12-4-2007

Medical insecurity: when one size does not fit all

Patricia A. Williams
Edith Cowan University

DOI: 10.4225/75/57b556dcb8766
5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

Medical insecurity: when one size does not fit all

Patricia A H Williams
Edith Cowan University,
trish.williams@ecu.edu.au

Abstract

Security is most commonly seen as a business concept. This is one reason for the poor uptake and implementation of standard security processes in non-business environments such as general medical practice. It is clear that protection of sensitive patient information is imperative yet the overarching conceptual business processes required to ensure this protection are not well suited to this context. The issue of sensitivity of information, together with the expectation that security can be effectively implemented by non-security trained professionals creates an insecure environment. The general security processes used by business, including those for risk assessment, are difficult to operationally put into practice in the medical environment and this one-size-fits-all approach is shown to be ineffective. Therefore more explicit models are required which provide contextually relevant guidance and can be implemented within the capability of those using them.

Keywords

Medical informatics, information security, models.

INTRODUCTION

Health care is an information intensive industry, which increasingly recognizes the importance of information in managing patient care (Spil, Stegwee, & Teitink, 2002). In particular, general medical practice presents a complex work setting in which there is a lack of time and increasing pressure to record the details of every interaction and activity. Information technology has long been seen as a panacea for these problems. In Australia there has been an increase in the use of information technology for such clinical purposes from only 15% in 1997 to 95% in 2006 (Henderson, Britt, & Miller, 2006). Despite this increase general practitioners still distrust computer systems and their ability to be able to provide the single solution for connecting all health information, which is a key objective for a government seeking to transform Australia's health-care system (HealthConnect, 2005). Among the reasons for this distrust are inadequate levels of knowledge of the technology being used, together with privacy and security issues (Henderson, Britt, & Miller, 2006; Tzelepi, Pangalos, & Nikolacopoulou, 2002).

Research has shown that communication facilitated by, but not replaced by, technology and networking plays an intrinsic part in patient care (Coiera & Tombs, 1998). Yet progression in the use of information communication techniques is hampered by interruption of workflow and reticence to adopt new computing and communication technology. This can be attributed to the potential impact error which is more serious in the health care setting than elsewhere. Health information systems are therefore a combination of human and technical interaction and cannot be considered independently (Lorenzi, 2004). As many researchers have identified, it is not the technology itself that poses the problem but the effective use of the technology (Furnell, 2005). Consequently, it is the socio-technical perspective that needs further consideration and development if innovative technologies are to be widely adopted. In the development of sophisticated computing and information communication systems, existing risks have changed in formulation but the "tenets of security and control still remain nearly the same, its 'how to' dimension has undergone radical changes" (Raval & Fichadia, 2007).

A combination of the environment in which medical security is considered, together with a lack of ability of those in this environment to effectively implement appropriate security measures (Williams, 2008), implies a complexity in applying security in the medical context which is unavoidably greater than similar application in a business oriented environment. The business environment in general is better structured to cater for IT initiatives, inclusive of security, than medical practices.

This paper investigates the problems inherent in providing adequate information security in an environment that places a high value in trust yet concurrently is driven by technology which contradicts this. In exploration of this topic, the acquisition, use and dissemination of information is not considered, rather the implementation and use of information security measures in medical practice are the primary area of importance. The paper does not discuss details of specific information security measures nor specific potential vulnerabilities or attacks. Further,

information security is considered in light of electronic based information rather than that of paper-based records. In essence the use of typical security and risk assessment procedures do not lend themselves to easy implementation in the medical environment. A one-size-fits-all approach has significant drawbacks creating insecurity in an environment that demands effective protection.

SECURITY DEFINED

From a technical perspective security is viewed in terms of strategic, tactical and operational goals. Whilst commonly understood by the security and business professions, these terms have different connotations in the medical profession. In both the computing and the security field it is common to use these terms when referring to core business processes. However, use of these terms needs to be contextualised as such terms do not have a consistent place in the medical environment.

The complete process of information security includes objectives and associated strategy that define policy, which in turn delineates the processes required, which in turn is deconstructed into specific procedures (Figure 1.1). This process provides for the maximum level of security to be defined based upon the strategic objectives.

