2005

The underestimation of threats to patients data in clinical practice

Patricia Williams
Edith Cowan University

The Underestimation of Threats to Patient Data in Clinical Practice

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

Abstract

Issues in the security of medical data present a greater challenge than in other data security environments. The complexity of the threats and ethics involved, coupled with the poor management of these threats makes the protection of data in clinical practice problematic. This paper discusses the security threats to medical data in terms of confidentiality, privacy, integrity, misuse and availability, and reviews the issue of responsibility with reference to clinical governance. Finally, the paper uncovers some of the underlying reasons for the underestimation of the threats to medical data by the medical profession.

Keywords

Medical informatics, security, data protection, access control, confidentiality.

INTRODUCTION

"The healthcare industry has historically lagged behind other industries in its understanding of information security issues and the funds expended for adequate information security programs. Information systems (IS) audit and security professionals will have a greater challenge on their hands to help those organizations protect the confidentiality, integrity, and availability of clinical, financial and human resource information." (Jones, 1998). The advances in computer and communications technology have increased the awareness of the susceptibility of sensitive patient information to breaches of privacy and confidentiality (AHA Insurance Resource, 1999). Also, navigating the various legislative changes in individual countries is proving difficult for the physician responsible for protection of patient data (Gilkes, Casimiro, McEvoy, MacFarlane, & Kitchen, 2003). The use of legislation to protect the privacy and confidentiality of patient information promotes the notion of accountability. However, it has been suggested that they should instead be promoting improved sharing, management and communication of information (Meredith, 2005). Whilst the law is seen as a protective tool it should also allow a more open approach to the use of information. Patient information is used for much more than individual patient health status management; it is used to inform future clinical practice; to plan health services; and as a clinical research and evaluation base (Black, 1999). More importantly, to be able to inform clinical practice and other research activities, patient information must be accurate and complete.

A review of the literature reveals that there are few publications on the adequate protection of medical data, whilst there are numerous reviews on how confidentiality affects medical practice and how legislation should be interpreted. Whilst most countries are still in the stages of discussing the importance of confidentiality, few have answers as to how to approach it. This leaves the question as to why the security of medical data is poorly performed. Perhaps, like other information dependent industries, "data security seems like a costly and boring chore" ("Leaders: Hot data; Data protection," 2005). Alternatively, perhaps it is too hard an area to tackle, or that the once protective culture of trust in handling medical information still holds strong.

THREATS TO MEDICAL DATA

As in any field, security of medical data can be defined as affecting:

- Confidentiality, accessible by authorised personnel only;
- Integrity, ensuring assets modified by authorised parties only (also includes accuracy); and
- Availability, ensuring accessibility by authorised users, when required. (Pfleeger, 1997)

These issues must be viewed from the physical, data related and management perspectives. The physical threats may incur data loss however physical security concerns are widely discussed in texts on computer security and related publications (Dennis, 2002; Pfleeger, 1997). The issues of physical security are the same as for any open access environment. However, confidentiality and privacy are primary concerns for medical data, as are the integrity, misuse and availability of the information.

Confidentiality and Privacy

Firstly, it is important to understand the difference between confidentiality and privacy as the terms are often used synonymously, although incorrectly. Confidentiality can be defined as "entrusted communication of information which is considered private and implies an ethical or legal principle" (Centre for Cancer Education, 1998a), whilst privacy is defined as "the state of being free from intrusion or disturbance in one's private life or affairs" (Centre for Cancer Education, 1998b). Broadly speaking, confidentiality in medicine refers to the non-disclosure of personal information without consent, whereas privacy is associated with identification of an individual from data or information. "Maintaining patient confidentiality and obtaining the consent of patients to share information about themselves are core principles of the medical profession" (Chester, 2003). This premise is being threatened as the requirement to keep copious notes, in order to meet both government reporting requirements and for potential information sharing, poses risks in patient information disclosure without consent.

In Australia, legislation has been inadequate in terms of protection of health information (Williams, 2005). This is confirmed by the report of the Australian Health Information Council where privacy legislation is being revisited and patient consent regarding shared information is being opened to public debate (ICTSC, 2004). An added level of complexity exists in Australia where public and private health providers are working together in the national health system. This creates confusion under which rules and regulations each provider is working under.

