

Security Immunization Using Basic Countermeasures

P. A. H. Williams

School of Computer and Information Science
Edith Cowan University
Joondalup, Western Australia

Abstract – *The increased use of computing has significantly raised the profile of information security within the clinical environment. Medical information security is concerned with protecting the assets of a medical practice. These assets include hardware, software and intellectual property. To date, computer and information security in this environment has been poorly applied. Whilst the tenets of confidentiality and privacy are paramount in the practise of medicine, they are inadequately protected in the evolving electronic environment. Protection stems from an acknowledgment that risks exist, the identification of the assets to be protected, and the application of security countermeasures to manage the risks. In this field, many guidelines have been developed, however most are not easily applied by physicians and non-technical staff charged with the responsibility of securing their medical systems. However, there are basic countermeasures can be applied with minimal technical knowledge of information security.*

Keywords: Medical information security, computer security, countermeasures, health.

1 Introduction

In Australia, there is wide spread use of computers in general practice for a variety of applications, which include practice management, prescription printing and to a lesser extent, patient clinical records [1]. General Practitioners have a professional obligation to maintain currency in medical treatments and developments through continuing medical education and on-going professional development [2]. Traditionally this has meant referencing textbooks, reading numerous journals and keeping up to date with the vast amount of printed pharmaceutical information. Internet technologies have provided an alternative low cost vehicle to access to a wide range of patient and medical information. It has been reported that in Canada at least sixty-six percent of practitioners are using the Internet to support their clinical practice [3], and in the UK this figure is report to be as high as ninety-six percent [4]. Statistics for Australian practice were reported at seventy-six percent in 2001 and this has no doubt risen [5]. Further the widespread use of email has the potential to significantly improve communications between medical professionals. The electronic transfer of data between

auxiliary services such as pathology laboratories and medical practice is commonplace [6]. Almost all Australian practices use computers for administrative tasks such as billing and most now have a computer in the consulting room for prescription printing and clinical record management. These factors, in conjunction with the government push for integrated national electronic health records [7], provide a strong case for information security review in general practice.

Information security features exist in software and operating systems, yet poor utilization of these features can often be attributed to the lack of usability or comprehension of the features [8]. Even the most common security measures are misused, such as not changing passwords periodically, group passwords, out of date virus protection, and lack of auditing, and so on.

Medical information is a fundamental asset of a medical practice. Protection of this asset is a primary activity in quality governance. Thus, medical information security is concerned with the protection of this asset, namely patient, clinical and business data held by the medical practice. Asset protection should be viewed as a continuing process, however it is one that is seriously underestimated in importance in medical practices worldwide [9].

The process of effective information security includes

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

The process of risk assessment begins with identification of assets; potential threats and the existence of vulnerability of these assets. A key component of this is the judgment of impact, in which any loss of protection would result [10]. The resultant protection should be considered in terms of countermeasures for prevention, detection and correction. This paper discusses the current perception of risk and the fundamental assets in this medical

environment. It further explains why current guidelines are insufficient and discusses basic security measures that can be put in place for effective frontline protection.

2 Risks

In Australia there is an underestimation of risk in medical practice in regards to information security [9]. In particular, healthcare is an area that has been slow to understand the risks and adopt appropriate measures to address them [11]. This situation has been compounded by the difficulty faced by practitioners in understanding the many and varied legal statutes that apply to all data in terms of electronic collection, retention and transmission [12]. The underestimation of risk results in a lack of appropriate and often basic measures, being put in place [13]. Inconsistent backup procedures, group access codes, lack of intrusion detection and infrequent auditing are a few of the disturbing yet basic security procedure failures.

The concept of risk relates to the possibility of an adverse event occurring. Risk is therefore a combination of a threat, vulnerability and value of the asset. Vulnerability occurs when there is a weakness that can be used to cause harm to the asset [14]. The management of risk involves assessing risk and putting plans in place to control it [15]. The process of assessing risk begins with identification of assets.

3 Assets

In any medical practice the assets include not only the patient data collected, but management and other clinical support data.