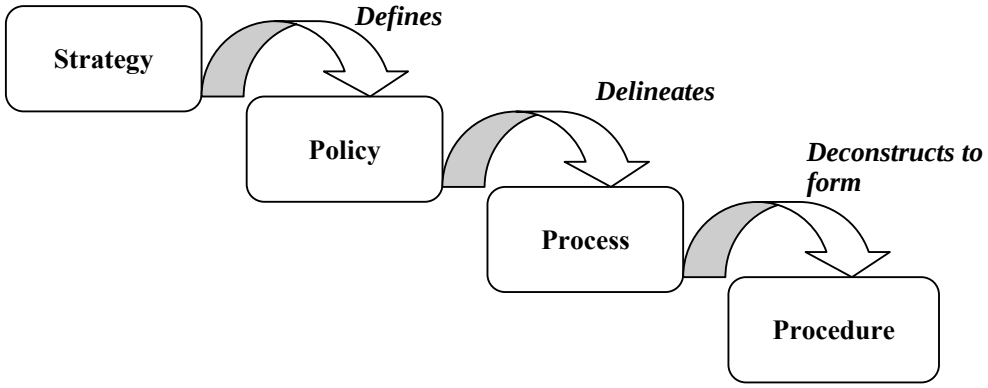

Figure 1.1 The complete process of information security

Each community of practice has different requirements. The medical environment has specific and demanding requirements which must be met legally, professionally and ethically. A holistic view of information security is therefore required in this context. Failure to provide this may result in increasing security breaches, litigation, compromises in quality of patient care and potentially even loss of life. Given the nature of the general medical practice environment, a holistic approach must have the ability to be implemented by the practice itself and address the differences in motivation, capability and ability therein. Therefore, using the conceptual processes in this model could decrease the time spent in duplicating and redeveloping policy and procedures, standardise management, save time in new staff training and orientation and address the information security risk management issues as technology evolves and societal and legal expectations change (Bachman & Malloch, 1998). In order to do this it is first necessary to obtain a clear understanding of exactly what security means in the medical context.

Security is defined as "the safety of a state or organisation against criminal activity such as terrorism" and being "certain to remain safe and unthreatened; protected against attack or other criminal activity" (Pearsall, 1999, p.1295). Further, from a computer science perspective this includes accidental incidents and natural disasters. In terms of information security this is approached using combinations of strategies encompassing physical, personal, operational, communications and network security measures. Security is based on three critical characteristics which are confidentiality, integrity and availability, also known as the three pillars of security (Pfleeger, 1997). As such, information is open to generalised threats which include errors and omissions, theft and fabrication, sabotage, espionage, loss of availability, hackers, malware, and breaches of privacy and confidentiality.

Confidentiality is the core principle of most security policy medical or other and is concerned with access to information by authorised individuals. A breach of confidentiality is when unauthorised access to information occurs. As such access to information must be strictly controlled according to legal and ethical considerations to ensure that patient information is accessed by authorised and authenticated personnel. Therefore, the confidentiality of patient information refers to the obligation by the health care practitioner not to disclose information given by the patient or resulting from examination of the patient, to any other person or

organisation, without first obtaining patient consent (Holloway, 2004). Further, the medical practitioner is given the responsibility to grant secondary access to patient information as the patient fiduciary and can grant temporary access in emergencies. Therefore the issue of access in the medical environment needs to be sophisticated to allow only legitimate access. Privacy is a facet of confidentiality which delineates that the information collected, used and stored, should be used only for the specified stated purpose for which it was collected. This is in contrast to confidentiality and observation of information, as privacy relates to the use of information, subject to the knowledge of the person providing that information (Joshi, 2003). The traditional view of confidentiality is increasingly under question as health problems in individual patients become complex and requires multiple healthcare providers' involvement. The once overarching Hippocratic Oath,

> What I may see or hear in the course of the treatment, or even outside of the treatment in regard to the life of men, which on no account must one spread abroad, I will keep to myself holding such things shameful to be spoken about. Extract from the Hippocratic Oath (Holloway, 2004)

becomes increasingly difficult to adhere to in the emerging electronic modern practice of medicine and presents new ethical dilemmas for medical practitioners (Davis, Domm, Konikoff, & Miller, 1999). Thus, access control is a multifarious matter and policy rules may be role based, task-based, content based or context-based.