The discussion on confidentiality also includes the rights of patients and what they should be allowed to see. As Meredith (2005) points out, there are questions over patient rights to view information that may be harmful to them or received from third party health providers. This highlights yet more complexity on ownership of records, the right to view and use information, and information sharing. Given that in the UK a revised confidentiality code of practice emphasises informing patients of the use of their data, and that most people seem uninterested in the issue, perhaps the efforts put into confidentiality would be better put to ensuring patients are aware of their rights about data (Adams, Budden, Hoare, & Sanderson, 2004). However, other studies report that whilst "data protection and information sharing issues are poorly understood by doctors, but of vital importance to patients" (Pati, 2004).

To address some of the issues in privacy the Australian Health Ministers' National Health Privacy Working Group is developing a National Health Privacy Code. Where sensitive personal information is recorded, "privacy is a fundamental principle underpinning quality health care", and the proposed code is designed to "safeguard the health privacy and dignity of all individuals; achieve national consistency in health privacy protection - across jurisdictions and between the public and private sectors; and take into account changes in the way personal health information is handled as a result of technological change" (Commonwealth Department of Health and Ageing, 2004). The technological changes leading to electronic communication and EMR have brought a fresh set of challenges in maintaining privacy. The benefits of increased access to information for the patient must be weighed against the increased privacy risks (ICTSC, 2004).

Public Health

Public health and epidemiological research are areas which may cross the boundaries of privacy although not always confidentiality. "Public health is the arena in which clinical medicine, epidemiology, management, politics, and the law all meet—or perhaps more accurately, collide." (Lyons et al., 1999). Indeed, there have been suggestions that public health will suffer from the increasing limitation of data protection legislation (Lawlor & Stone, 2001). It becomes the traditional debate of the good of the patient versus the good of society. As Strobl, Cave and Walley (2000) suggest significant amounts of research, both epidemiological and in health economics, would not be possible if only completely de-identified data were used. The accuracy of this research depends on linking of data using codes, although not necessarily identifying individuals. Patient consent is usually the concern in matters of public health research. Arguably it is in all our interests to protect the general population against infectious disease, however to do this, confidential data is needed for which it is not always possible to obtain consent. Therefore, privacy may be maintained but the premise of confidentiality may be compromised as data is passed on without consent (Turnberg, 2003). Clearly epidemiological health research has many issues that need resolving in relation to the use of patient data and obtaining consent. Debate on confidentiality and the wider public gains using individual patient data are yet to be well thought-out (Ward et al., 2004).

Other issues: criminal or carelessness.

Although not such as obvious an issue is the maintenance of confidentiality and privacy when residual files has been left on a hard disk, or deleted files are recovered. Data recovery from hard disk crashes and corruption is possible using data recovery services or home software tools (Steers, 2005). The threat therefore exists of careless disposal and recovery of files with criminal intent. There have been numerous occurrences of private and confidential data being left on computer hard disks that have subsequently been on sold or reused, in which the receiver has been able to reconstitute the residual data on the disk (Evers, 2005). Such data protection concerns should not be overlooked in either the physical or ethical sense.

Integrity and misuse

Integrity, loss and misuse of data are also key issues in the medical environment. The movement of data in a paper based system has the potential for loss, particularly if there are multiple health care providers involved. There are some provisions for protection of paper based records which disappear in the electronic environment. The ability to lock information away one place and control individual access is more straightforward. Likewise, the custodian of the paper based records has an acute understanding the confidential nature of those records, whereas once the information is replicated and disseminated more widely the responsibility understanding can become diluted. The Australian Health Information Council points out that the infrastructure and standards that are used for paper-less transfers of data must ensure the integrity and modification process of that data (ICTSC, 2004). Authentication and non-repudiation are essential to these procedures.

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 (Aiken, 1999; Commonwealth Department of Health and Aged Care, 2000). Technology unfortunately does not have all the solutions to data misuse and loss. Health providers have a significant number of data security related occurrences each year, some of this is attributed to the lack of importance staff place on adhering to security policy and procedure (Carter, 2000).

Another consideration to the integrity of data is the way in which new wireless technologies are used. With the arrival of the personal digital assistants (PDA) and the tablet PC, the mobility facilitated by wireless communications has been vastly increased. These devices have a specific set of security concerns attached to both the device technology and their operation in medical practice (Rosenthal, 2004; Terado & Williams, 2005). Although there is concern of interception during data transfer with such devices, there is also a problem of accuracy of records where synchronisation with a central database is concerned (Veltman, 2003; Williams, 2005). The integrity and dependable nature of the data itself is important. It has been shown that the usefulness of clinical databases is often described in terms of its comprehensiveness of the data set and the information accessibility (Gilkes et al., 2003). Ensuring that integrity and completeness occurs is a fundamental principle of information management.

