How Addressing Implementation Issues can Assist in Medical Information Security Governance

P.A.H. Williams

School of Computer and Information Science,
Edith Cowan University, Western Australia
e-mail: trish.williams@ecu.edu.au

Abstract

Research has shown that multiple factors affect the implementation of effective information security in general medical practices. These relate to trust, capability, costs, time, knowledge level, poor implementation, attitude and inconsistencies in objectives. This paper discusses these issues, their affect on medical information security practice and their solutions as part of an information security governance process. At present there are more questions than answers to these issues, however identification of them is the first step to improve security practice in the medical environment.

Keywords

Medical Security, Information Security, Governance, Information Security Management.

1. Introduction

Research shows that many factors contribute to the effectiveness of information security including trust, capability, costs, time, lack of knowledge, and attitude, together with deficiencies in knowledge of legal requirements, use of technology, and awareness of insecurity impacts (Mahncke and Williams, 2007; Ruighaver *et al.* 2007). In identifying the issues associated with the security of electronic medical data inclusive of ethical concerns and delineation of responsibility, an appreciation of the complexity of information security in medical practice is essential. The identification of the cultural and social elements of the context play a significant role in the effectiveness of medical information security (Williams, 2007a). This paper discusses the factors which influence security practices in the medical environment, the actions that are necessary to redress the negative balance and their relevance to an overall information security governance process.

2. The complexity of the medical information security environment

The practice of information security in the medical environment is made complex by confusion over the legal requirements of electronic information protection and a lack of knowledge of information security standards (RACGP, 2003; Tomes, 2005). These issues arise because there exist a deficiency in familiarity with laws and standards as they apply to electronic medical data by medical practices. Laws and standards should be used to drive the formulation of information security practices (Information Security Forum, 2007). Unfortunately security standards are written for security and information technology specialists and therefore their use by non-technical staff is improbable. In addition, most of the standards apply to the technical aspects of security and are not context or profession specific. For instance, issues of data availability (service provision) and data quality are key factors in healthcare and therefore require more specific protection. Further, the general nature of standards means that the application of them to a specific context requires time and resources to develop. Typical general medical practices have neither time nor resources to allocate to this task. Further, as technology becomes more commonplace and electronic health records utilised, implementation of even basic security measures can be problematic for those whose core business is not security.

The complexity involved in using electronic information in general medical practice shows that a culture of trust exists which may in fact hamper rather than contribute to good information security protection (Stetson, 1997). Undefined responsibility and a lack of relevant information security knowledge create a more insecure information environment. Thus, there is a need for information security governance that can be implemented in a practical manner. Contextualisation of such information security governance includes accountability, ethical, efficient, secure and legal handling of information. Moreover, improvement in security practice can be achieved as it is implicit in an information security governance framework (IT Governance Institute, 2006). In order to inform the development such a framework it is necessary to take an information systems research approach.

3. Research Method

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 *et al.* 2007). Whilst this form of assessment may be useful, it does not address the 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 *et al.* 2007), organisational coordination (Boella and van der Torre, 2006) and many web based environments (Lacohee *et al.* 2006). Indeed, in order to keep pace with technology and its growing uses, mathematical modelling of the reliance on computing trust rather than human trust for information security is being developed , (Kallath, 2005; Nielsen *et al.* 2007).

The vulnerabilities in medical information security are associated with specific influencing factors. These factors are discussed in depth in the following section, and are based upon the results of recent research into how medical information security can be improved in medical practice. With the increasing acceptance of the psychological and social factors in the use of information technology (Klein and Myers, 1999), an interpretive approach using action research was used to investigate the factors affecting information security in medical practices. As a research method, it is becoming a popular model for research into areas of social science and health, particularly those involving primary care (Wuest and Merritt-Gray, 1997). The methodology encompasses both the structural formality of traditional research with a sociological perspective. As an overarching methodology for information security research, the action research cycle supports assessment of the current theoretical and real-world integration of information security practices to prompt question raising, planning, fieldwork, followed by analysis and reflection.

