHI. While EHRs may inevitably replace traditional paper notes, concerns about information security need to be addressed convincingly before national rollouts can occur [France et al., 1994]. Specifically, we look at the gap that exists in one of the most widely recognised security standards, the HIPAA final security rule [HHS] and demonstrate an effective conformance to the rule.

II. ELECTRONIC HEALTH RECORD SECURITY ISSUES

A. Security Incidents

Security incidents reported to CERT/CC Statistics [2] in 2003 were 137 529, a 67% increase in the number of incidents from the previous year. Security posture assessments of the healthcare industry show the highest percentage of Internet vulnerabilities, an average of 61.07 percent compared to an average of 27.37 percent across other industries [4]. The following examples show the types of incidents that can occur;

- Hacker infiltrated University of Washington gaining access to confidential patient data [5]
- Health Net mailed a list of patient's names being treated for depression to nearly 5,000 physicians due to a programming error.
- Kaise Permanente online application revealed information of one customer to another customer. [6]
- Cancer patient records was found on a memory stick that was sold by a staff member. [7].

These examples demonstrate the diversity of possible security incidents and enforces a well known fact that no information system can be 100 percent safe. It is not a matter of solely preventing security incidents but providing controls that will ameliorate the exposure of sensitive information due to an incident, be it malicious or unintentional.

B. Electronic Health Record legislation and standards

Health Insurance Portability and Accountability Act of 1996 proposes a set of standards to regulate the electronic interchange of health information and to protect the confidentiality and security of electronic health information that a not specific to a particular technology. Other standards such as HL7 [8] have adopted a more technical stance describing specific implementation details of the security services that should be enforced. HIPAA's restricted of specifications inhibit systems interoperability and increase the tendency toward the adoption of multiple divergent standards without any substantive benefit to security. HL7 reliance on standards would mean that security would be more consistent and therefore arguably more reliable. However, problems that plague standards still exist, such as how do we manage changing requirements and changing technologies?

Furthermore, the security requirements (and therefore the implementation of security services) of one healthcare provider may not translate well to another healthcare provider.

0-7803-8940-9/05/$20.00 ©2005 IEEE.

A final point of interest is with regards to the HIPAA final security rule. Section 164.314 states that with regards to a contract between a healthcare provider and a business associate, it is the responsibility of the healthcare provider to ensure that the transmission of PHI to the aforementioned business associate is not at risk. That is, the business associate must have a similar or higher level of security. This is particular pertinent point when we discuss the issues relating to autonomous sharing of PHI and the ad-hoc creation of business relationships.

C. EHR Requirements

While standards such as HL7 seek to secure the transmission of data [8], the end to end security requirements are more complex. The sensitivity surrounding personal medical data further compounds the problem [9]. Healthcare users may be discriminated or socially ostracized by the accidental or malicious exposure of sensitive information. [10]. It is important to remember that unlike paper based models where an exposure or intrusion is confined to a single document or file, the distributed EHR model creates the possibility of a patient's entire medical history being compromised.

As pointed out in [11], it can be assumed that while, healthcare providers have their patient's best interests in mind; they are not in best position to ensure the security of EHRs. A successful implementation of a distributed EHR framework should not require the users to have to make overtly complex decisions with regard to the security of the document they are using. Conversely, the framework should provide the healthcare providers the flexibility to arbitrarily define the security of a particular document if so required. Healthcare consumers should also be able to make their own decisions about the security and privacy of particular elements of their PHI. Finally, it is important that in meeting these security and privacy requirements, legitimate use of EHRs are not hindered. Mechanisms should be in place to allow access to the EHR in emergency situations and by relevant authorities.

The section illustrates the breadth of the problem faced when trying to maintain adequate security and privacy. Maintaining the security and privacy of EHRs are compounded by the need to maintain functionality. It would be pointless if we applied strong encryption to the entire EHR or to messages passed between healthcare providers if it did not accommodate the processes existing in the healthcare system. Nor would a security process work if it was not conducive to use by healthcare providers.