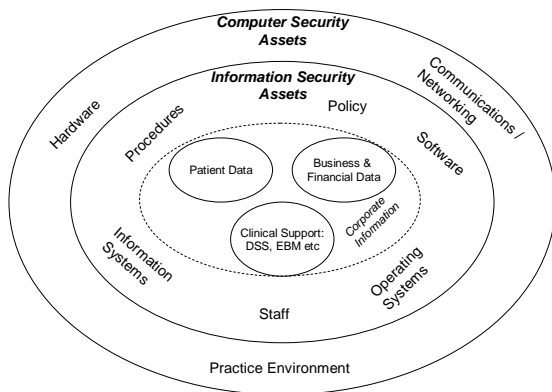


Figure 1. Assets in the General Practice security.

Further, the software programs used, the operating system and all hardware, including the telecommunications and networking equipment, are also primary assets to be protected. In addition, the practice policies and personnel knowledge are also assets making up the 'information' environment. Figure 1 shows how these assets are structured in a general practice.

4 Guideline confusion

Most countries consist of a mix of government and private practice health organizations designed to deliver quality health care to patients. Standards, such as ISO 17799, are essential to control communication, information access, reducing costs of innovative new systems, and protecting privacy. The key assistance that standards provide is in relation to process and procedures; consistency in information representation; and secure data transfer.

Whilst these standards and legal documents detail in a general sense what aspects of security need consideration, they are not written in lay terms and do not provide sufficient guidance to be of practical use [16]. The types of threats to consider and what controls are suitable are typically context specific. Many professional medical organizations are attempting to assist medical practitioners in this area, such as the Royal Australian College of General Practitioners (RACGP). The RACGP General Practice Computing Group has recently published a set of guidelines intended for general practitioners on the security issues of data [17]. 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 and patient records.

5 Countermeasures

The protection of assets must be considered in terms of the three essential elements of security: confidentiality, integrity and availability [18]. The countermeasures discussed in this section relate to these elements as they affect the assets identified in figure 1. These cover the computer security assets, as distinct from the information security assets. Also, further consideration is given to wireless networks as they are rapidly becoming a special case for security measures.

5.1 Computer Security Assets

In a medical practice, the computer security assets relate mainly to the physical environment. That is inclusive of the computing hardware, the networking

and communications equipment and other aspects of the practice environment such as paper records. These types of assets are protected by physical security measures. Further, wireless networks are included in this group as the issues of access relate directly to the communications network and physical layout.

5.1.1 Physical security

Physical security is important in maintaining the availability of information. In a tradition networking environment, physical security is related to access and building security. In the medical location many of these basic countermeasures are overlooked – the reception area is left open to access and unattended, consultation rooms left with the doors open (for security reasons!) and when shut they are left unlocked. These are simple flaws in security to overcome.

Ensuring the continuing availability of the network and the controlled shutdown of a network in the occurrence of a power failure is important. The use of a battery backup and power line conditioner are therefore essential. Such equipment is easily installed by merely connecting power plugs and being made aware of the procedure to follow if the equipment becomes active in the event of a power failure. Protection against fire and flood (such as burst water pipes) is also a basic countermeasure and one that is often overlooked with the installation of computer networks. Consideration of where the server and communications components are placed is a simple but astute tactic.

Gaining an accurate picture of what physical assets the practice has and where they are located is a straightforward initial step. Unauthorised connection of equipment to a network, such as modems, can create serious holes in the security of system. Sometimes set up to circumvent other controls, however innocently, these actions leave the network open to attack. Further, since management of these assets is also part of the security portfolio, knowledge of where physical assets were purchased, where they can be serviced and repaired and what warranty applies can also be helpful [19]. The use of mobile equipment such as laptops and personal digital assistants must also be considered. The security risks with such equipment in the medical environment are well documented [20]. Careful disposal of computer equipment should also be considered.

