Proceedings of the 28th IEEE
EMBS Annual International Conference
New York City, USA, Aug 30-Sept 3, 2006

The Need for Technical Solutions for Maintaining the Privacy of EHR

Pradeep Ray, Senior Member IEEE. and Jaminda Wimalasiri

***Abstract*—Electronic Health Records (EHR) /Electronic Patient Records (EPR)/ Electronic Medical Records (EMR) provide the basis for e-Health services. Since information in these records (containing patient healthcare information) need to be shared amongst multiple healthcare providers and healthcare professionals, privacy issues of EHR have been a major inhibitor in the implementation of EHR/EMR/EPR systems. This paper presents EHR privacy requirements in the context of two major e-Health frameworks, namely HealthLink in Australia and HIPAA in USA. The paper concludes with a discussion of some evolving web-based solutions.**

I. INTRODUCTION

THE Electronic Health Record (EHR) is the keystone of a medical information system. Acting as an electronic version of paper medical record or chart, the EHR has been touted for years [1] as an essential part of the multifaceted face of medicine in the information system era. While the benefits of adopting EHR have been detailed in numerous proposals for both healthcare organizations and national initiatives, privacy advocacy groups insist that the issues around privacy have not been addressed adequately at a technical or a business process level. This was reflected in a nationwide survey conducted in February 2005 by Harris Interactive of Rochester, N.Y. that found that 70 percent of people were somewhat or very concerned that personal medical information would be leaked because of weak data security [2]. This sentiment has no doubt been exacerbated by disclosures including; Christus St. Joseph Hospital, Houston Texas (16,000 records compromised by theft), University of Chicago Hospital (employee found selling patient data) and Wilcox Memorial Hospital, Kauai, Hawaii (130,000 records compromised by theft).

The sensitivity of Privacy of Health Information (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, the issues in providing a uniform standard for security and privacy of EHR, 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. It has been observed that most breaches of security occur within an organization [3].

This paper discusses privacy issues for EHR based on case studies in different parts of the world. The paper begins with a categorization of EHR privacy issues and then discusses some evolving solutions to the problem.

II. PRIVACY ISSUES IN EHR SYSTEMS

Based on our experience of privacy research in e-business, we may classify the privacy issues in the following seven categories, consent, transparency, control over the record, collection limitation, data security, accuracy and identifiers.

We now discuss these issues with respect to two case studies:

- HealthLink in Australia
- HIPAAA in USA

The first case study presented in this paper is the Health*elink* system that is a new initiative by NSW Health. (HealthLink) on distributed/networked EHRs. The aim of the system is to collect and store information during the various interactions between a healthcare consumer and their different healthcare providers. The information will be automatically maintained and will be available for display on-line as a single 'secure' electronic record. The system is currently undergoing two trials. The following people will be automatically included in these trials.

- People aged over 65 as at 23rd March 2006, living in the Hunter region
- People aged under 15 as at 25th May 2006, living in the Greater Western Sydney region.

The information collected in the Health*Link* system will include a summary of treatments you have received, results from blood tests or x-rays and discharge referrals. The trials have already received fair amount flak due to the decision of an opt-out system rather than an opt-in system. [3]. Table 1 presents a review of privacy descriptions in Healthlink based on the above seven categories.

The second case study presented in the article is on HIPAA. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a set of rules that standardize the communication of electronic health information between healthcare providers and health insurers. The rules are intended to protect the privacy and security of individually identifiable health information. To that end, the HIPAA Privacy Rule (Code of Federal Regulations, Title 45, part 164) specifies the requirements around how entities that our

Manuscript received March 30, 2006.

Pradeep Ray is with the School of Information Systems, Technology and Management, University of New South Wales, Australia (phone: +61 2 93855890; fax: +61 2 96624061; e-mail: p.ray@unsw.edu.au).

Jaminda Wimalasiri is a research student in the School of Information Systems, Technology and Management, University of New South Wales, Australia.

1-4244-0033-3/06/$20.00 ©2006 IEEE.