Another requirement relates to the HIPAA rule regarding the trust placed in business contacts. If a healthcare provider is to share PHI with another entity, it bears the responsibility of ensuring that the security or privacy of the data transmitted will not be jeopardized during transit or by the third party entity. The trust, at this stage, must be established through a face to face negotiation process. Ideally, we would like to have an EHR that is completely portable. A healthcare consumer should be able to use the services of any healthcare provider irrespective of prior arrangements between healthcare institutions. In order to allow this ad-hoc creation of business relationships, the infrastructure needs to be able to verify the authenticity of a healthcare provider as well as provide a determination of his or her access rights.

D. Our Position

The above sections present aspects of the healthcare landscape that seeds the motivation for our research. The security incidents demonstrate how, despite sometimes perceived adequate security measures, the privacy and security of health records must always be considered to be at risk. This is particularly important when we consider that HIPAA mandates that the originator of the EHR is responsible of their security and privacy when they are provided to third party healthcare providers. However, we cannot ignore the vast potential benefit of sharing EHRs and standardization efforts have not yet offered a comprehensive solution. The proposal we present in the paper is a prototype infrastructure that will mitigate these security risks yet allow seamless transactions involving EHRs between healthcare organizations. Through the use of a service-orientated architecture that incorporates layered encryption and security tags we can provide the best possible privacy protection for healthcare consumers. We propose that healthcare providers expose web services that facilitate secured access to their EHRs. Through the use of security tags and an encryption infrastructure we can ensure that only individuals with appropriate access rights can access sensitive portions of EHRs. The main contribution of this paper is to present how a service-orientated architecture can be deployed to affectively address the privacy concerns of healthcare consumers.

III. SERVICE ORIENTATED ARCHITECTURE AND WEB SERVICES

A. Why Service Orientated Architecture?

A service orientated architecture (SOA), simply put, involves breaking down an application such as an enterprise Electronic Health Record application into individual business functions such as obtain the EHR of this particular patient [12]. The benefits of SOA are widely recognized and are the basis for web services. These benefits are particular advantageous to the healthcare industry.

- SOAs allow organizations to *respond* to changing business conditions in a fast and flexible manner given the ease of which services can be redefined and reused. Healthcare is faced with constant change, beyond any other industry, causing it to flux in and out of a hyper-turbulent state. [13] The SOA will, for instance, allow the healthcare providers to adapt to the changing security and privacy requirements as new issues and legislations present evolve.
    - SOAs are particular effective at *sharing* data, information and knowledge. The use of open

standards and protocols support effective communication between organizations. The problems of incompatible system architectures are not a problem.

- Finally, SOAs support numerous security features and identity management frameworks. Policy based management of security and privacy ensure data is protected against access from unauthorized parties.
- There are, of course, numerous other advantages of SOAs but those listed above are particularly relevant to the healthcare landscape and pertinent to this discussion.

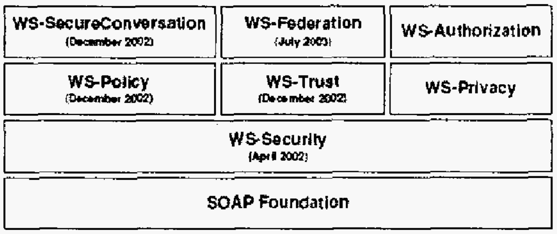
B. *Web Services Security*

Web services are now the preferred way to link applications both within and without an organization in a loosely-coupled, language neutral and platform independent way as touted by World Wide Web Consortium. Web services use a Service Orientated Architecture as described in the previous sections. Furthermore, the technologies and their inherent security features provide additional support for its use within a healthcare architecture.

A key technology that is used in all aspect of web services from service description to delivery is XML. The World Wide Consortium has issued three XML-based standards for security;

1. XML Key Management Services – digital signatures are used to authenticate a message's source.
2. XML Encryption – this protects the privacy of the message
3. XML Key Management Services – public key registration and validation.