The second pillar, integrity, is concerned with the quality and correctness of information. Information may be exposed to corruption, destruction, incompleteness and falsification which affect the integrity of that information. For reasons of patient safety, corruption of medical information is a serious issue, as is the prevention of binding or merging of patient information with other information. Whilst important for all data types, integrity is particularly important in the case of electronic medical images as corruption or alteration of data may be difficult to detect (Tzelepi, Pangalos, & Nikolacopoulou, 2002). Further, integrity includes the premise that information is only altered by authorised people (authentication) and that this authentication is reliable and ensures non-repudiation.

The third pillar, availability, is concerned with ensuring that information is provided to authorised users at the time it is required. System reliability and reliability of access are both elements of availability. In the medical environment, access to information is essential to the continuity of patient care in an environment which is becoming increasingly dependent on sharing of information.

It could be argued that medical information systems are subject to the same security issues, vulnerabilities and threats that any other information systems are open to. Whilst this may hold true in principle, the medical environment presents other unique characteristics, particularly in relation to confidentiality and privacy that other business environments do not.

Contextual differences

The public and even many health care professionals, perhaps out of a lack of understanding of security principles and practices, assume that the high ethical standards expected of health care personnel are enough of a deterrent to the misuse of patient information in all but exceptional cases. This view is contradicted by the fact that medical records are routinely available to non-medical personnel for essential business functions such as claim payment processing. Moreover, medical information has concrete monetary value to other stakeholders than the health care provider (Ateniese, Curtmola, & de Medeiros, 2002).

Security for general practice is bound by information that is contained within a practice and does not include the application of that information independently. For instance electronic prescribing is a major activity in patient management and as such has been the focus of both research (Adkins, 1997; Dufour, Fieschi, & Fieschi, 2004; Mundy & Chadwick, 2003) and government objectives (Medicare Australia, 2007). The problems in specific aspects of information usage such as information transfer to other health providers and the protection of information taken outside the practice facility such as health professionals taking information home (McLean & Anderson, 2004), email communications (Cook, Schattner, & Pleteshner, 1999; Kane & Sands, 2000; Mandl, Kohane, & Brandt, 1998) and use of the Internet (Coiera, 1996; Ilioudis & Pangalos, 2000) are not considered discretely and are seen as inclusive of information security practice.

Core professional activities

In a wider electronically connected environment, such as global electronic health records, the threats and risks may be considered overrated in comparison to the benefits (Carter, 2000). However, the responsibility for the protection of information will always return to the assurance of confidentiality and privacy afforded to the individual patient, and as such the risks cannot be ill-considered despite any potential benefits. Therefore, the process of being informed in an area that is not one's core profession, such as information security for medical

practitioners, requires both an appreciation of the wide range of threats for which information is exposed and a grounding in the responsibilities associated with this. Consequently, an assessment of potential risk and appropriate protection must be undertaken. The general practice environment needs relevant guidance that is useful to both practitioners and practice managers, and that demonstrates the need for adherence to requisite information security standards and principles. This requires a fusion of information security (i.e. standards and technical competence) with the patient-care oriented environment. The resulting union should bring clarity of purpose, in easy to understand terminology, with a clear and definitive structure.

To date, much of the research into information systems security is based on formal risk assessment, focussing on the origin of risks to inform model development and subsequent mitigation strategies (Misra, Kumar, & Kumar, 2007). Whilst this form of assessment may be useful, it does not address the current problems of information security implementation and subsequent understanding of vulnerability in the medical context. The primary concern of general medical practice is the welfare and treatment of patients and not the security of the information systems infrastructure. The problem of balance between information security and the core industry processes is not uncommon in other environments such as e-commerce (Hutter, Mantel, Schaefer, & Schairer, 2007), organisational coordination (Boella & van der Torre, 2006) and any web based environment (Lacohee, Phippen, & Furnell, 2006). Such is the magnitude of the problem in a ubiquitous computing world that mathematical modelling of reliance on computing trust rather than human trust for security situations is being developed in order to keep pace with technology and its growing uses (Kallath, 2005; Nielsen, Krukow, & Sassone, 2007). Hence research which extends into natural language application of policy and management of information security in order to ensure information governance particularly in the medical setting is required (Becker, 2007).