TABLE I
HEALTHLINK PRIVACY REVIEW

Issue	Description
Consent	- The ‘opt-out’ system implies personal information will be collected from everyone who meets the eligibility criteria. While users can opt-out, some demographic data is kept by the system. If the users do not opt-out within 30 days, medical information is kept from day 1 till the point the user opts out from the system.
Transparency	There are two dimensions to transparency. 1) Access to the EHR and 2) Disclosure of how the system works. The Healthe*Link* system provides access to the EHR via the internet. There is some concern that the older users will not be able to access their record due to the unfamiliarity with the medium. Secondly, the authentication requirements are not sufficiently robust. The Healthe*Link* trial, furthermore, rates poorly on transparency due to the lack of visible privacy policies and details on the personal information that will be stored.
Control over the record	This category refers to controlling the visibility of certain parts of the EHR. The HealtheLink system allows any participating healthcare provider to see to whole record. For example, a community health centre will be able to see pathology reports. Furthermore, any healthcare provider can see any patient’s record. They are not restricted to healthcare consumers that are actively being treated by them.
Collection limitation	This category refers to the ability to restrict particular pieces of information from being collected. Again, the user does not have any ability to select particular pieces of information from being collected.
Data Security	Given the fact that the access rights of any healthcare providers allow access to **any** EHR, this opens the system to large scale disclosures. Audit trails will be maintained but as there is no linkage between provider and consumer, privacy breeches cannot be detected automatically.
Accuracy	HealtheLink allows the user to access, verify the contents of the EHR and if necessary, modify the information contained.
Identifiers	Local level patient health identifiers are being used in HealtheLink trials to ensure a consumer's medical information is unambiguously linked to that person. There is no discussion on the ability to anonymize data.

governed by HIPAA may use and disclose collected and protect health information [5].

TABLE 2
HIPAA PRIVACY RULE REVIEW

Issue	Description
Consent	The Privacy Rule prohibits health care providers from disclosing health information of a consumer to health plan administrators without a patient’s explicit written authorization. This must include what data is being disclosed and the expiry data for this data. There are no technical requirements around this rule. Your consent is, however, not required for treatment, payment, or other health care operations. For example, in an emergency situation, healthcare provider would be able to access all facets of your medical record. Furthermore, no consent is required for the transmission of the EHR from one doctor’s office to another for the purposes of treatment.
Transparency	The rule mandates that a healthcare provider be able to request a full transcript of their EHR from their provider. However, without they may not be aware of the transmission of the record to other healthcare institutions.
Control over the record	HIPAA regulation mandated the individual’s right to request an amendment or correction to their healthcare record. This may not be technically feasible given that there is no control over the number of copies that may exist of a particular record.
Collection limitation	While there is a requirement for the organization to define the types of access to the EHR, there is no requirement for role based access control. As such, users are not able to restrict what parts of the EHR are visible to various healthcare providers. There is no ability to demarcate sections of the healthcare record as being sensitive or private.
Data Security	Surveys have indicated that a significant failing in HIPAA is the lack of training and education in HIPAA compliant organizations. The lack of a technical standard for privacy requirements implies the reliance on procedures and business processes. A lack of training and education imply an inherent data security risk. (AIHMA, 2005)
Identifiers	The final rule for the Employer Identifier, which became effective in July 2002, establishes a standard for a unique employer identifier.

Our analysis has shown significant gaps in the protection of health care information. While we realize an all encompassing solution to all the concerns around privacy and security are unlikely to be met, given the volatile nature of the technology and healthcare landscape, we believe that certain foundations can be set now that will allow the EHR to evolve to the changing requirements. These concepts have been touched on in our work [3], but did not articulate a strategy for mapping between the privacy requirements/concepts and these aforementioned foundations.

The following section details the main privacy issues that must be addressed and demonstrably viable solution to this problem.

III. EHR PRIVACY REQUIREMENTS

While standards such as HL7 seek to secure the transmission of data [6], the end-to-end security requirements are more complex. The sensitivity surrounding personal medical data further compounds the problem [7]. Healthcare users may be discriminated or socially ostracized by the accidental or malicious exposure of sensitive information. [8]. 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 [9], 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.

We illustrate the situation with a typical in a healthcare scenario in Fig. 1.

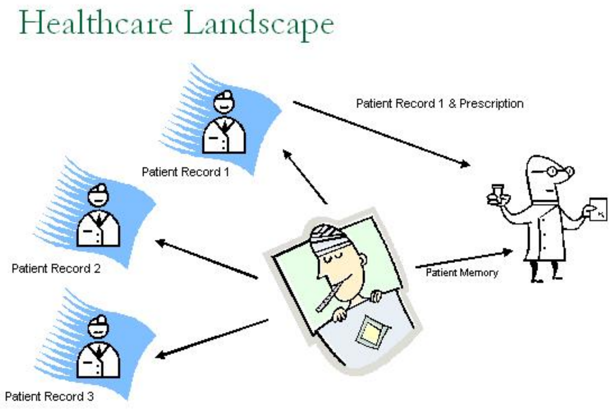


Fig. 1 Healthcare scenario

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.