Six general medical practices in Australia and England were interviewed to collect data on existing information security processes. This data was collected in order to assess the current situation and investigate the underlying issues and attitudes to information security management. The qualitative data focused on demographics, current practice, issues and barriers, and perceptions of security. The interviews were transcribed and significant themes (influencing factors) identified using NVivo computer software (QSR, 2002). The analyses revealed several themes were recurrent throughout the interviews and appear to have a major impact on the resulting security implementation profile. The themes identified were trust, capability, cost, time, knowledge (or lack of), poor implementation technique, attitude and inconsistencies (Williams, 2008b).

4. Influencing factors

The research established links between social and behavioural features which affect good security practice such as trust, capability, cost, time, knowledge level, implementation ability, attitude and inconsistencies between principles and behaviour. As such, changes to medical practitioners' conceptions of information security and their behaviours may be a fundamental step to improve information security practice. The following discussion explains the impact of each of these factors; the resolution of their negative impact; and how the resolution could be included in an information security governance model to contribute to improving medical information security. Each of these factors has the potential to improve security practices if addressed in a cohesive and holistic manner, and as part of an overarching information governance approach to security.

4.1. Trust

Trust is the foundation upon which patient confidence and confidentiality is based (Mulligan and Braunack-Mayer, 2004). In the research trust was identified as having an undue influence on the implementation of security and particularly in relation to reliance on staff, software, technology and medical authorities. To affect any alteration in trust requires a dual approach solution to be adopted. Firstly and most easily dealt with is the issue of trust in outside influences or physical attributes such as third-party support, software and hardware. Affecting change in this area requires that education and an increase in awareness be present. Secondly and more difficult to incorporate into information security is a culture of trust. A realisation of its presence and a more realistic perspective of this culture of trust should be considered where information security is concerned in the medical environment. Indeed, in recent years clinical governance has been used to promote a culture of quality and accountability in clinical practice. Parallels to the clinical governance paradigm as a driver for improvement in information security governance in the medical environment is perhaps one way forward.

4.2. Capability

Capability can be defined as the ability to carry out actions. The capability of staff needs to be catered for and should be an integral part of an information security governance process. However, capability can also mean the potential for improvement or development in ability such as increasing skills through experience and education. Capability in the medical context may also be concerned with the medical practice's ability to access the resources it requires rather than just development of staff skills. This is affected by cost, time and knowledge level. It is an area best suited to identification of ability to meet predefined standards. In order to prove effective information security governance, comparison to benchmarks and professional standards is necessary. Further, the maturity of security practices in an organisation should be assessable. This is an uncomplicated exercise if security processes are explicitly defined, improvement pathways identified and investment in resources is provided. Hence, capability is an integral aspect of any governance model.

4.3. Cost and time

Cost and time have significant impact on what day-to-day activities are undertaken in a medical practice, particularly when it comes to technology and security (Cushman, 1997; Porcheret et al., 2004). In particular this refers to the cost of technological solutions and the cost of utilising outside expertise. These issues are addressed collectively because in the medical environment these issues are often associated together. Both could be catered for in addressing capability and by the development of policy. Since policy drives procedure, the accountancies for cost and time should be made in these policies driven by the strategic objectives. Therefore, cost and time are issues which need to be integrated seamlessly into an information security governance model.

4.4. Knowledge level

Knowledge level refers to the knowledge and understanding by medical practice staff, of responsibilities, software and system function, security protections, risk, legal requirements and technical expertise. The issue is closely related to capability and to the establishment of objectives for security at a strategic level. A lack of knowledge was reported in the data at all levels from strategic down to procedural.

This issue needs to be addressed specifically at varying points in any information security governance framework covering each level of strategy policy process and procedure.

4.5. Poor implementation

Poor implementation incorporates a lack of effective action in policy, access control, backup procedures, system and staff monitoring and availability planning. This creates an insecure environment, often unbeknownst to the medical practice. It is an issue that is related to capability but is essentially driven from a strategic level, where a lack of appropriate policy and process can be observed. To support improvement, an information security governance model would need to address this in the first instance by education. However, the assessment of implementation and capability requires that monitoring of process and procedure also be undertaken in order to identify poor implementation and areas for improvement. This activity would also be maintained by benchmarking to known standards.