ONE-SIZE FITS ALL?

It is crucial to provide suitable overall security processes to support and enable secure delivery of information in modern medical practice. Breaches in medical information security are well documented (Anonymous, 2003; "Leaders: Hot data; Data protection", 2005; Neame & Kluge, 1999). As with other areas of society and business, understanding the specific security issues is a necessity if risk management and countermeasures are to be effective. There is no 'one size fits all' solution (Brill & Leetz, 2005; Kates, 2001). As Fox (1998) suggests the role of security has changed "boundaries between trusted and untrusted entities are harder to distinguish". In situations where a blanket approach to security has been put into practice, serious concerns have been cited, suggesting that such security is unworkable and adversely affecting the use of technology for health communication (McAlearney, Schweikhart, & Medow, 2004; Terado & Williams, 2005). Further, there is increasing recognition of specific threats to information due to flaws in countermeasure implementation (Valli, 2006a, 2006b; Woodward, 2006). These problems are not peculiar to the medical environment. Traditional approaches to information security tend to be monolithic. This approach works to increase the knowledge of everyone in the organisation relying on the premise that awareness in a basic level of security will result in better security protection for the organisation (Valentine, 2006). However, such assumptions are rapidly being proven obsolete as the following discussion highlights.

Failure of a universal approach

There is considerable literature on the failure of the traditional universal approach to information security. Examples include exposure of sensitive information (Jones, 2006), e-commerce content interception (Wright, 2001) and many breaches of security (AHA Insurance Resource, 1999; Ammenwerth, Iller, & Mahler, 2006; AusCert, 2006; Hayes, 2004; IT Governance Institute, 2006). These provide examples of where a blanket approach to information security has failed to identify potential vulnerabilities.

The success of government funded monolithic programs is also questionable such as the US-CERT (Department of Homeland Security, 2003), the UK Information Technology Security Awareness for Everyone (ITSafe) (HM Government, 2007) and the Get Safe Online ("Get Safe Online", 2007). These are touted as national solutions to security of information issues, however the ITSafe program and the US-CERT purport to address the protection of critical national infrastructure while providing little more than newsletters, documents on information security and email alerts of virus and Microsoft and Apple operating system vulnerabilities and fixes. The 'Get Safe Online' project is a cursory ten-minute guide to Internet information security also designed for home and small business. As they are these initiatives do little to address the real potential problems of information security and their effectiveness is difficult to measure. Further, it is the nature of information security to be an evolving and shifting target that is difficult even for the security professions to keep up with. Clearly customisable solutions for distinct environments are needed.

Further, standards such as US National Institute for Standards and Technology (NIST, n.d.) provide a comprehensive overview of information security represented by numerous security measures and their

relationship with one another. NIST provides a broad overview of information security to assist in understanding the topic and discusses the benefits of security controls. It is comprehensive although general in nature, and specifically excludes details on how to implement a security program or to adapt it for a particular context. However NIST acknowledges that reliable information security must be easy to use, in that it has a higher probability of usage if it is seamless and easy to implement. The Organisation for Economic Co-operation and Development (OECD) paper (2002) concurs with this view that it is the creation of a security culture to protect information systems and networks which suggests using social constructs rather than technical ones. It bases its guidelines on nine complementary principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment. The OECD recommended that the policies and security measures should be ethically and socially driven.