Availability

Availability relates to both the access to data and access to the computing services. Some of the issues in this area are standard physical security matters, whilst others relate to availability of infrastructure and timely access to data. For instance, access to patient records is important when dealing with patients out of the normal consultation or hospital environment. The use of mobile devices to provide access to patient records at the point of clinical care is being trialled worldwide and is providing both access to medical records and clinical decision support (Bower, 2004; Carroll, Tarczy-Hornoch, O'Reilly, & Christakas, 2004). Availability of electronic information, in particular the adoption of electronic medical records, is also affected by standardisation of information. The Australian Health Information Council suggests that the representation of data is the key to information sharing and includes standardisation in clinical terminologies, decision support, risk assessment, clinical workflow, and communication methods (ICTSC, 2004).

Even more fundamental to data availability are the security concerns of data protection in the form of backup and protection against power surges. Whilst these are two important measures, they are also the most poorly met requirements in security. “Today's healthcare delivery system involves a complex array of medical computerized information databases and instrumentation. These microprocessor-based computers are extremely sensitive to power anomalies such as brownouts, blackouts, spikes and line noises. While electrical companies make every effort to maintain reliability, there is no guarantee of power quality and availability” (Appelt, 2005).

CLINICAL GOVERNANCE: WHO TAKES RESPONSIBILTY?

When data is situated in one place and is effectively under the auspices of a discreet medical entity, the responsibility for the data lies with the management of the entity. This situation becomes more complicated as patient information is transferred from one entity to another in electronic form. This raises questions such as ownership of the data; responsibility for ensuring confidentiality; and responsibility for data integrity. These issues become blurred and often too difficult to answer. For instance, when data is transferred from a pathology laboratory to a general practice, who assumes responsibility to ensure the data remains intact and correct? The answers may vary depending on what stage of the transfer the data is at risk. When creating and sending the data is it clearly the responsibility of the pathology provider. When it is received by the practice it then becomes their responsibility. Whose responsibility is it when it is in transit? In assessment of risk and apportioning responsibility inevitably discussion is in terms of legal ramifications. Moreover, perhaps a perception exists that the problems will rarely occur and therefore are not considered important. This issue can only be reconciled using risk assessment techniques.

The patient perspective must also be considered. In general, medical information is recorded by the practitioner and normally patients do not decide which pieces of information are retained. Consideration is required when sharing medical records both within a practice and in any proposed national electronic records scheme. If a patient chooses not to have some information shared, the affect on their subsequent medical care must be considered. This has wider ramifications for population health and research where data is collected about the health and disease status of sections of society (Carter, 2000).

Finally, there is increasing pressure on health service providers to show best practice. This is both in terms of outcomes for the patient and in terms of costs and contributions to medical research (Chester, 2003). As more information is required to be given to the health governing bodies, the confidentiality of patient information is again compromised. Medical data is needed for many purposed including medical research, disease registries, medical education, public health monitoring, planning regional patient service, risk management and medical complaint/misconduct investigation. Indeed the General Medical Council in the UK suggests that demonstrated best practice and professional standards can be effective strategies against the lack of security in disseminating patient information (Chester, 2003).

CONCLUSION: UNDERSTANDING THE THREAT

A lack of recognition of the issues involved in computerized databases and basic security measures indicates a dangerous gap in the security of medical data. Despite the introduction of electronic medical records some 20 years ago (Bolton & Gay, 1995), medical practitioners and their professional associations are only now realising the potential that technological connectedness brings. At the same time they are realising the problems linked to the major deployment of such initiatives. Many healthcare professionals are unclear about privacy and data protection laws and what they mean in practice (Meredith, 2005).