5.1.2 Wireless networks

Wireless networks are a special case in networking as they pose significant security problems yet are

popular due to the benefits provided by increased mobility. As our networking capabilities, particularly in the area of wireless networking, have increased so to have the incidence of malicious threats [21]. These threats include denial of service, viruses and worms. Other threats which may not be so obvious include bandwidth theft and information corruption. The versatility that wireless networking has provided is helpful to the practice of modern medicine. Yet such systems have security vulnerabilities, arguably of greater importance given the sensitive information they are carrying. Standards exist to ensure a secure system and provide associated minimum technical specifications. In the case of wireless systems using 802.11 wireless standards this includes encryption using Wired Equivalent Privacy (WEP). Whilst this method provides a basic level of security, (enough to deter the opportunistic hacker and therefore suitable for home users), it is ineffective against serious threats [22]. The first step in securing a wireless network is to know the pattern of coverage it provides, called a footprint. This footprint can then be adjusted to remain within the confines of the building and therefore limit vulnerability. It should be noted that whilst the configuration of a network may remain constant, the vulnerabilities may not due to software upgrades.

5.2 Information Security Assets

The information security assets encompass all other assets within the medical environment. This includes software programs, data, policies and other intellectual property (including staff) contained in the practice.

5.2.1 Staff

The staff in a practice form both part of the information system itself and part of the risk to the computer based information systems. Responsibility, access control, and monitoring are all issues specific to the staff of a practice. Intellectual property and other intangible assets also need protection. Physical security of personnel is not discussed here.

First and foremost, responsibility for security should be clearly defined. Whilst everyone in the practice is accountable for security and their part in maintaining a secure environment, identifying who is capable of managing the overall security for the practice and allocating them the responsibility is an important first step. The strategic decision making may come from the partners in a practice, the owners or the management group, however security is not an issue to leave to chance and it must be managed and monitored to be effective. Part of this task is to assess what the

current situation is in regards to basic security measures and identify areas for immediate improvement.

From a risk perspective, access control and password management are essential. Password protection has been shown to be highly ineffective, yet it remains our primary method of protection for many systems. Whilst many of the controls should be established using policy, education and awareness of practice staff is also required. Education in password protection best practice and why it is required should be undertaken. It is insufficient to simply ask staff to change their passwords regularly. What is required is an awareness of why this is important in terms of potential consequences of hackers or intruders getting into the system, or indeed opportunistic intrusions by patients or visitors to the practice. Understanding the type of threat, the seriousness of breaches in security, the potential outcome and how they can be moderated, contributes greatly to the protection of a system by the staff themselves. Further, since intrusion detection requires monitoring and additional expertise, 'prevention is obviously better than cure'. The theft or selling of personal and sensitive information is becoming a serious risk for medical practices. Misuse of health information will occur where there is perceived value of personal information to third parties. There are numerous examples in the media and in official reports recounting incidents where personal information has been misused. Information has been sold to pharmaceutical companies and genetic information has been used for employment and insurance restrictions [23, 24] Technology unfortunately does not have all the solutions to data misuse and loss. Medical practices have a significant number of data security related occurrences each year, many of these are attributed to the lack of importance staff place on adhering to security policy and procedure [25].

There is much discussion on computer monitoring of employees and significant evidence that security breaches are most often from within the organization [26]. Whilst monitoring can be undertaken by electronic means, the most basic of measures is auditing. Most, if not all, software programs in use today in Australian medical practices have auditing functions built in to them. However, these checks often fail for two reasons: firstly, the auditing is either switched off or not checked due to time constraints or even lack of understanding of their use; and secondly, when group password and logins are used the auditing function is of little use. When up to forty-eight percent of violations and errors are accidental [27], it seems only common sense to utilize such facilities and analyze the reports.

Monitoring of other computer use, for instance email and breaches of security through communication, are detectable but require additional software and time to analyze, and may indeed be illegal to use. A simple yet effective measure is to require employees to sign a statement agreeing to the expectations of behaviour in regard to email, privacy of information and computer usage. In addition, written policy on normal usage should be clearly outlined.

Lastly, it is vital that the practice have exit procedures that encompass confidentiality and immediate reversion of access when a staff member leaves employment. This is often overlooked, as setting up and revoking access is a managerial task or may require intervention from the software supplier.

5.2.2 Policy and procedure

A security policy addressing the potential threats is a necessity. This must include clear definition of responsibilities and be contextually correlated to the specific electronic information systems used. Managing risk is the key element in data protection, since there is a choice when a risk is identified to accept it, reduce it or protect against it [28]. Policy is a countermeasure that is interwoven in all aspects of asset protection discussed in this paper. As mentioned earlier, whilst interpretation of the legalities and standards can be difficult, it is a prudent action to ensure that the practice meets the basic requirements of responsibility and compliance in relation to these. In many cases it is defensible to at least show best practice is being attempted.