Consequences

As the increasing inadequacy of the one-size-fits-all approach is realised, and as information security issues become philosophically too grave to ignore, an opposing isolated approach to information security has developed, for instance where only access control is addressed or database integrity is considered. These specific approaches too have problems in their complex nature and inability to be easily implemented. Universal approaches to information security in the medical environment which enforce outside views of information security onto an area which is highly patient care focused, and does not tolerate well interruptions in workflow, will not be successful. If a more relevant approach is not adopted then growing vulnerabilities of medical information systems will emerge. The consequence of this could be a significant increase in breaches of confidentiality and privacy of information contained in medical information systems. There is no doubt that changes in technology have resulted in considerable changes in medical care, diagnosis and therapeutics. Information technology and its associated technologies such as high speed networking are being adopted progressively for "crucial clinical activities instead of being restricted to support activities, [and with this] there is an increasing risk that security breaches will occur that can have significant effects on the delivery of patient care" (Barber, Louwerse, & Davey, 1998). A significant information security issue in terms of availability would be apparent if for instance there was a loss of networking bandwidth during a critical telemedicine consult as a result of network malfeasance such as denial of service or bandwidth stealing.

Further, as in the business environment, increasing accountability in addition to the basic medical premise of confidentiality will become important. This accountability includes proof of appropriate use of information, its integrity, availability and accuracy, declared responsibility for the information and the tracking of disclosures of information. The consequences of poor information security in this context have the potential to be more fundamentally detrimental to patients than monetary based business breaches (Ferreira et al., 2004). For instance, lack of availability of clinical information in situations where acute or emergency care is required can have fatal consequences. Approaches that assist successful information security implementation in the medical environment are increasingly needed as the medical profession becomes more reliant on information technology. The issue is not restricted to a specific medical practice rather it needs acknowledgement of the wider environment in which it operates. The information systems used in the medical environment are dependent upon both the critical technological and general infrastructure including power, water and transport. Whilst the individual practice may not have control over the security of this infrastructure, a failure of it will impact the medical practice's function. Examples of this can be as devastating as natural disasters and the September 11 attacks to a more mundane burst water main outside the practice premises. Thus information security, accountability and business continuity is about planning for the impact of such events.

If this need for a governance approach to information security is not met, then perhaps the security profession is negligent in its responsibility to other professions. Ultimately, the result will be increased litigation against the medical profession itself, as this is where the accountability as executor of the patient record is retained. Further, the adoption of electronic medical records, the push to share local and national patient information and the increased use of the Internet will change the nature of information security problems. Current information security solutions and practices may no longer provide effective solutions in a distributed clinical record environment (Redman, Warren, & Hutchinson, 2005). If such changes are not catered for in this unbounded computing environment it may have serious effects on confidentiality, privacy and integrity of patient information as well as affecting availability, and ultimately patient care.

CONCLUSION

The medical environment is arguably more complex than other people-centred environments, which is due in part to the sensitivity of the information collected, stored, manipulated and utilised. One distinct issue is that as healthcare security practitioners, "we write for security specialists when we want to be read by practising clinicians and administrators. When we can communicate in such a way that addresses the use of the computer

as a tool to clinical practice then perhaps they will listen" (Allaert, Blobel, Louwerse, & Barber, 2002, p.ix). What is needed is an easily understood guide to good clinical information security practice that provides sound, low cost solutions to improve information security of clinical practice information. In the medical environment, information security threats can range from mere inconvenience to seriously affecting the day-to-day operations in a medical practice. Whilst threats and breaches of information security may not prevent the medical practice functioning in its ability to provide patient care, it would cause inconvenience and affect the efficiency with which this is delivered. Such events can be costly as patient and other information are key assets of a medical practice in the 2000's. Loss of data, loss of reliability and integrity, or breaches of confidentiality can result also in efficacy and legal problems.