4.6. Attitude

Attitude is evidence in the data collected by reflection on the approach taken to meet minimum standards; the dislike of technology; a lack of prioritisation of security; and misunderstanding of the role the practice must take in the security process. This issue is potentially more difficult to address than other influencing factors. Fundamentally, increased awareness of the seriousness of information security and its associated implications is required. This may be through education in legal responsibilities and through specific professional guidance. From a governance perspective, attitude is possibly the most important issue in that it is a strategic concern, which drivers the complete information security process. An alteration in attitude would inevitably flow down through the organisation. If the management (in this case - general medical practice partners) is not committed to governance then this will be reflected in staff practices (Halligan and Donaldson, 2001). An information security governance model must address this at a preliminary stage by establishing the basis for governance such as knowing the legal, ethical and professional requirements, and identifying roles and responsibilities.

4.7. Inconsistencies

Inconsistencies highlight the discrepancy between what is considered important and what is actually enacted. Information security governance would align these discrepancies as security actions would be derived from strategic objectives informed by recognition of responsibility. Further, monitoring and compliance would promote cyclical improvement.

5. Addressing the Influencing Factors Using an Information Security Governance Model

The literature and guidelines available for the medical environment are content based rather than process based. Therefore , developing models to address the influencing factors in terms of process rather than procedure is necessary. Whilst a reference framework such as COBIT could be considered, it is not specific to information security governance (it is a framework for IT governance). Further, such frameworks require interpretation and lack detail on 'how' to undertake some processes (von Solms, 2005). Its application may be warranted in larger organisations with significant IT management capability however it is unsuitable to medical practices that do not have such resources. Similarly, using ISO17799 could be considered however it is technically oriented and requires integration into an overall process of security governance. The primary issue with the use of high level frameworks and technical standards is the application of them in a non-security oriented environment without the necessary expertise or resources.

The medical practice environment requires a more accessible model for governance. Therefore this research was the driving force behind the development of the Tactical Information Governance Model for Security (TIGS) as shown in Figure 1. The model considers the context specific needs of the medical environment. There are currently no other models similar to TIGS in existence specifically relating to medical practice. The model is a mixture of conceptual understanding and specific information security processes. Traditional security approaches to 'good security' are most often focussed on risk management and comprise risk assessment and risk mitigation (Stoneburner *et al.* 2002), however as the TIGS model shows this is only part of the process.

The model tackles the influencing factors as principal constructors based upon established information security management activities. Consideration is given to the concept of security layering particularly in an environment where it may be untenable to implement a total security solution in one pass. Realistically, basic security is better than no security and layering increasingly complex security measures on top of basic levels can make a significant improvement in protection. The TIGS model allows implicitly for this to take place using repeated passes for process improvement.

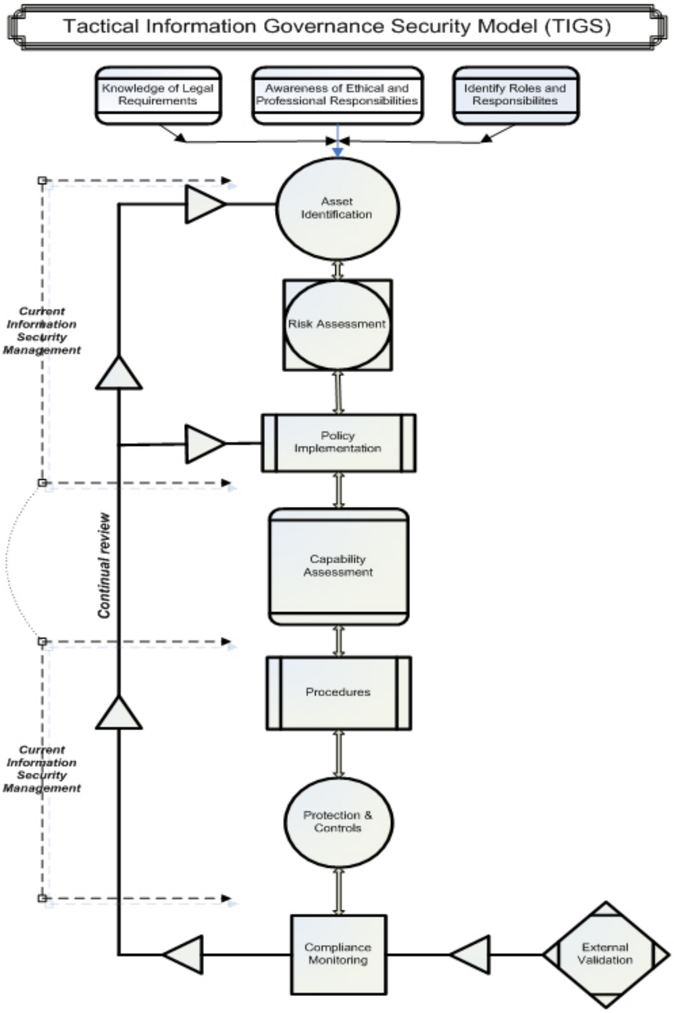
Tactical Information Governance Security Model (TIGS)
Knowledge of Legal Requirements
Awareness of Ethical and Professional Responsibilities
Identify Roles and Responsibilites
Asset Identification
Risk Assessment
Policy Implementation
Capability Assessment
Procedures
Protection & Controls
Compliance Monitoring
External Validation
Current Information Security Management
Continual review
Current Information Security Management

