A review of security of electronic health records

Khin Than Win

Abstract

The objective of this study is to answer the research question, 'Are current information security technologies adequate for electronic health records (EHRs)?' In order to achieve this, the following matters have been addressed in this article: (i) What is information security in the context of EHRs? (ii) Why is information security important for EHRs? and (iii) What are the current technologies for information security available to EHRs? It is concluded that current EHR security technologies are inadequate and urgently require improvement. Further study regarding information security of EHRs is indicated.

Keywords: *Electronic health record; information security; confidentiality; privacy*

Patient safety is an important issue in the healthcare industry. Electronic health records (EHRs) form an integral part of the healthcare system and it is imperative that EHRs are safe. EHRs have a variety of functionalities which include storage of health information and data, results management, order entry and management, decision support, electronic communication and connectivity, patient support, administrative processes and reporting and population management (Institute of Medicine 2003). Clearly, impaired integrity of EHRs could have undesirable outcomes in any of these areas. There is evidence that breaches of security have an impact on patient health care. Issues of confidentiality and abuse of data cause many healthcare providers to oppose the coordination of medical databases despite their potential benefits (Gaithersburg 2000). Without question, therefore, information security of EHRs is an important issue. This paper, which addresses the question 'Are current information security technologies adequate for EHRs?', is an initial exploration of the current state of information security of EHRs. The research question can be regarded as being in three parts: (i) What is information security in the context of EHRs? (ii) Why is information security important for EHRs? and (iii) What are the current technologies available and applied to information security of EHRs?

As in any information system, security of EHRs is of crucial concern. Confidentiality, integrity and availability are attributes of information security (Anderson 1999). Confidentiality is a form of informational privacy characteristic of certain relationships, such as the physician-patient relationship. Personal information obtained in the course of that relationship should not be revealed to others unless the patient is made aware of this intention and consents to disclosure (Gostin et al. 1993). Integrity of EHRs is important, as any changes or inaccuracy in data can have an impact on the healthcare process. Health information needs to be readily available to the authorised person at the time when it is required.

Security of EHR systems can be implemented by the physical security of the system, providing access only to authorised users, through the implementation of firewall and encryption technologies. Sensitive health information such as HIV status, obstetrics history and mental health history could become more easily accessible as health records become fully automated. If sensitive health information is accessible by others, this would clearly represent a breach of the patient's privacy. Healthcare providers and other stakeholders have a duty to maintain the confidentiality of data and systems, and need to deter access by unauthorised users.

Advancement of technology increases user accessibility and privacy protections involve the use of specific technologies. Protection of patient records can be achieved by implementing security policies to control access, appropriate authorisation before releasing the health data and by providing additional security measures to more sensitive data (Chilton et al. 1999). Healthcare providers and users of health information need to abide by the law of privacy to ensure patients' confidentiality; there is legislation to protect health information privacy in many countries. In the United States of America, the *Health Insurance Portability and Accountability Act* (HIPAA) emphasises privacy of health information, and all healthcare organisations and providers are obliged to follow the privacy and security regulations of HIPAA. In Canada, the *Personal Information Protection and Electronic Document Act* (PIPEDA) protects personal health information against use by commercial enterprises across provincial and national boundaries. The *Privacy Act* applies to the public sector and the *Statistics Act* applies to identifiable health information (Health and the Information Highway Division 2004).

In Australia, the *Privacy Act 1988* (Cwlth) established a privacy regime that covered health information in the private sector. the *Health Records (Privacy and Access) Act 1997* (ACT) was based on twelve privacy principles that have been tailored to suit the health environment. In Victoria, the *Health Records Act 2001* (Vic) came into effect from 1 March 2002 (Health Information Privacy Office 2002). In NSW, the *Health Records and Information Privacy Act 2002* came into effect from 1 September 2004.