Solutions to the issues of information security in general medical practice are currently being developed. One potential solution is the Tactical Information Governance for Security (TIGS) model (Williams, 2007a) which provides the overarching framework upon which to meet the diverse yet comprehensive requirements of information security in terms of strategy, policy, process and identifies procedures. This model is accompanied by a capability framework that characterizes the development of procedures based upon capability within the medical practice (Williams, 2007b). This framework enables medical practice staff to manage the information security process themselves and attain self-actualization in correlation with Maslow's hierarchy of needs (Maslow, 1943). Maslow's work established that human beings seek to satisfy successively higher needs by prioritising higher achievement, provided that lower needs are satisfied. Indeed, Maslow's work has been applied to security previously in terms of specific measures as well as process (Grimes, 2006; Potter, 2005; Seath, 1993). Whilst business conceptual models can provide a good base from which to develop understandings, the one-size-fits-all approach lacks clarity of application for the general medical practice context where a framework for improvement that can be measured against policy, legal and professional requirements is essential if information security is to be managed and effective. Further development to construct a suite of capabilities that can be fitted into the TIGS model and allows for holistic model testing is being undertaken. Research is also being undertaken to investigate the extension of the TIGS model for inter-health service secure communication governance.

REFERENCES

Adkins, P. (1997). Harnessing and controlling the information deluge. *Australian Family Physician, 26*(1), 25-29.

AHA Insurance Resource. (1999). *AHA launches unique program to protect against information security risks*. Retrieved 14 August, 2005, from http://www.hospitalconnect.com/aha/key_issues/hipaa/privacy/ecomprehensive.html

Allaert, F.-A., Blobel, B., Louwerse, K., & Barber, B. (Eds.). (2002). *Security standards in healthcare information systems: A perspective from the EU ISIS MEDSEC project* (Vol. 69). Amsterdam, Netherlands: IOS Press.

Ammenwerth, E., Iller, C., & Mahler, C. (2006). IT-adoption and the interaction of task, technology and individuals: a fit framework and a case study. *BMC Med Inform Decis Mak, 6*(3), Published online

Anonymous. (2003). ID theft tops fraud list again. *ABA Bank Compliance, 24*(2), 5.

Ateniese, G., Curtmola, R., & de Medeiros, B. (2002). Medical Information Privacy Assurance: Cryptographic and System Aspects. *Third Conference on Security in Communication Networks 2002* Retrieved 26 June, 2006, from citeseer.ist.psu.edu/article/ateniese02medical.html

AusCert. (2006). *2006 Australian Computer Crime and Security Survey.* Retrieved 13 August, 2006, from http://www.auscert.org.au/images/ACCSS2006.pdf

Bachman, J. P., & Malloch, K. M. (1998). Developing a common nursing practice model. *Nursing Management, 29*(1), 26-27.

Barber, B., Louwerse, K., & Davey, J. (1998). White paper on health care information security. *ISHTAR White Paper* Retrieved 19 Jan, 2006, from http://ted.see.plymouth.ac.uk/ishtar/deliverables/white%20paper.html

Becker, M. Y. (2007). Information governance in NHS's NPfIT: A case for policy specification. *International Journal of Medical Informatics, 76*(5-6), 432-437.

Boella, G., & van der Torre, L. (2006). Coordination and Organization: Definitions, Examples and Future Research Directions. *Electronic Notes in Theoretical Computer Science, 150*(3), 3-20.

Brill, R., & Leetz, W. (2005, May 2005). *Security implementations in the healthcare enterprise.* Paper presented at the CARS 2005: Computer Assisted Radiology and Surgery, Berlin, Germany

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

Coiera, E. (1996). The internet's challenge to health care provision. *British Medical Journal, 312*, 3-4.

Coiera, E., & Tombs, V. (1998). Communication behaviours in a hospital setting: an observational study. *British Medical Journal, 316*(7132), 673-676.