Figure 1: Tactical Information Governance Model for Security (TIGS) (Williams, 2007b).

In summary the influencing factors are included in the TIGS model as follows:-

- Trust – using a holistic process for improvement and education through the capability activity trust may be supported. Further, drawing parallels with clinical governance would assist with this.

- Capability – development of the capability module and using maturity level assessment (Williams, 2008a) will assess and guide capability.

- Cost and time – appropriate and relevant policy development and implementation will begin to address this concern. Further, clearly defined procedures may assist in minimising these issues.

- Knowledge level – whilst this issue needs to be defined at a policy level, it is clearly addressed in the capability activity where education and planning improvement is incorporated.

- Poor implementation – good policy development, participation in capability and identification through compliance monitoring address this problem.

- Attitude – increasing awareness and ultimately improving attitude towards security, begins with the highest level of the TIGS model where executive level roles and responsibilities, and legal and professional requirements are defined.

- Inconsistencies- these are identified in the compliance monitoring and external validation activities, and improvement in them is supported by the capability activity.

6. Conclusion

The responsibility for the patient medical record lies with the patient's doctor. It is therefore important that medical practitioners have an understanding of the requirements of good information security practice. Further, knowing where to locate relevant information and how to meet legal requirements means that an understanding of the full gamut of information security issues is required. The increasing demands of both patients and government to create accountable and transparent health systems mean that governance will be a driving force in electronic information usage. This task will be similar to that of the introduction of clinical governance some ten years ago. Assisting the medical profession to meet these demands will mean that the security professions must contribute to defining context specific processes and procedures. The issues highlighted in this paper can be addressed through an information security governance framework such as TIGS, and may prove invaluable in an increasingly litigious environment.

References

Boella, G., and van der Torre, L. (2006), "Coordination and Organization: Definitions, Examples and Future Research Directions", *Electronic Notes in Theoretical Computer Science,* Vol. 150, No. 3, pp3-20.

Cushman, R. (1997), "Serious technology assessment for health care information technology", *Journal of the American Medical Informatics Association,* Vol. 4. No. 4, pp 259.

Halligan, A., and Donaldson, L. (2001), "Implementing clinical governance: turning vision into reality", *British Medical Journal,* Vol. 322, No. 7299, pp1413-1417.

Hutter, D., Mantel, H., Schaefer, I., and Schairer, A. (2007), "Security of multi-agent systems: A case study on comparison shopping", *Journal of Applied Logic,* Vol. 5, No. 2, pp303-332.

Information Security Forum (2007), The Standard of Good Practice for Information Security, , www.isfsecuritystandard.com/SOGP07/pdfs/SOGP_2007.pdf, (Accessed 5 March 2008).

ISACA. (2007), COBIT, www.isaca.org/template.cfm?Section=COBIT6, (Accessed 11 February 2007).