Consent

Consent plays an important role in maintaining patients' privacy. Informed consent implies that a patient is fully informed of the implications of their medical status, and gives voluntary agreement to divulge or permit access to or the collection of their health information. Many organisations with access to health information have not obtained the individual's consent for disclosing personal information (Gaithersburg 2000). Effective notification and truly informed consent requires that individuals know and understand the contents of the record. It is unethical to use implied consent when the patient is not fully aware of information disclosure. Health data should not be processed in the absence of explicit consent unless they are needed for medical purposes or undertaken by a professional who in the circumstances owes a duty of confidentiality. According to the *Health Records and Information Privacy Act 2002* (NSW), health information must not be disclosed to anyone other than for its primary purpose. However, healthcare providers do need to disclose confidential information where a failure to do so would constitute a threat to public or private interests; for example, reporting communicable diseases to the appropriate health organisation. This measure ensures the safety of the public and it is important to disclose information in these instances.

Coiera and Clarke (2004) identified the following consent models: *General Consent with Specific Denials* and *General Denial with Specific Consent*. *General Denial with the Specific Consent* ensures maximum privacy as the patient's consent is required for any single access to records. This model may not be suitable for integration into EHRs as it could impede the workflow of healthcare providers, particularly in emergency situations. System administrators may be able to override the consent mechanisms. However, if consent is treated as a legal document and healthcare providers access the record without permission, there can be serious consequences and there should be legislation in place for such a situation. There can also be negative consequences if the patient's condition is not known as a result of access denial. There could also be a risk to healthcare providers if, for example, a patient's violent behaviour is not known due to the consent mechanism; there is a balance between the denial and access of consent mechanisms. Consent is important for consumer trust and respect for patient autonomy. A consent mechanism that gives the patient control over their records should not undermine the healthcare delivery process (Win, Croll & Cooper 2003). There should be an overriding mechanism for monitoring or reporting in the interests of public health. Although the focus of healthcare has changed from healthcare providers' paternalistic approach to a more consumer consent-oriented approach (Eysenbach 2000), implementing consent should not have a negative impact on the healthcare and treatment.

The case of *KJ vs Nepean Cancer Care Centre* (Connolly 2004) highlighted the importance of the patient's consent for the EHR system. As EHRs have been targeted to be implemented in Australia with the development of Health*Connect* trials and the National E-Health Transition Authority, this case reminds us of the importance of obtaining patients' consent and the level of access to records.

Incidents of security breaches

The following are examples of incidents of security breaches related to EHRs:

- University of Michigan Medical Center patient records were left exposed to the public on the Internet because the centre thought that they were on a server protected with a password (Carter 2000).
- A Florida state public health worker brought home a computer disk with the names of 4000 HIV positive patients and sent the names to two Florida newspapers (Stein 1997; Jurgens 2001).
- A hacker infiltrated the University of Washington Medical Center's computer system and stole at least 5000 cardiology and rehabilitation medicine patients' records (Lemos 2000; Songini & Dash 2000; Chin 2001).
- A hacker pointed out the vulnerabilities of the system because he had penetrated an unidentified medical centre in New York and another in Holland (Lemos 2000; Chin 2001).
- Kaiser Permanente accidentally sent the private correspondence of over 850 of its members to approximately 19 people in August 2000 (Fried & Pittman 2001).
- University of Minnesota researchers mistakenly revealed the names of deceased kidney donors to the recipients in a survey that they sent out (Sullivan 2002).

If a patient's information is disclosed accidentally or unintentionally, it may constitute an infringement of privacy, and cause embarrassment, ruin or damage to the individual's career, dismissal from work, loss of health insurance worthiness and financial loss (Waegemann 2000).

Information security and medical research

The *Health Records and Information Privacy Act 2002* (NSW) states on p. 59 that 'The organization that holds health information must not use the information for a purpose other than the purpose for which it was collected unless the use of health information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics in the public interest.'

There is a concern by some researchers that requirements for the patient's consent and anonymity will undermine their research (Evans & Ramay 2001; Roberts & Wilson 2001; Cox 2001). Production of substandard or flawed research is less ethical than the use of anonymous data by professional researchers (Roberts & Wilson 2001). Effective monitoring of vaccine safety, outbreak responses, and control of infectious diseases can be undermined if patient privacy has overridden the surveillance (Evans & Ramay 2001). In certain cases, universal inclusion of data is not possible as a result of lack of patient consent. For example, a cancer registry in Germany failed to achieve its mission as informed consent is required according to the law (Dudeck 2001). Data gathered from the multicentre acute renal disease registry was of limited use because only 52 percent of subjects provided informed consent (Ingelfinger & Drazen 2004). There can therefore be a conflict of interest between privacy and data accuracy, which can threaten patient safety.