Procedures, resulting from policy, need to be in place in regards to the numerous aspects of security which must be covered. For instance, procedures for alteration, and particularly deletion of information, should be specific to ensure that legislative requirements are fulfilled and that accidental removal or corruption is avoided. Not only can such actions be a legal concern, they also have the potential to cause serious injury through a lack of patient information or incorrect information [29].

5.2.3 Software and operating systems

It is essential to protect the system availability from denial of service attacks and virus infection. The use of a firewall, correctly and appropriately configured is mandatory. This configuration can be beyond the capability of practice staff and may require additional assistance, however it is important that the practice

understands what is in place and are assured that the setup provides the protection they require. Similarly, protection using anti virus and spyware software have become basic countermeasures, yet these are often not in place or not regularly updated [30]. Operating system updates too must be applied as they become available. Both of these software related activities have been made easier by the manufacturers who provide for automatic electronic updates via the internet. Once activated, these protections can run unattended.

Access control includes file and folder permissions, printing and other service access. Whilst it is outside the boundary of capability of most staff, access control to files, folders and other sections of the system should be set at an appropriate level for the practice. This may require assistance from the software supplier; however an undertaking from the supplier to ensure consistency with practice requirements should be sought. Understanding how secure a system is, is an essential part of asset protection.

Business continuity planning and disaster recovery planning are two aspects that are sometimes given poor consideration and regularly confused as one concept. Most practices are dependent upon their computer systems and networks to operate effectively and efficiently. This requires that business continuity planning be in place so that normal functions can still be undertaken in the event of a disruptive event. Ultimately, the practice of medicine is a human activity, and in emergency situations access to previous history may not be possible. However access to patient and other clinical information can affect both the quality of care and the ability of a physician to consult effectively and for a practice to function normally. Whilst short periods of down time may be inconvenient, prolonged periods of inaccessibility to the network can create significant problem both administratively and clinically. This is in contrast to disaster recovery planning which provides a plan for recovery from a major event. A major factor in disaster recovery is the role of backup. This is an area that is inadequately addressed in Australian medical practice [13]. Daily, weekly and monthly backup should be preserved and checked for errors; backup should include data and software; and procedures, including keeping periodic backups off-site are essential.

5.3 Corporate Information

Protection of the actual data contained within the practice, which is the patient data, financial data and other clinical support material, in terms of availability and confidentiality will result from the protection of the

outer layers of the assets from figure 1. The integrity of the data and the tracking of changes using auditing is an often overlooked method of security breach detection. As human interaction with the data is the weakest link in the security chain, it is imperative to have some control mechanisms in place. Most software packages contain some auditing features; however as discussed previously these are often not switched on or not periodically reviewed.

Maintaining and assessing data quality is a major area for current research. In medicine it is not only the integrity (correctness) of the data that must be assured, it also requires that anomalies are avoided and the semantics of the patient information are homogeneous.

6 Conclusions

Understanding the risks and nature of threats is the first step in securing a network in a medical practice. Education and informing staff both of the risks and the appropriate actions can be an effective and simple countermeasure. Whilst a full risk assessment of the environment is a more holistic approach to the problem, implementing basic protective strategies are a good start.

The issues of electronic information in medicine has recently given rise to the term *Information Governance*, defined as providing “a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service” [29]. It is clear that information security is more than a technical issue; it is a people issue and more importantly a legal one. Accountability alone should motivate medical practice to take a closer look at its processes and procedures in this area. Clearly, governance, (which is a known term in medicine in relation to clinical governance) is both an executive level activity in terms of decision making, and a managerial activity in the implementation of strategy [31]. As such, there will be changes required in how medical practice approaches this issue, particularly as many practices operate on a trust basis and in general the medical profession is reluctant to be paralleled with business enterprise. Therefore, a cultural shift has to occur. It is well reported that the culture of an organization and the support of the management, is a key factor in the adoption and incorporation of practices within that organization [32]. Culture can therefore play a major role in the actions of the staff in a medical practice. The development of a specific culture in any environment takes time and persistence, if it is not inherent in the existing culture. It can however be a strong facilitator of change. The seriousness with which

security is considered, and behaviour displayed by practitioners themselves, can significantly influence the practices of staff [33]. Once again policy plays a major role in this if the culture is to be affected [34].

