2005

Physician secure thyself

Patricia Williams
Edith Cowan University

Physician secure thyself.

Patricia A H Williams
School of Computer and Information Science
Edith Cowan University
trish.williams@ecu.edu.au

Abstract

Whilst discussion rages on the issues relating to security of medical data and the reason why it is important, there is little published information on how to tackle even basic security challenges for medical practice in Australia. Research suggests an underestimation of the threats to medical data by medical practitioners, hence there is sufficient reason to promote development of tools to assist medical practice with technical issues they are unfamiliar with. This paper provides an initial dialogue on how these security issues should be addressed. Included is a framework for risk assessment and elaboration of the implementation process to make medical data in Australia secure.

Keywords

Medical informatics, security, risk assessment, data protection.

INTRODUCTION

As more data is held electronically it becomes easier to copy and disseminate. This is one of the positive aspects of our information age; however, this has security repercussions particularly in the medical field. The once sacred trust between patients and doctors now requires more consideration if confidentiality is to be maintained. A consequence of the use of communications technology and by association, a perceived eroding of confidentiality, has seen medical ethics guidelines revised, stressing the protection of patient-doctor confidentiality. Yet, still more reflection is necessary in view of the possible legal implications (Pati, 2004). This is only one issue of security that Australian medicine is now faced with. Another issue is that of data protection. Frighteningly, in an Australian survey undertaken in 2002 (Holzer & Herrmann, 2002), only 84% of practices that used a computer system backed up their data. Of these only 76% retain a backup offsite and only 46% have had the backup tested. Only half of practices had any sort of power filter or battery backup or disaster plan, whilst alarmingly barely one third has any determination method for detection of unauthorised external access. All respondents' listed network or software application password access control as the only method of data security. On average only 50% had policies covering use of security, yet all with computers had Internet connections. This indicates an alarming underestimation of the threats to medical data by the medical practitioners.

This paper follows on from discussion on the threats of security to medical data (Williams, 2005a), to elaborate on the practical side of security for medical practitioners in terms of risk assessment. These threats to medical data relate to confidentiality and privacy (authorised accessibility), integrity and misuse (authorised modification), and availability (authorised accessibility when required). The next step in the security of medical data is to assess the risks the data is subjected to. Risk assessment is a term commonly used in medicine and more in specifically public health. It refers to "The qualitative or quantitative estimation of the likelihood of adverse effects that may result from exposure to specified health hazards or from the absence of beneficial influences" (Last, 1988, p.93). From a computer security viewpoint this definition is similar where risk assessment "assigns levels of risk to various threats to the network security by comparing the nature of the threats to the controls designed to reduce them" (Dennis, 2002, p.308).

Whilst there exist academic frameworks for risk assessment in specific situations such as Telemedicine (Stamatiou et al., 2002), there is little non-technical guidance for medical practitioners and staff responsible for security of medical data. The overall process for security of medical data should include:

- risk assessment to obtain an overview of the anticipated threats and risks to data;
- development of policies and procedures for those responsible for security, and other staff, to follow; and
- implementation of protection measures appropriate to the environment.

In the development of risk assessment and the resulting protection procedures, it is important to recognise the different levels of security threats each medical provider is open to, as these may differ for each practice or hospital (Panko, 2003). This paper discusses the processes involved in risk assessment and how these can be implemented in practice. It also considers some aspects of protection that should be considered for an environment where technical expertise may not be readily available.

ASSESSING RISKS

The Risk Assessment Process

For any organisation, risk assessment is an important security measure. The old saying that 'you cannot manage what you cannot measure' is never truer than in the sphere of security. The nature of medicine is such that much of the patient data recorded is not 'mission critical'. The data retained in a primary care environment is used primarily in the management of chronic disease and to assess potential health risk. The majority of this information is historical but may be used on a regular or episodic basis during clinical consultations. In contrast, the nature of medical data is not the same for data collected in an emergency department, where it is used in situ and rarely accessed subsequently. Therefore, the context in which the data is being used is important to assessing a risk. Additionally, there is a business perspective for medical practitioners who are responsible for the financial wellbeing of the practice. Thus, risk assessment is contextual and whilst the process can be generalised, the application of it cannot.