Information security and technology

The most common authentication mechanisms seen in current EHRs are an 'identifier' together with a 'password' (Allaert et al. 2004). Implementation of a firewall to prevent external access to data can be seen in most healthcare organisations. As EHRs would be integrated between healthcare organisations, access levels become important for the system. Access control mechanisms can be applied for health information confidentiality. Implementing role-based access control mechanisms can maintain the confidentiality of the patient's health information according to the patient's consent. Each healthcare provider might have multiple roles and there may be a different range of services for different purposes for each role. Each role can include a location limit and access and time limitations (Parnell & Fearon 2002). Role-based access control is in place in most healthcare organisations (Barrows & Clayton 1996; Parnell and Fearon 2002). Audit trails become an important tool for data security as some of the security breaches have resulted from misuse of access privileges by authorised persons (Barrows & Clayton 1996). Nevertheless, it was noted that audit trails often can exceed the size of the original file by several orders of magnitude (Bilykh et. al 2003) and their use may not be pragmatic.

There are different security mechanisms implemented in EHRs to enhance information confidentiality. One example of security mechanism implementation is in the Alberta computer record systems where users need to punch in a unique identification number along with an electronic tag with a constantly changing digital number (Cotter 2003).

Biometrics identification is an alternative mechanism for authentication and identity verification. Retinal pattern analysis, voice pattern identification, hand characteristics and automated fingerprint analysis based on pattern recognition are some of the biometrics methods applicable for authentication (American Society for Testing and Materials n.d.).

Implementing an RFID chip is an another identification and authorisation mechanism for securing health information. However, inserting these under the skin is an invasive procedure. Beta testing of these devices have been started in the United States of America and about 40 people were involved in the initial testing (Schuerenberg 2005).

In Australia, the Australian Department of Health and Ageing has initiated research to implement a national approach to consent technology. The legal and technical implementation requirements (Clarke 2002) and design principles (Coiera & Clarke 2004) were identified as a result of this research. Digital signatures, PKI and Kerberos technologies were used for the different e-consent mechanisms in these projects.

Other projects use security agents to maximize the data security. Gritzalis & Lambrinoudakis have proposed a security architecture for interconnecting health information systems through security agents. The system ensures confidentiality through data exchanged, content integrity and access control, single sign-on authentication services, role based access control and auditing (Gritzalis & Lambrinoudakis 2004).

Most users of EHRs believe that password checking included in the system will ensure system security of EHRs. However, password checking alone to ensure access restriction does not secure adequate security for EHRs. Programs with common password protection use sub-routines that check against a hash-code of the password. Debuggers and disassemblers can reverse-engineer the binary program code to the human readable form and execute program instructions. This can search the sub-routine that decides acceptance or rejection of the password (Horst 2001). Thus, in addition to the password, there should be some mechanisms to enhance information security.

Symmetric cryptographic algorithms can be applied to protect the confidentiality of data during data transmission and storage. These algorithms can also be reversed so using asymmetric algorithm will allow strong authentication of all people accessing the database (Quantin, Allaert & Dusserre 2000).

Different projects and different organisations have implemented different security technologies for information security; however if consent has not been granted, they have not addressed the data for medical research purposes. This problem remains to be solved.

Different access models for EHRs have been proposed to address this. Kluge has proposed four different access models which are described in the Table. These models address use, storage, communication and manipulation of health data (Kluge 2004).

Confidentiality of medical research data can be obtained through anonymity and de-identification in various health service research projects. (Ohno-Machado, Silveria & Vinterbo 2004). However, there are concerns about privacy of health information because de-identified data does not guarantee confidentiality; the anonymity in research databases can be

Table 1. Access models (Kluge 2004)

	Healthcare professionals actively engaged in patient care	Research, planning and related purposes	Tracking and monitoring	Comments
Automatic authorized access model	Yes	Yes	Yes	Flag any other access
Modified automatic access model	Yes (identified data)	Yes (de-identified data)	Yes	Data in two streams (identified and deidentified)
Explicit consent model	Yes (with patient consent)	Yes (with patient consent)	Yes	Patients need to understand the consequences
Two stage model	(automatic + explicit consent model) + expansion of the modified automatic consent model – permissible to non-healthcare professional with explicit consent			

reversed through the 'disambiguation' process (Dreiseitl, Vinterbo & Ohno-Machado 2002). 'Ambiguating' data tables in combination with cell suppression, column suppression and encryption will ensure data confidentiality (Dreiseitl, Vinterbo & Ohno-Machado 2002).