The increased use of computing has significantly raised the profile of information security within the clinical environment. Security should be seen as a process rather than a result [35]. It is imperative to create policy and procedures that are easy to follow and enact, rather than rely only on technological solutions that are often incorrectly used. It should also be remembered that security is an evolving and changing practice and thus policies and procedures need to change too. Since users are presented with security decisions they are unable to make an informed choice about (such as pop-up windows and automatic downloads when using the Internet), there is much to be gained by using non-intrusive and transparent security features in software and systems, that can be pre-set for a specific environment [8]. Currently, education and awareness of security, and what the consequences are, is the only method open to improve security use, in common software products at least. Ultimately, the user needs to not only 'feel' protected but be assured they have the necessary security in place for the risk they are prepared to carry. "It is now widely accepted that security requirements cannot be addressed by technical means alone, and the chances of success will be significantly influenced by the people involved" [36].

A lack of fundamental security measures by Australian practices are a precarious gap in the security of medical data. However, there are basic countermeasures that can be implemented with little knowledge of security matters. Medical practitioners understand their medical and business environment well, and this is what such measures should be based upon. Further, it is clear that future research must aim to increase the awareness of medical practices to the risks in information security, yet in the meantime putting in place fundamental actions will go a long way to protecting the most valuable assets of a practice.

7 References

- [1] A. Cook, P. Schattner, and C. Pleteshner, "The experiences of one divisional group of GPs in introducing computers into clinical practice" *Australian Family Physician*, vol. 28, pp. 971-975, 1999.
- [2] S. Petersen, "Time for evidence based medical education," *British Medical Journal*, vol. 318, pp. 1223-1224, 1999.
- [3] S. Martin, "Younger physicians, specialists use Internet more," *Journal of the Canadian Medical Association*, vol. 170, pp. 1780, 2004.
- [4] T. J. Spyt, P. A. C. Watt, M. C. Boehm, and P. R. Stafford, "Online patient support systems - is there a need?", *British Journal of Clinical Governance*, vol. 7, pp. 250-254, 2002.
- [5] P. A. H. Williams and S. P. Maj, "Drowning or waving? Is the Internet the lifebuoy for Australian General Practitioners drowning in a sea of reference material?", in *Proc. eHealth: a Futurescope. Third International Conference on Advances in the Delivery of Health Care*, London: City University, 2001.
- [6] P. A. H. Williams and S. P. Maj, "Is the internet an integral part of general practice in Australia?", in *Proc. Medinfo2001 Congress. Towards Global Health: The Informatics Route to Knowledge*, London, 2001.
- [7] NEHTA. (2006). *National e-health standards development: A management framework*. [Online]. Available http://www.nehta.gov.au/component/option,com_frontpage/Itemid,1/
- [8] S. Furnell, "Why users cannot use security", *Computers & Security*, vol. 24, pp. 274-279, 2005.
- [9] P. A. H. Williams, "The underestimation of threats to patient data in clinical practice", in *Proc. 3rd Australian Information Security Management Conference*, Edith Cowan University, Perth, WA, 2005, pp. 117-122.
- [10] D. Lewis, "Keeping the doors open," *Computer technology review*, vol. 23, pp. 32, 2003.
- [11] R. L. Jones, "The Internet and healthcare information systems: How safe will patient data be?", *IS Audit & Control Journal*, vol. 2, pp. 25, 1998.
- [12] C. E. Gilkes, M. Casimiro, A. W. McEvoy, R. MacFarlane, and N. D. Kitchen, "Clinical databases and data protection: Are they compatible?," *British Journal of Neurosurgery*, vol. 17, pp. 426, 2003.
- [13] G. Holzer and N. Herrmann. (2002) *Informatics survey for practice managers*. SA Divisions of General Practice. [Online]. Available http://www.sadi.org.au/survey/Practice_Managers_Survey_2002.pdf.