In April 2002, IBM and Microsoft published a joint security whitepaper that details a security architecture within the web services environment. The model was built on these XML standards and the specifications as shown in the figure below.



WS-SecureConversation (December 2002)
WS-Federation (July 2003)
WS-Authorization
WS-Policy (December 2002)
WS-Trust (December 2002)
WS-Privacy
WS-Security (April 2002)
SOAP Foundation

Fig. 1 Web Services Security Specifications

These specifications are the basis for implementing a secure SOA using web services. The healthcare industry, however, presents unique security and privacy challenges. Meeting these challenges requires us to extend the functionality of these specifications to meet the requirements of the industry. We begin the next section by providing an example of an encounter typical in a healthcare scenario. This encounter forms the basis of our subsequent discussion.

IV. A HEALTHCARE SCENARIO

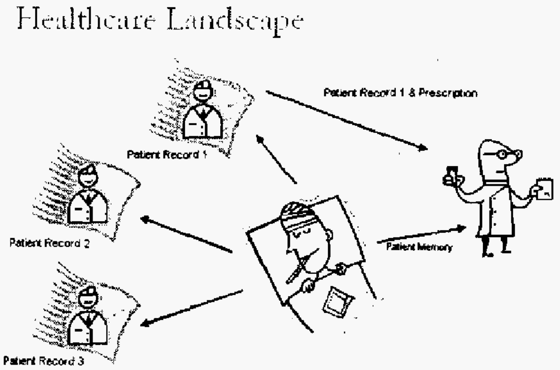


Fig. 2 Healthcare scenario

The figure above presents a typical healthcare scenario. A patient routinely visits multiple healthcare providers, depending on the particular healthcare needs. Each healthcare provider, therefore, has a unique view of the patient's healthcare status. Ideally, each healthcare provider would like to have an integrated view of the patient's healthcare status based on an aggregation of all the patient records. This involves a healthcare provider requesting from another healthcare provider his version of the patient's EHR. However, each doctor has a responsibility to protect his patients' interest in terms of the privacy of their EHR. For instance, a patient may have an embarrassing illness that he does not want to share between healthcare providers. Furthermore, the doctor has to ensure that the security provided by the requesting healthcare provider is at least as secure as his own institution. And finally, the doctor has to ensure that the requesting healthcare provider has the authority to access the information.

A. *Security Information exchange*

HIPAA specifies the need for a "Chain of Trust Partner Agreement", which is a contract entered into by two entities in which they agree to electronically exchange data and to protect the integrity and confidentiality of the data. The ultimate goal is to maintain the same level of security at each link in the chain. [14] We feel that this sort of requirement is applicable to any healthcare network where there is a potential for PHI to cross organization boundaries. At this stage, this agreement cannot be made automatically. However, if we aim to achieve completely transparent and seamless sharing of PHI amongst distributed healthcare entities, we require the ability for applications to exchange security information as well. This information will need to contain both organizational specific security details like access control lists and security policy as well as information regarding encryption standards such as PKI.

Our implementation uses the WS-Policy specification to implement a validation process to ensure that the web service only allows transactions from healthcare providers with a WS-Policy that support similar security standards. The WS-Policy store details such encryption standards, certification authorities and attributes authorities as well as Access Control List. These details are also used to validate and authenticate the healthcare provider.

B. XML based EHR Security

The transmitted EHR document is in the form of an XML document. During the security negotiation process or during the creation of a particular data segment of the EHR, a segment of the EHR might be considered particularly sensitive. Given that the security policies of foreign healthcare providers are not always trusted and/or the information of a patient may be particularly sensitive (e.g. a celebrity's medical record); the local healthcare institution may prefer additional security measures such as encryption. The architecture proposed in [1] utilizes XML encoding during the transmission of EHRs to remote CCS via the agent infrastructure. Within a SOA, we find, similarly, that EHR are transmitted as XML documents. These security protocols provide an additional level of security for the architecture. Only certain elements within the EHR can be encrypted using one of the security standards. For example an entire EOC and billing details may be encrypted leaving the rest of the EHR readable. These encrypted elements can only be accessed by the party with the appropriate key or access rights. The benefit of using this type of encryption is that the semantic information of the EHR is not lost. Other healthcare providers that provide intermediate services such as nurses or technical staff can still access, manipulate and forward the data to the relevant physicians without comprising the privacy of the patient.