A simplification of the risk assessment process is given in figure 1. Firstly, identification of the information critical to the practise of medicine and information critical to the business is required. In security terms these are referred to as 'assets'. The assets must be considered in terms of the three essential elements of security: confidentiality, integrity and availability (Tomes, 2005). It must also judge the impact any loss of protection would result in (Lewis, 2003). The process of risk assessment begins with cataloguing the assets (in this case the financial and patient data); identifying the potential threats to these assets; and recording the protection methods available. The protection should be considered in terms of preventative measures, detective measure and corrective measures. Next, a matching of the data assets to the potential threats is undertaken, producing an identification of risks. Following this, an assessment of the level of risk to an asset must be made. The level of risk is derived by reflection on the impact the threat would have were it successful, against the possibility of its occurrence. Next, a correlation of the level of risk of a threat to an asset must be made. This is to gain an understanding of the vulnerability of that asset. Lastly, possible control measures can be assigned to each threat/asset combination. In any assessment of risk and development of controls, the overriding commonsense approach should be taken, in that only those risks that can be reasonably anticipated need to be subject of the controls (Tomes, 2005).

Full documentation on the controls and procedures should be up to date and retained as part of the intellectual property of the institution or practice. For instance, the methods of electronic data transmission protection should be recorded as the guidelines for such transmissions where they exist do not specify a particular method or standard (Gilkes, Casimiro, McEvoy, MacFarlane, & Kitchen, 2003). The type of information being shared and its method of transmission must both be considered.

Details on the type of threats to consider and what controls are available are context specific. For instance, the Royal, Australian College of General Practitioners (RACGP), General Practice Computing Group has recently published a set of guidelines intended for general practitioners on the security issues of data (Schattner, 2005). The intended use is for those with little technical knowledge. The guidelines are the first of their kind specifically for medical practitioners who need to protect both their business data and their patient records. The checklist covers the basics of computer security measures as the "10-item IT security guidelines":

- Responsibility for security issues;
- Established policies and procedures;
- Access control;
- Disaster recovery
- Consulting room and front desk security
- Backup
- Viruses
- Firewalls
- Network maintenance
- Security electronic communication (Schattner, 2005, p.5).

The guidelines themselves indicate (from a security viewpoint) the fundamental nature of the security measures suggested. The increased use of electronic communication will require more complex measures. Security of electronic communications together with the use of firewalls will covers some hazards of Internet use, however, unless there is a thorough understanding of the potential threats, the use of these security measures may not be sufficient.