IT Governance Institute. (2006), *Information security governance: Guidance for boards of directors and executive management (2nd ed.),* IT Governance Institute, Rolling Meadows, IL, USA, ISBN:1-933284-293.

Kallath, D. (2005), "Trust in trusted computing - the end of security as we know it", *Computer Fraud and Security,* Vol. 2005, No. 12, pp4-7.

Klein, H. K., and Myers, M. D. (1999), "A set of principles for conducting and evaluating interpretive field studies in information systems", *MIS Quarterly,* Vol. 23, No. 1, pp67-94.

Lacohee, H., Phippen, A. D., and Furnell, S. M. (2006), "Risk and restitution: Assessing how users establish online trust", *Computers and Security,* Vol. 25, No. 7, pp486-493.

Mahncke, R., and Williams, P. A. H. (2007), "The issues in securing electronic health information in transit", in Arabnia, H.R. and Aissi, S. (Eds.), *The 2007 World Congress in Computer Science, Computer Engineering, and Applied Computing - SAM'07 - The 2007 International Conference on Security and Management* (pp. 489-495). CSREA Press, USA, ISBN: 1-60132-048-5.

Misra, S., Kumar, V., and Kumar, U. (2007), "A strategic modeling technique for information security risk assessment", *Information Management and Computer Security,* Vol. 15, No. 1, pp64-77.

Mulligan, E., and Braunack-Mayer, A. (2004), "Why protect confidentiality in health records? A review of research evidence," *Australian Health Review,* Vol. 28, No. 1, pp48-55.

Nielsen, M., Krukow, K., and Sassone, V. (2007), "A Bayesian Model for Event-based Trust", *Electronic Notes in Theoretical Computer Science,* Vol. 172, pp499-521.

Porcheret, M., Hughes, R., Evans, D., Jordan, K., Whitehurst, T., Ogden, H., et al. (2004), "Data quality of general practice electronic health records: The impact of a program of assessment, feedback and training", *Journal of American Medical Informatics Association,* Vol. 11, p.78.

QSR. (2002), NVivo (Version 2.0.163), [Computer Program], QSR International.

RACGP. (2003), "Handbook for the management of health information in general practice", www.racgp.org.au/privacy/handbook, (Accessed 15 February 2007).

Ruighaver, A. B., Maynard, S. B., and Chang, S. (2007), "Organisational security culture: Extending the end-user perspective", *Computers and Security*, Vol. 26, No. 1, pp56-62.

Stetson, D. (1997), "Achieving effective medical information security: Understanding the culture", *Bulletin of the American Society for Information Science,* Vol. 23, No 3, pp17-21.

Stoneburner, G., Goguen, A., and Feringa, A. (2002), *Risk Management Guide for Information Technology Systems (No. Special Publication 800-30)*, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD.

Tomes, J. P. (2005), “Prescription for data protection”, *Security Management*, Vol. 49, No. 4, pp75-77.

von Solms, B. (2005), “Information Security governance: COBIT or ISO 17799 or both?”, *Computers and Security,* Vol. 24, No. 2, pp99-104.

Williams, P. A. H. (2007a), “The effects of IT on information culture in general medical practice”, in *TILC 2007 T2-Technology and Transformation: Transforming Information and Learning Conference*, Edith Cowan University, Perth, Western Australia, ISBN: 0-7298-0652-9.

Williams, P. A. H. (2007b), “Information governance: A model for security in medical practice, *Journal of Digital Forensics, Security and Law,* Vol. 2, No. 1, pp57-72.

Williams, P. A. H. (2008a), “A practical application of CMM to medical security capability”, *Information Management and Computer Security*, Vol. 16, No. 1, pp58-73.

Williams, P. A. H. (2008b), “When trust defies common security sense”, *Health Informatics Journal,* Vol. 14, No. 3.

Wuest, J., and Merritt-Gray, M. (1997), “Participatory Action Research”, in J. M. Morse (Ed.), *Completing a Qualitative Project: details and dialogue* (pp. 283-309), Sage Publications Inc, Thousand Oaks, California, ISBN: 076-1906-010.