C. Security Rating

The XML documents transmitted between web services can adopt any EHR standard, such as HL7 Clinical Document Architecture or openEHR. The XML tags as specified by these architectures provide semantic information to the EHRs. This semantic information allows the system to distinguish between entries that are related to a particular episode of care (EOC) from, say, the patient's family history. This paper suggests the use of a security tag, similar to the current Encrypted Data Tag of XML, to attribute segments of information with security information. That is, elements of the EHR could be rated based on sensitivity. For example, an EOC regarding an embarrassing illness such as an STD would be tagged with a high security rating. In our prototype, the web service compares the security rating with web services security policy document described above to make a determination of whether the information should be released. We proposed that a simple architecture utilizes a numerical rating for representing security access roles. These numerical ratings can be mapped onto roles based on the ACL on the healthcare provider's infrastructure. Provided, there is sufficient trust in the foreign healthcare providers' authentication policy, only the relevant staff should be able to access the relevant information. This is an inherently scalable approach to securing the EHR without inadvertent restricting authorized healthcare entities.

For instance, if a patient expresses his/her wishes for privacy and the doctor then specifies that the details of this particular episode of care are of a higher security setting. All other information in the patient record, including information regarding the patient's prescription is still accessible as these security values have not been changed. As such, a pharmacist filling out the prescription using the remote EHR can fill the prescription without having access to the details of the patient visit. His clinical software would recognize the security rating and attempt to remove such information from the immediate view. Physicians that particularly need to view this information we still be able to. This prevents the accidental disclosure of sensitive information. For example, an unrelated physician browsing through the record would not accidental come across this information. Of course, this requires a lot of trust, especially if the EHR is shared with an unrelated healthcare provider. Furthermore, security rating should be tied to access control list. However, because role based access is not clearly defined in the HIPAA for instance, and more likely than not, not properly enforced, access to this private information may not be defined within an organization.

D. Layered Encryption

Unfortunately, relying solely on security tags implies trusting the organizational policies and applications of the receiving healthcare institution. We have no way of ensuring that the security tags are respected or if the organizational structure means that the nurses have the same access as doctors, for instance. Furthermore, security tags do not provide protection against malicious incidents. The use of encryption provides a second layer of protection. While encryption itself is widely used, we deploy encryption in a manner that makes it more suitable for the healthcare environment. Conventionally, we would expect the entire document to be encrypted. Only healthcare entities with access to relevant decryption keys would be able to see *any* information contained with the EHR. This would present an unnecessary burden on the system. Even healthcare entities with the right privileges would have to go through the process of acquiring the keys and decrypting the information. The administrative issue would be problematic, even potentially dangerous especially in emergency situations when the PHI within an EHR is urgently required. While encrypting the entire EHR makes it inherently safe, any healthcare provider with the key would be able to see the entire record. In this situation, this would be contrary to the patient's wishes. She only wanted to restrict a portion of the EHR. We propose linking encryption to the security tags. As such we only encrypt parts of the EHR and the encryption is depended on the security tag value and the WS-Policy document.

For this example, we will be using the prototype demonstrated in [1] but is equally applicable to any technology such as web services. After exchanging security information including access control lists, the system identifies the site as one that does not have comparable security infrastructure as the source of the EHR. The system then encrypts portions of the EHR or denies access to portions of the EHR. If the remote station particularly requests a portion of the EHR that is rated as sensitive, a chain of trust agreement can be established manually. In that scenario, the remote healthcare entity would already possess a copy of the encrypted EHR. The entity would only need to verify his identity to the certificate holding body (either third party or the source of the EHR) to obtain the relevant key. This key could be passed through any other secure means. This manual step is required especially when the agents deal with unknown healthcare entities. However, when EHRs are passed within large healthcare institutions, some portions of the EHR still need to be encrypted. This prevents access by other individuals such as nurses. However, since the parties are trusted, we would like to avoid the manual process of acquiring keys. This stage is completed during the exchange of security information. In our prototype, this information is stored by the agents and the agent platform. As such, only the physician's application can decrypted the encrypted information. Other personnel may still be able to access other aspects of the EHR (based on the organization policy of the institution) but the secure details can only be read on a workstation that contains the relevant keys.