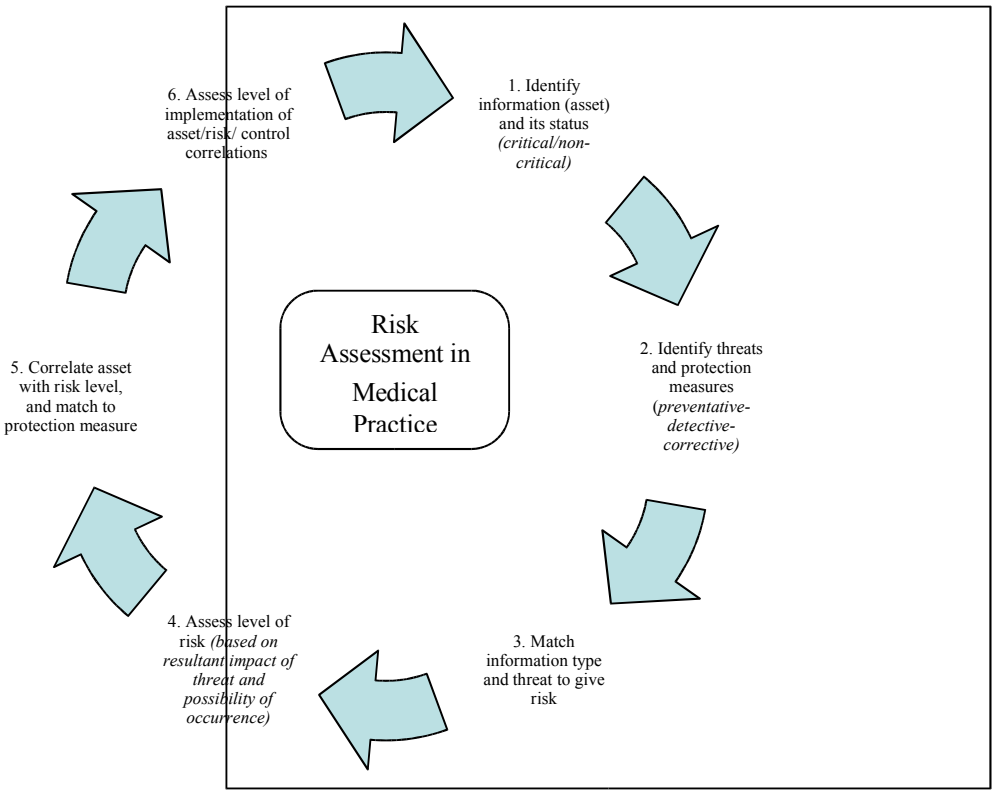

Figure 1: The risk assessment process.

Implementation of the Process

To make the process of risk assessment fit the intended environment, it is useful to draw parallels between security risk assessment and medical risk assessment. In view of the fact that it is unlikely that most primary health care providers will have access to security expertise, this approach may assist those responsible for the management of data security in clinical practice.

1. Identify information

The first step is to identify the electronic data to be protected. It is important to classify critical data and non-critical data. The classification can be by database, or more commonly by application. It should include the patient data; financial data; reference material; practice management and clerical information retained by the practice. Further, the software that is used to run the applications should be identified. Lastly, the physical hardware needs to be recorded, for instance servers, printers, and PCs, as the software cannot run without the hardware! Also, the expectations and requirements for data availability must be calculated as a benchmark to ascertain what level of security risk and failure the practice can sustain.

2. Identify threats and controls

This activity consists of identifying responsibilities, threats, and protection methods. It is essential that allocation of responsibility for security should be assigned. Next, identification of the threats should be undertaken. Good examples of the potential data and computer threats can be found in texts such as Dennis (2002. p.305). However, for the medical environment these should be identified with the issues of confidentiality, privacy, integrity and availability in mind. For instance, the interception and unauthorised access to information are important issues. Patient identifiable data is now regularly sent electronically to the Australian Health Insurance Commission by general practices to claim payment for services (Medclaims). The control method for this is the Australian Government public key infrastructure (PKI) encryption. Another example in the day to day running of a medical practice is access control, which can be a significant concern. Access control is mainly managed by password authentication. If authentication is to be effective, it needs to be consistent with a role-based level approach. Normal passwords chosen by users are a high risk authentication technique. Unfortunately, the use of smartcards and biometrics is not yet commonplace. In addition, the type of technology becoming popular in the

medical environment, due to the demand for increasing mobility, like personal digital assistants (PDA), creates added interception and synchronisation issues. Unlike the US's Health Information Portability and Accountability Act (HIPAA), which specifies strict regulation on wireless data protection, Australia has no such data security compliance regulations (Veltman, 2003; Williams, 2005b). Integrity and error correction of data can also be problematic. Meredith (2005) cites examples in the UK where patient information is regularly checked by the patient themselves. This technique has been proven to assist not only in the accuracy of the data but has improved the quality of the consultations and understanding by the patient of their treatment. This can be considered an effective control measure.

Lastly, in identifying threats and control, protection measures must can be named and classified into preventive, detective and correction methods. For this task research into available methods may be required. Useful but less technical information can be gained from sources such as the GPCG (RACGP, 2005; Schattner, 2005). A major factor for this and any protection method is policy and procedures management.

3. Matching threats to data assets

Matching the information and threats will result in a matrix of potential risks. This is essential to gain an overall picture of the security issues facing the practice.