- [14] C. P. Pfleeger, *Security in computing*, 2nd ed. Upper Saddle River, NJ: Prentice Hall, 1997.
- [15] M. Gerber and R. von Solms, "Management of risk in the information age," *Computers & Security*, vol. 24, pp. 16-30, 2005.
- [16] F.-A. Allaert, B. Blobel, K. Louwerse, and B. Barber, "Security standards in healthcare information systems: A perspective from the EU ISIS MEDSEC project," in *Studies in Health Technology and Informatics*, vol. 69, J. P. Christensen, A. Hasman, L. Hunter, and e. al., Eds. Amsterdam, Netherlands: IOS Press, 2002, pp. 240
- [17] P. Schattner. (2005). *The GPCG computer security self-assessment guideline and checklist for General Practitioners*. Department of General Practice, Monash University, East Bentleigh, Victoria, Australia .
- [18] J. P. Tomes, "Prescription for Data Protection," *Security Management*, vol. 49, pp. 75-77, 2005.
- [19] *Information security management—Implementation guide for the health sector*, Standards Australia HB 174—2003, 2003.
- [20] E. Terado and P. A. H. Williams, "Securing PDAs in the healthcare environment," *Journal of Information Warfare*, vol. 4, pp. 61-68, 2005.
- [21] J. C. Frenzel, "Data security issues arising form integration of wireless access into healthcare networks," *Journal of Medical Systems*, vol. 27, pp. 163-175, 2003.
- [22] A. Woodward, "Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations", in *Proc. 3rd Australian Information Security Management Conference*, Perth, Western Australia, 2005, pp. 133-140.
- [23] J. Aiken. (1999). *Proposed bills would restrict access to medical records*. [Online]. Available <http://www.cnn.com/ALLPOLITICS/stories/1999/04/27/medical.records/>
- [24] Commonwealth Department of Health and Aged Care. (2000). *The benefits and difficulties of introducing a national approach to electronic health records in Australia: Report to the Electronic Health Records Taskforce*. [Online]. Available http://www.healthconnect.gov.au/pdf/ehr_apxb.pdf
- [25] M. Carter, "Integrated electronic health records and patient privacy: possible benefits but real dangers," *Medical Journal of Australia*, vol. 172, pp. 28-30, 2000.
- [26] S. S. Ariss, "Computer monitoring: benefits and pitfalls facing management," *Information & Management*, vol. 39, pp. 553-558, 2002.
- [27] C. Vroom and R. von Solms, "Towards information security behavioural compliance," *Computers & Security*, vol. 23, pp. 191-198, 2004.
- [28] T. J. Owens, S. Tachakra, K. A. Banitsas, and R. S. H. Istepanian, "Security a medical wireless LAN system", in *Proc. 23rd Annual EMBS International Conference*, Istanbul, Turkey, 2001, pp. 3552-3555.
- [29] The Joint General Practice Information Technology Committee of the General Practitioners Committee and the Royal College of General Practitioners. (2005). *Good practice guidelines for general practice electronic patient records - July 2005*. Department of Health & Royal College of General Practitioners. [Online]. Available <http://www.dh.gov.uk/assetRoot/04/11/67/07/04116707.pdf>
- [30] J. Johnston, J. H. P. Eloff, and L. Labuschagne, "Security and human computer interfaces," *Computers & Security*, vol. 22, pp. 675-684, 2003.
- [31] S. Posthumus and R. von Solms, "A framework for the governance of information security," *Computers & Security*, vol. 23, pp. 638-646, 2004.
- [32] K.-L. Thomson and R. von Solms, "Information security obedience: a definition," *Computers & Security*, vol. 24, pp. 69-75, 2005.
- [33] J. Leach, "Improving user security behaviour," *Computers & Security*, vol. 22, pp. 685-692, 2003.
- [34] R. von Solms and B. von Solms, "From policies to culture," *Computers & Security*, vol. 23, pp. 275-279, 2004.
- [35] R. LeVine, "Technology evolution drives need for greater information technology security," *Computers & Security*, vol. 24, pp. 359-361, 2005.
- [36] S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," *Computers & Security*, vol. 25, pp. 27-35, 2006.