The section has 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 were 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.

The next Section presents evolving technical solutions in two distinct cases:

1. Sharing of EHRs by multiple healthcare providers as required in many public healthcare systems
2. Web based health information systems driven by patients in the context of evolving consumer health paradigm.

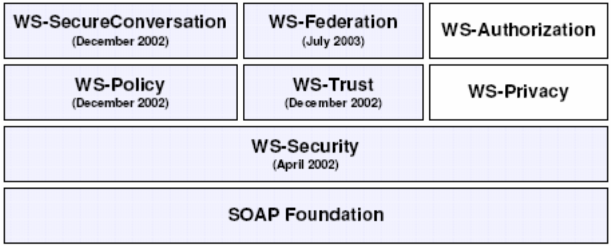
IV. EVOLVING TECHNICAL SOLUTIONS

Although there have been many models and techniques suggested by researchers in e-business security, the security of PHI is a unique problem in e-Health sector and we illustrate that with two cases (provider-driven and consumer driven) described above. We begin with provider-driven solution based on web services and XML in subsections A and B. Subsection C illustrates the consumer-driven situation.

A. 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 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 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 [10].



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. 2 Web Services Security Specifications

In April 2002, IBM and Microsoft published a joint security white paper 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 2.

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.

B. *XML based EHR Security*

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.

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. 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. *Platform for Privacy Preferences (P3P)*

Thanks to the proliferation of the Internet, consumers can now directly access healthcare related information over the web where sites ask for consumer private information with certain privacy statements. P3P is developed by W3C as an Industry standard to provide an automated way for users to gain more control over the use of personal information on the website they visit and it is applicable for any type of e-business (healthcare, finance retail etc.). The emphasis is on increasing the user confidence in online transaction to present them with meaningful information about the Web Site Privacy Practices. (www.w3c.com/p3p). P3P scopes out, notices and advertise to the user the data collection practices over the HTTP by the website and matches with the personal privacy preferences of the website user. This standard has been adopted by common browser software, such as the Internet Explorer. It saves the web surfer from having to read and think about the privacy protection considerations at each site the person goes to.

Since P3P was not designed for protecting the privacy of PHI in healthcare, P3P has a number of drawbacks. For example, P3P cannot monitor whether websites adhere to their own stated policy and procedures. P3P does not provide any security on data communication that could be addressed using Public Key Infrastructure. P3P Policy adds additional level of complexity without adding additional level of protection, since the healthcare consumers need to configure their browsers to take the advantage of P3P. No valid standard independent audit is available for web sites privacy practices.

We believe a more comprehensive solution is required for the privacy of EHR in the context of web savvy consumer social perspective. The solution needs to encompass technological, legal and social factors. Hence we have been working on a social, trust-based model that would verify, validate and enforce the privacy policies publicized by the website. This involves an independent trusted third party that would provide assurance to the users. This model cannot be discussed here due to space constraints and more details are available in [12].

REFERENCES

[1] Institute of Medicine. The computer-based electronic medical record: An essential technology for healthcare. NAP, Washington, DC, 1991(revised 1997).

[2] Rash, M.C. Privacy concerns hinder electronic medical records. The Business Journal of the Greater Triad Area (Apr. 4, 2005).

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

[4] Health eLink, Electronic Health Record, NSW HEALTH, URL: http://www.healthelink.nsw.gov.au/patients, accessed 2006

[5] The state of HIPAA privacy and security compliance. *AHIMA*. Apr. 2005. http://www.ahima.org/marketing/email_images/2005PrivacySecurity.pdf

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

[7] 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

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

[9] 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

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

[11] Wimalasiri, J.S., Ray, P. and Wilson,C.S., **Security of Electronic Health Records based on Web Services**, Proceedings of the IEEE Healthcom2005, Busan, Korea, June 2005

[12] A Chowdhury and P. Ray, "A Model for the Enforcement of Privacy Protection in Consumer Healthcare'", accepted for International Conf. on Smart Homes and Health Telematics (ICOST2006), Belfast, Northern Ireland, June 2006