Whilst data sharing is vulnerable to unauthorised access, reduced integrity and issues of confidentiality, many of the issues arise from poor system configuration and inadvertent access activities. To compensate for lack of information elsewhere the General Practice Computing Group have recently released a guideline for security in general practice. These guidelines include responsibility for security issues; policies; access control; disaster planning; backup; internet controls; and secure communications (Schattner, 2005). Even when ‘basic’ security measures are in place a new breed of risks is on the horizon with the advent of national electronic patient records. In the mean time, good protection, monitoring and auditing should be in place. Gilkes et al (2003, p.427) suggest that data protection is “the balance between facilitating important research and audit, and protecting patient confidentiality”. There is clearly a need to address elementary security concerns such as access control and auditing, however this should be addressed at the developmental software and database planning stage rather than at implementation. The evolving way in which we use electronic health information needs to be reflected in the production of clinical IT systems.

The Australian Health Online Committee (Commonwealth Department of Health and Ageing, 2004) research concluded that the obstructions to information sharing were overestimated, particularly when compared to the potential benefits that sharing can bring. Despite this realising the potential for sharing is by no means uncomplicated. This discourse highlights the critical issues pertaining to security in clinical practice, particularly relating to confidentiality and privacy. The underestimation of the potential for damage to both records and reputation by the medical profession has occurred from lack of understanding and from the conservative, trustful culture of the profession. Unfortunately these threats must be taken serious if patient information is not be put at risk as we move forward in the technological revolution.

REFERENCES:

Adams, T., Budden, M., Hoare, C., & Sanderson, H. (2004). Lessons from the central Hampshire electronic health record pilot project: issues of data protection and consent. BMJ, 328(7444), 871-874.

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

Aiken, J. (1999, April 27). Proposed bills would restrict access to medical records. Retrieved 15 August, 2005, from http://www.cnn.com/ALLPOLITICS/stories/1999/04/27/medical.records/

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

Black, N. (1999). High-quality clinical databases: Breaking down barriers. The Lancet, 353(9160), 1205-1206.

Bolton, P., & Gay, R. (1995). Review of computer usage among RACGP members. Australian Family Physician, 24(10), 1882-1885.

Bower, N. S. (2004). Put technology at your fingertips with a PDA. Nurse Practitioner, 29(2), 45-46.

Carroll, A. E., Tarczy-Hornoch, P., O'Reilly, E., & Christakas, D. A. (2004). The effect of point-of-care personal digital assistant use on resident documentation discrepancies. Pediatrics, 113(3), 450-454.

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

Centre for Cancer Education. (1998a). Confidentiality. Retrieved 14 August, 2005, from http://cancerweb.ncl.ac.uk/cgi-bin/omd?query=confidentiality

Centre for Cancer Education. (1998b). Privacy. Retrieved 14 August, 2005, from http://cancerweb.ncl.ac.uk/cgi-bin/omd?query=privacy

Chester, M. (2003). Abused by the NHS: patient consent and confidentiality. Consumer Policy Review, 13(2), 38.

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. Adelaide, Australia: Flinders University.

Commonwealth Department of Health and Ageing. (2004). The proposed National Health Privacy Code. Retrieved 14 August, 2005, from http://www7.health.gov.au/pubs/nhpcode.htm

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

Evers, J. (2005, May 21). Dumped hard drives tell all. Retrieved 17 August, 2005, from http://news.com.com/2061-10789_3-5726835.html

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.

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.

Lawlor, D. A., & Stone, T. (2001). Public health and data protection: an inevitable collision or potential for a meeting of minds? International Journal of Epidemiology, 30(6), 1221-1225.

Leaders: Hot data; Data protection. (2005). The Economist, 375(8432), 18.

Lyons, R. A., Sibert, J., McCabe, M., Donnelly, P. D., Shellens, T., & Evans, D. (1999). Injury surveillance programmes, ethics, and the Data Protection Act. BMJ, 319(7206), 372-375.

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

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

Pfleeger, C. P. (1997). Security in computing (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Rosenthal, K. (2004). Get “smart" with a PDA. Journal of Nursing Administration, 34, 17.

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.

Steers, K. (2005, May). Salvage the files you lost from your hard drive. PC World, 23, 164.

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

Terado, E., & Williams, P. A. H. (2005). Securing PDAs in the healthcare environment. Journal of Information Warfare, 4(1), 61-68.

Turnberg, L. (2003). Common sense and common consent in communicable disease surveillance. Journal of Medical Ethics, 29(1), 27-29.

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

Ward, H. J. T., Cousens, S. N., Smith-Bathgate, B., Leitch, M., Everington, D., Will, R. G., et al. (2004). Obstacles to conducting epidemiological research in the UK general population. BMJ, 329(7460), 277-279.

Williams, P. A. H. (2005). 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