Cook, A., Schattner, P., & Pleteshner, C. (1999). The experiences of one divisional group of GPs in introducing computers into clinical practice. *Australian Family Physician, 28*(9), 971-975.
Davis, L., Domm, J. A., Konikoff, M., & Miller, R. A. (1999). Attitudes of first-year medical students toward the confidentiality of computerized patient records. *Journal of the American Medical Informatics Association, 6*(1), 53.
Department of Homeland Security. (2003). US-CERT United States Computer Emergency Readiness Team. Retrieved April 20, 2007, from www.us-cert.gov
Dufour, J.-C., Fieschi, D., & Fieschi, M. (2004). Coupling computer-interpretable guidelines with a drug-database through a web-based system - The PRESGUID project. *BMC Medical Informatics and Decision Making, 4*(1), 2.
Ferreira, A., Correia, R., Antunes, L., Palhares, E., Marques, P., Costa, P., et al. (2004, 24-25 June 2004). *Integrity for electronic patient record reports.* Paper presented at the 17th IEEE Symposium on Computer-Based Medical Systems, 2004. (CBMS 2004).
Fox, B. (1998). "Cooperative Security": A Model for the New Enterprise [Electronic Version]. Retrieved 26 June 2006 from citeseer.ist.psu.edu/316968.html.
Furnell, S. M. (2005). Why users cannot use security. *Computers & Security, 24*(4), 274-279.
Get Safe Online. (2007). Retrieved April 20, 2007, from www.getsafeonline.org
Grimes, R. A. (2006). SECURITY ADVISER: The evolution of corporate security - As companies balance ease-of-use with security, they move up the steps of Grimes' Hierarchy of Security Needs [Electronic Version]. *InfoWorld*, 28, 9. Retrieved 12 May 2007 from Expanded Academic Index.
Hayes, S. (2004). *Software tools for risk analysis and management.* Retrieved November 1, 2005, from http://www.risksociety.org.nz/seminars/softwaretools.pdf
HealthConnect. (2005). *HealthConnect Implementation Strategy*. Version 2.1 6 July 2005. Retrieved November 1, 2005, from http://www.healthconnect.gov.au/pdf/implementation.pdf
Henderson, J., Britt, H., & Miller, G. (2006). Extent and utilisation of computerisation in Australian general practice. *Medical Journal of Australia, 185*(2), 84-87.
HM Government. (2007). *ITSafe: IT security warning service*. Retrieved April 20, 2007, from itsafe.gov.uk
Holloway, F. (2004). Confidentiality: threats and limits. *Psychiatry, 3*(3), 11-13.
Hutter, D., Mantel, H., Schaefer, I., & Schairer, A. (2007). Security of multi-agent systems: A case study on comparison shopping. *Journal of Applied Logic, 5*(2), 303-332.
Ilioudis, C., & Pangalos, G. (2000). Development of an Internet Security Policy for health care establishments. *Medical Informatics & The Internet in Medicine, 25*(4), 265 - 273.
IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2nd ed.). Rolling Meadows, IL, USA: IT Governance Institute.
Jones, A. (2006). Cradle to grave - security failure to the very end. *Computer Fraud & Security, 2006*(9), 4-8.
Joshi, J. B. D. (2003). *Chapter 1 Introduction to the Management of Information Security*. Retrieved 11 November, 2005, from www.sis.pitt.edu/~jjoshi/IS2820/Spring06/chapter01.doc
Kallath, D. (2005). Trust in trusted computing - the end of security as we know it. *Computer Fraud & Security, 2005*(12), 4-7.
Kane, B., & Sands, D. Z. (2000). *Guidelines for the clinical use of electronic mail with patients.* Retrieved 16 November, 2000, from http://www.amia.org/pubs/other/email_guidelines.html
Kates, J. (2001). The Reality of Hackers. *Risk Management, 48*(7), 50-57.
Lacohee, H., Phippen, A. D., & Furnell, S. M. (2006). Risk and restitution: Assessing how users establish online trust. *Computers & Security, 25*(7), 486-493.
Leaders: Hot data; Data protection. (2005). *The Economist, 375*(8432), 18.
Lorenzi, N. M. (2004). Beyond the gadgets. *British Medical Journal, 328*(7449), 1146-1147.
Mandl, K. D., Kohane, I. S., & Brandt, A. M. (1998). Electronic Patient-Physician Communication: Problems and Promise. *Ann Intern Med, 129*(6), 495-500.
Maslow, A. H. (1943). A Theory of Human Motivation [Electronic Version]. *Psychological Review*, 50, 370-396. Retrieved 14 May 2007 from http://psychclassics.yorku.ca/Maslow/motivation.htm.
McAlearney, A. S., Schweikhart, S. B., & Medow, M. A. (2004). Doctors' experience with handheld computers in clinical practice: qualitative study. *British Medical Journal, 328*, 1162.
McLean, I., & Anderson, C. M. (2004). The security of patient identifiable information in doctors' homes. *Journal of Clinical Forensic Medicine, 11*(For), 198-201.
Medicare Australia. (2007*). Practice Incentives Program.* Retrieved April 09, 2007, from http://www.medicareaustralia.gov.au/providers/incentives_allowances/pip/new_incentives/im_it.shtml
Misra, S., Kumar, V., & Kumar, U. (2007). A strategic modeling technique for information security risk assessment. *Information Management & Computer Security, 15*(1), 64-77.
Mundy, D. P., & Chadwick, D. W. (2003). Security issues in the electronic transmission of prescriptions. *Medical Informatics & The Internet in Medicine, 28*(4), 253 - 277.