4. Assessing level of risk

A level of risk has to be assessed in light of the protection currently in place and the impact the threat would have if successful. Assigning such risks (relative risks) is not uncommon in clinical diagnosis and management of disease. It forms part of the clinical decision making processes of medical practitioners and is used in methods such as clinical decision analysis. The statistical assignment of risks is not an exact science; it is the process of assigning a likelihood of the event occurring given the controls in place. Relative risk in medicine is represented as the incidence of a disease among those exposed over the incidence in those not exposed (Barker & Rose, 1984). In security the equation is similar in that it is assessed as the occurrence of the event given the control measures over the occurrence without the control measure (CQU Computer Security Committee, 1996). In computer security this risk is assigned as low, moderate or high, rather than a statistical result.

5. Correlating information, level of risk and protection

The correlation of the data to be protected, its potential risks, and the control measures that can be used can be a complicated exercise but is an essential one. This activity will allow a full picture of the vulnerability of the practice to be created. As part of this step, disaster recovery plans should be developed.

6. Assessing current protection

Finally, a review of the measures currently in place must be performed. This allows effective decisions to be made, and actions taken to improve the security and protection of the medical data. As an example, many common security problems can be assisted by education. Many healthcare professionals are unclear about the details, or even the existence, of privacy and data protection laws or what they mean in practice (Meredith, 2005). Strobl (2000) lists a misunderstanding and perplexity over the interpretation of data protection acts as a major contributor to the confusion decision makers are forced to face when managing patient data. Another common problem is power security. Electrical protection can be easily afforded by using an uninterruptible power supply (UPS). The device allows time to complete current work and facilitate correct close-down procedures (another susceptibility of data to loss through incorrect switching off procedures). A UPS can be a cost-effective and cost-avoidance measure in security (Appelt, 2005). There are many such straightforward measures that can be put into practice.

CONCLUSION: FUTURE CONERNS

The approach taken to risk assessment and security is important. Gilkes et al (2003, p.427) suggest that data protection is "the balance between facilitating important research and audit, and protecting patient confidentiality". They describe a situation where a patient information database has 'medium' security. In this case medium is translated as the data being held on a specific computer hard drive, where the logon and database are password protected. In terms of the potential risks this 'medium' definition of security it sadly inadequate. The emphasis has been placed on meeting legal requirements rather than assessing the inherent risks in both recording, retaining and using such information. Perhaps some of the responsibility lays with the providers of the health records systems themselves, in that accountability for security should be part of the IT development process. The changing nature of how we use electronic health information needs to be addressed at a root level during the construction of clinical IT systems.

As discussed widely in the literature, the lack of government policy and legal protection in Australia is of concern (ICTSC, 2004; Williams, 2005b). However, this should not prevent clinical practitioners from taking seriously the responsibility for protection of medical data. Ultimately, they may be required to meet strict

security and data protection standards similar to those in place in the US under the HIPAA (Department of Health and Human Services, 2003). The implementation of such guidelines can be characterised by the report recently that a US medical centre has moved from the traditional password and user identification security to a new biometric system. Driven by the need to meet the increasingly demanding legislation in the US, medical practices are increasingly turning to biometric security (Dalton, 2004). Whilst Australia is a long way off from the restrictions of the HIPAA legislation, action taken now will certainly alleviate the pain of risk assessment when it ultimately comes into force.

The technological advances made in clinical medicine are paralleled by the advances in computing and communications. “Integrated electronic health records are increasingly seen as the way to achieve quality and continuity in treatment, fill the gaps in public health research and contain costs” (Carter, 2000). The internet is becoming a viable alternative to data transfer between health care providers over other forms of communication. The security issues in using a public network must be seriously considered. Security policy and awareness are the keys to good protection, in addition to monitoring and audit controls. For areas were patient data cannot be adequately restricted in a network then encryption should be considered (Jones, 1998).