Australian surveys on information security

Schattner and Pleteshner (2004) have documented Australia's survey on data security in 'The GPCG computer security project: final report'. It was noted here that an Adelaide Central and Eastern Division of General Practice informatics survey found that most electronic communication was sent in unsecured form (Schiller 2003). A survey from the ACT Division of General Practice which surveyed 45 practices in the ACT region found that most practices have Internet connection; however, 69 percent of those did not have a firewall. Fifty-one percent of practices indicated that illegal access to patient clinical records could be possible as passwords for access to their medical software were inadequate or non-existent (Rose 2003). It can be seen therefore that information security measures for some health information systems are still inadequate.

Discussion

EHRs contain sensitive patient information which can have an impact on the patient's health and even their life. EHRs involve different health information management activities for different purposes and information security is important for all these functionalities. There are continuing discussions and developments in the area of consent mechanisms to ensure information security of patients. As discussed earlier in this paper, requirements of consent for use of health information should not impede medical research and disease surveillance. Consequently, there needs to be a mechanism to address this efficiently to maintain patient privacy and fulfil the requirements of research and the epidemiology. Multiple broadcast encryption schemes incorporated into EHRs could be one of the solutions to this problem (Susilo & Win in press). However, this scheme is based on the unique identification of users of EHRs (patients, healthcare providers, medical researchers and so on) and this will need to be addressed first. Different authorisation mechanisms incorporating cryptographic techniques could possibly enhance the information security of EHRs. Information security of EHRs should be studied extensively to ensure patient safety through providing secure EHRs to healthcare providers, consumers, primary and secondary users of EHRs.

Breach of information security can stem from breach of confidentiality by authorised users, and abuse of their access privileges. Therefore, ethical and legal responsibilities of users should also be considered for the information security of EHRs. This study focuses on the technological aspect of information security in EHRs and does not cover the legislations, standards and policies for enhancing information security of EHRs.

Conclusion

In conclusion, this paper has addressed the research question, 'Are current information security technologies adequate for EHRs?' and it can be seen that implementing information security should address both private and public interests to achieve maximum usage of EHRs. Current information security technologies are as yet inadequate and there is still room for improvement for the security of EHRs.

References

Allaert, F.A., Le Teuff, G., Quantin, C. and Barber, B. (2004). The legal knowledge of the electronic signature: a key for a secure direct access of patients to their computerised medical record. *International Journal of Medical Informatics* 73: 239-242.

American Society for Testing and Materials (n.d.). *E1714-00: Standard Guide for Properties of a Universal Healthcare Identifier (UHID)*. Available at: <http://www.astm.org/cgi-bin/SoftCart.exe/index.shtml?E+mystore>.

Anderson, R.J. (1999). Information technology in medical practice: safety and privacy lessons from the United Kingdom. *Medical Journal of Australia* 170(14): 181-185.

Barrows, R.C. Jr and Clayton, P.D. (1996). Privacy, confidentiality and electronic medical records. *Journal of the American Medical Informatics Association* 3: 139-148.

Bilykh, I., Bychkov, Y., Jahnke, J.H., McCallum, G., Obry, C., Onabajo, A. and Kuziemsky, C. (2003). *Can GRID services provide answers to the challenges of national health information sharing?* Proceedings of the 2003 Conference of the Centre for Advanced Studies. Canada, IBM Press: 39-45.

Carter, M. (2000). Integrated electronic health records and patient privacy: possible benefits but real dangers. *Medical Journal of Australia* 172: 28-30.

Chilton, L., Berger, J.E., Melinkovich, P., Nelson, R., Rappo, P.D., Stoddard, J., Swanson, J., Vanchiere, C., Lustig, J., Gotlieb, E,M., Deutsch, L., Gerstle, R., Lieberthal, A., Shiffman, R., Spooner, S.A. and Stern, M. (1999). Pediatric Practice Action Group and Task Force on Medical Informatics. Privacy protection of health information: patient rights and pediatrician responsibilities. *Pediatrics* 104: 973-977.