Neame, R., & Kluge, E.-H. (1999). Computerisation and health care: some worries behind the promises. *British Medical Journal, 319*(7220), 1295.
Nielsen, M., Krukow, K., & Sassone, V. (2007). A Bayesian Model for Event-based Trust. *Electronic Notes in Theoretical Computer Science, 172*, 499-521.
NIST. (n.d.). *An Introduction to Computer Security:The NIST Handbook* (No. Special Publication 800-12): National Institute of Standards and Technology.
OECD. (2002). *OECD guidelines for the security of information systems and networks: Towards a culture of security*. Paris: Organisation for Economic Co-operation and Development.
Pearsall, J. (Ed.). (1999). *The concise oxford dictionary* (Tenth ed.). Oxford, England: Oxford University Press.
Pfleeger, C. P. (1997). *Security in computing* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.
Potter, B. (2005). IT security needs hierarchy. *Network Security, 2005*(5), 14-15.
Raval, V., & Fichadia, A. (2007). *Risks, controls and security: Concepts and applications*. USA: John Wiley & Sons.
Redman, J., Warren, M., & Hutchinson, W. (2005). System survivability: a critical security problem. *Information management & computer security, 13*(2/3), 182.
Seath, I. (1993). Turning theory into practice. *Managing Service Quality*, 35-37.
Spil, T. A. M., Stegwee, R. A., & Teitink, C. J. (2002). *Business intelligence in healthcare organisations.* Paper presented at the 35th Hawaii International Conference on System Sciences (HICSS-35'02), Hawaii
Terado, E., & Williams, P. A. H. (2005). Securing PDAs in the healthcare environment. *Journal of Information Warfare, 4*(1), 61-68.
Tzelepi, S., Pangalos, G., & Nikolacopoulou, G. (2002). Security of medical multimedia. *Medical Informatics & The Internet in Medicine, 27*(3), 169 - 184.
Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud and Security, June*, 17-19.
Valli, C. (2006a). *The Insider Threat to Medical Records; Has the Network Age Changed Anything?* Paper presented at the 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing - SAM'06 - The 2006 International Conference on Security & Management, Monte Carlo Resort, Las Vegas, Nevada, USA (June 26-29, 2006)
Valli, C. (2006b). *SQL Injection - Threats to Medical Systems; Issues and Countermeasures.* Paper presented at the 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing - SAM'06 - The 2006 International Conference on Security & Management, Monte Carlo Resort, Las Vegas, Nevada, USA (June 26-29, 2006)
Williams, P. A. H. (2007a). Information governance: A model for security in medical practice. *Journals of Digital Forensics, Security and Law, 2*(1), 57-72.
Williams, P. A. H. (2007b). A practical application of CMM to medical security capability. *Information Management & Computer Security, [Under review]*.
Williams, P. A. H. (2008). When trust defies common sense. *Health Informatics Journal 14*(3), (accepted for publication June 2007).
Woodward, A. (2006). Data Confidentiality and Wireless Networks: Mutually Exclusive? In H. R. Arabnia & S. Aissi (Eds.), *The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing - SAM'06 - The 2006 International Conference on Security & Management* (pp. 404-409). Monte Carlo Resort, Las Vegas, Nevada, USA (June 26-29, 2006)
Wright, A. (2001). Controlling Risks of E-commerce Content. *Computers & Security, 20*(2), 147-154.

COPYRIGHT