V. CONCLUSIONS

Legislation such as HIPAA's security rule will dramatically increase the focus on security and privacy issues of EHRs. The approach presented in this paper is an architecture that addresses some of the specific security and privacy requirements using a SOA. A key concept is establishing trust between healthcare providers. Using WS-Policies together with certification and authentication, a level of trust can be established. However, once trust levels are established, we still need a means to control the flow of information and protect the information once it is has been released. Through the use of layered encryption and security tags, we can mitigate some of the risks such as accidental exposure.

REFERENCES

[1] J. S. Wimalasiri, P. Ray, C. S. Wilson, "Maintaining Security in an Ontology Driven Multi-Agent System for Electronic Health Records", Provceedings of the IEEE Healthcom2004, Odawara, Japan, June 2004

[2] Carnegie Mellon University, CERT® and CERT Coordination Center®, "CERT/CC Statistics 198-2003", 2004 [Online] Available: http://www.cert.org/stats/#incidents

[3] Internet HealthCare Coalition (IHC) and California Health Care Foundation (CHCF), "Health Affairs Issue Examines e-Health", November 2000

[4] Cisco Systems Inc., 2002, "Network Security Solutions for Health Care, Making HIPAA SAFE" [Online] Available: http://www.cisco.com/warp/public/cc/so/neso/sqso/hipaa_wp.htm
F. H. R. France, P. N. Gaunt, "The need for security - a clinical view", Int J Biomed Comput 1994; 35 (Suppl 1): 189-194

[5] T. Chin, 2001, "Security breach: Hacker gets medical records", American Medical News, [Online] Available: http://www.ama-assn.org/amednews/2001/01/29/tesa0129.htm#top

[6] V. Colliver, 2004, "Software glitch reveals stranger's health history Kaiser applicant sees woman's information", San Francisco Chronicle, [Online] Available: www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/03/12/BUGND5J3PR1.DTL

[7] J. Leyden, 2003, "For sale: memory stick plus cancer patient records", The Register, [Online] Available: http://www.securityfocus.com/news/3129

[8] B. Bernd, 1999, "HL7 Security Services Framework", [Online] Available: www.hl7.org/library/committees/Secure/HL7basics3.rtf

[9] L. O. Gostin, J. Turek-Brezina, M. Powers, R. Kozloff, R. Faden, D. D. Steinauer, "Privacy and security of personal information in a new health care system", J Amer Med Assoc 1993; 270: 2487-2493.

[10] G. J. Annas, "Privacy rules for DNA databanks: protecting coded future diaries". Journal of American Medical Association 1993; 270: 2346-2350

[11] Health Canada, 2001, "Toward Electronic Health Records", [Online] Available: http://www.hc-sc.gc.ca/ohih-bsi/pubs/2001_ehr_dse/ehr_dse_e.html

[12] IBM, (2000) "Service Orientated Architecture and Web Services: Creating Flexible Enterprise for a Changing World", Ziff Davis Media Custom Publishing, 2000

[13] Blair, J.D., Payne, G.T. (2000), "*The Paradox Prescription: Leading the Medical Group of the Future*", Health Care Management Review, Vol. 25, No. 1, pp. 44-58

[14] L. Lisa, J. D. Dahm, T. Paul, E. Smith, 2000, "The Basics of HIPAA Business Partner and Chain of Trust Agreements", First National HIPAA Summit [Online] Available: http://www.ehcca.com/presentations/HIPAA/dahm-mon.pdf