Chin, T. (2001), Security breach: hacker gets medical records. *American Medical News* 44: 18-19.

Clarke, R. (2002). Consumer consent in electronic data exchange background paper, Xamax Consultancy Limited. Available at: <http://www7.health.gov.au/hsdd/primcare/it/docs/ecbackgrd.doc> (accessed March 2005).

Coiera, E. and Clarke, R. (2004). 'E-Consent': the design and implementation of consumer consent mechanisms in an electronic environment. *Journal of American Medical Informatics Association* 11(2): 129-140.

Connolly, C. (2004). Managing patient consent in a multidisciplinary team environment. *Privacy Law and Policy Reporter* 11: 1.

Cotter, J. (2003), Alberta health providers to share medical records via computer. *Canadian Press*, October 25.

Cox, P. (2001). Using patient identifiable data without consent. *British Medical Journal* 322(7290): 858.

Dreiseitl, S., Vinterbo, S. and Ohno-Machado, L. (2002). Disambiguation data: extracting information from anonymized sources. *Journal of American Medical Informatics Association* 9(6): 110-114.

Dudeck, J. (2001). Informed consent for cancer registration. *Lancet Oncology* 2: 8-9.

Evans, B. and Ramay, C.N. (2001). Integrity of communicable disease surveillance is important to patient care. *British Medical Journal* 322: 858.

Eysenbach, G. (2000). Consumer health informatics: recent advances. *British Medical Journal* 320: 1713-1716.

Fried, B. M. and Pittman, S. (2001). Protecting medical privacy in a digital age: beyond policies and procedures. A critical role for technology. California, Surf Control Inc. Available at:<http://itpapers.news.com>.

Gaithersburg, I.V. (2000). Electronic medical records and patient privacy. *The Health Care Manager*, March: 63-69.

Gostin, L.O., Turek-Brezina, J., Powers, M., Kozloff, R., Faden, R. and Steinauer, D.D. (1993). Privacy and security of personal information in a new health care system. *The Journal of the American Medical Association* 270(20):2487-2493.

Gritzalis, D. and Lambrinoudakis, C. (2004). A security architecture for interconnecting health information systems. *International Journal of Medical Informatics* 73: 305-309.

Health and the Information Highway Division (2004). Protection of personal health information, Canada. Available at: <http://www.hc-sc.gc.ca/ohih-bsi/theme/priv/index_e.html.

Health Information Privacy Office (HIPO) (2002). *Protecting the privacy of health information in the Northern Territory: discussion paper, March 2002*. Northern Territory Government.

Health Records and Information Privacy Act 2002 (NSW).

Horst, H. (2001). How to tamper with electronic health records. Available at: <http://www.gnumed.net/gnotary/tampering.html> (accessed May 2004).

Ingelfinger, J.R. and Drazen, J.M. (2004). Registry research and medical privacy. *New England Journal of Medicine* 350(14): 1452.

Institute of Medicine (2003). *Committee on data standards for patient safety: board of health care services. Key capabilities of an electronic health record system: letter report.* The National Academy of Sciences. Available at: <http://www.iom.edu/report.asp?id=14391> (accessed 8 August 2003).

Jurgens, R. (2001). *HIV testing and confidentiality: final report.* Canadian HIV/AIDS Legal Network & Canadian AIDS Society. Available at: <http://www.aids-hepatitisc.org/stigma/Hepatitis/HIV-testing-and-confidentiality.htm>.

Kluge, E-H. W. (2004). Informed consent to the secondary use of EHRs: informatics rights and their limitations. In: *Proceedings of the 11th World Congress on Medical Informatics, Part 1.* Fieschi, M., Coiera, E. and Li Y-C J. (Eds). Amsterdam, IOS Press: 635-638.

Lemos, R. (2000). *Medical privacy gets CPR*. Available at: <http://www.zdnet.com/zdnn/stories/news/0,4586,2667243,00.html> (accessed 17 May 2001).

Ohno-Machado, L., Silveira, P.S.P. and Vinterbo, S. (2004). Protecting patient privacy by quantifiable control of disclosures in disseminated databases. *International Journal of Medical Informatics* 73: 599-606.