A lack of recognition of the issues involved in computerized databases and basic security measure indicates a dangerous gap in the security of medical data. Whilst the Australian government has set up the Health Information Council whose terms of reference include privacy and security of data, it has fallen to the professional bodies, like the RACGP to devise basic guidelines. There is a clear need for assistance to medical practices to secure their data. This includes understanding the issues of security and performing risk assessment, as the first steps in acknowledgment of the safety and importance of security of medical data.

REFERENCES:

Appelt, K. (2005). Safeguarding data integrity from power failure. Health Management Technology, 26(3), 30-32.

Barker, D. J. P., & Rose, G. (1984). Epidemiology in medical practice (3rd ed.). Edinburgh: Churchill Livingstone.

Carter, M. (2000). Integrated electronic health records and patient privacy: possible benefits but real dangers. Medical Journal of Australia, 172(1), 28-30.

CQU Computer Security Committee. (1996). Annex 1 - Threat risk assessment. Retrieved 17 August, 2005, from http://www.cqu.edu.au/documents/compsec/guidelines/cqu_seca1.html

Dalton, A. (2004). Eye Spy. Hospitals & health networks, 78(11), 12.

Dennis, A. (2002). Networking in the internet age. USA: John Wiley & Sons.

Department of Health and Human Services. (2003). Health Insurance Reform: Security Standards; Final Rule. Retrieved March 28, 2005, from http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf

Gilkes, C. E., Casimiro, M., McEvoy, A. W., MacFarlane, R., & Kitchen, N. D. (2003). Clinical databases and data protection: Are they compatible? British Journal of Neurosurgery, 17(5), 426.

Holzer, G., & Herrmann, N. (2002). Informatics survey for practice managers. Retrieved 14 August, 2005, from http://www.sadi.org.au/survey/Practice_Managers_Survey_2002.pdf

ICTSC. (2004). Information and Communications Technology Standards Committee. Foundations for the future: Priorities for health informatics standardisation in Australia, 2005–2008 (No. ISBN 0 642 82642 0): Commonwealth of Australia.

Jones, R. L. (1998). The Internet and healthcare information systems: How safe will patient data be? IS Audit & Control Journal, 2, 25.

Last, J. L. (Ed.). (1988). A dictionary of epidemiology (2nd ed.). New York: Oxford Medical Publications.

Lewis, D. (2003). Keeping the doors open. Computer technology review, 23(8), 32.

Meredith, B. (2005). Data protection and freedom of information. BMJ, 330(7490), 490-491.

Panko, R. R. (2003). Business data networks and telecommunications (4th ed.). Upper Saddle River: Prentice Hall.

Pati, A. (2004). Manage your data. Medeconomics, 25(3), 40-41.

RACGP. (2005, 2/03/2005). Media release: GPCG launches computer security guidelines and checklist for General Practitioners. Retrieved 12 August, 2005, from http://www.racgp.org.au/document.asp?id=16079

Schattner, P. (2005). The GPCG computer security self-assessment guideline and checklist for General Practitioners. East Bentleigh, Victoria, Australia: Department of General Practice, Monash University.

Stamatiou, Y., C, Henriksen, E., Lund, M. S., Mantzouranis, E., Psarros, M., Skipenes, E., et al. (2002). Experiences from using model-based risk assessment to evaluate the security of a telemedicine application. In Telemedicine in Care Delivery — Technology and Application (TICD'02). 115-119.

Strobl, J., Cave, E., & Walley, T. (2000). Data protection legislation: interpretation and barriers to research. BMJ, 321(7265), 890-892.

Tomes, J. P. (2005). Prescription for Data Protection. Security management, 49(4), 75-77.

Veltman, C. (2003, May 21). Wireless ways on the wards: Handheld devices. The Financial Times, 5.

Williams, P. A. H. (2005a). The underestimation of threats to patient data in clinical practice. In 3rd Australian Information Security Management Conference [In publication]. Edith Cowan University, Mount Lawley, Perth, WA.

Williams, P. A. H. (2005b). Where are the policies for PDA usage in the Australian healthcare environment? In 4th European Conference on Information Warfare and Security. 401-408 & [CD-ROM]. University of Glamorgan, Wales, UK: Academic Conferences Limited.

COPYRIGHT