Parnell, S. and Fearon, A. (2002). *South and west Devon: ERDIP evaluation report, volume 2: proof of concept.* UK, NHS Information Authority.

Quantin, C., Allaert, F-A. and Dusserre, L. (2000). Anonymous statistical methods versus cryptographic methods in epidemiology. *International Journal of Medical Informatics* 60: 177-183.

Rindfleisch, T. C. (1997). Confidentiality, information technology and health care. *Communications of the Association of Computing Machinery* 40: 93-100.

Roberts, L. and Wilson, S. (2001), Argument for consent may invalidate research and stigmatize some patients. *British Medical Journal* 322: 858.

Rose, M. (2003*). A survey of computer security in the ACT Division*. Canberra, ACT Division of General Practice.

Schattner, P. and Pleteshner, C. (2004). *The GPCG computer security project: final report.* Monash University, The Department of General Practice in Affiliation with the Department of Rural Health, The University of Melbourne, Monash Division of General Practice.

Schiller, G. (2003). *Informatics survey of general practice.* Adelaide, Adelaide Central and Eastern Division of General Practice.

Schuerenberg, B. K. (2005). *Implantable RFID chip takes root in CIO, mobile health data and health data management.* Available at: <http://www.mobilehealthdata.com> (accessed 16 May 2005).

Songini, M.C. and Dash, J. (2000). Hospital confirms hacker stole 5,000 patient files: attack points to need for standards for patient records. *Computer World* 34(51): 7.

Stein, L. (1997). The electronic medical record: promises and threats; web security: a matter of trust. Web Journal, Volume 2, Issue 3, O'Reilly & Associates. Available at: <http://www.oreilly.com/catalog/wjsum97/excerpt/>.

Sullivan, B. (2002). Release of organ donor data prompts changes. *Computer World* Available at: <http://archives.cnn.com/2002/TECH/internet/02/16/organ.donor.data.idg/> (accessed March 2005).

Susilo, W. and Win K. T. (in press). Securing electronic health records with broadcast encryption schemes. *International Journal of Electronic Healthcare*.

Waegemann,. C.P. (2000). A matter of privacy for e-health: security policies – international privacy – internet security. Available at: <http://www.medrecinst.com/conferences/asia/proceedings/10-00/privacy.pdf> (accessed May 2001).

Win, K.T., Croll, P. and Cooper, J. (2003). *Privacy, confidentiality and consent of electronic health record systems.* Proceedings of the Eleventh Annual Health Informatics Conference, Darling Harbour, Sydney, Australia, 10–12 August.

Glossary

Information security is a collection of policies, procedures and safeguards that help maintain the integrity and availability of information systems and controls access to their contents (Rindfleisch 1997).

Integrity is the prevention of unauthorised *modification* of information. It is important to maintain information integrity as any changes in data can have an impact on healthcare.

Availability is the prevention of unauthorised *withholding* of information.

Confidentiality is the prevention of unauthorised *disclosure* of information.

Implied consent is where agreement may reasonably be inferred from the action or inaction of the individual and there is good reason to believe that the patient has knowledge relevant to this agreement.

Express consent is the consent given explicitly, either orally or in writing. Express consent is equivocal and does not require any influence on the part of provider seeking consent.

General consent with specific denials refers to an instance in which a patient attaches specific exclusion conditions to the general approval of access to the record for future accesses (Coiera and Clarke 2004). ***General denial with specific consent*** refers to an instance in which a patient issues a blanket block on all future accesses, but allows the inclusion of future use under specified conditions (Coiera and Clarke 2004).

Khin Than Win *MBBS, DCS, IDCS, MSc, PhD*
Lecturer
School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522
AUSTRALIA
Phone: +61 2 4221 4142
Facsimile: +61 2 4221 4170
Email: win@uow.edu.au

Biographical information

Khin Than Win is a Lecturer in the School of Information Technology and Computer Science, University of Wollongong, Australia. She is a medical doctor with a PhD in health informatics. Her research interests are in issues related to electronic health record systems and quality and safety in healthcare. She teaches health informatics subjects and supervises several Honours and postgraduate research students in health informatics.