

The Role of Standards in Medical Information Security: An Opportunity for Improvement.

P. A. H. Williams

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

Abstract – *Standards are an essential feature in an unregulated field such as computing. Thus, when computing and the healthcare environment are combined, the requirement for standards is imperative. For instance, the combination of sensitive information and mobile technology presents increased complexity in information security. Whilst we have many worldwide standards for information security including OSI 17799, little has been done in interpretation of these to ensure quality. Standards are written for specialists in the field and in the case of information security, for security specialists, yet we expect them to be read and implemented by non-technical healthcare staff. This results in the limitation of standards to be easily applied. This paper suggests that a more holistic approach is taken to the development of standards, in which standards and associated context specific guidelines are developed.*

Keywords: medical data; standards; security, information security.

1 Introduction

Health is an area that is dependent on information both for accurate patient care and for the management of health services. Standards are therefore critical to the consistency of information sharing and its effectiveness. In order to provide any discourse on the use and effectiveness of standards, it is constructive to understand the position of law and standards. Further, to position this within the medical context a review of current standards is presented. Consequently, the role standards play in information security is discussed, including the benefits and limitations of their application. The subsequent discussion suggests an alternative approach to the development of standards and their use within the medical information security environment, using existing models of quality assurance such as the Systems Security Engineering – Capability Maturity Model (SSE-CMM).

Standards are an essential feature of any industry in order to ensure levels of quality. This is vitally important in the field of computing, where a multitude of hardware, software and data formats have resulted from an industry that thrives on diversity and a lack of standards. In such an environment, creating necessary and sufficient legislation is difficult. As a result, legal requirements are often incorporated in formal standards, rather than by specific regulation. It is therefore useful to understand the difference between laws and standards within the computing scenario.

1.1 Regulation versus standards

Laws regulate the use, collection, development and ownership of data, and are used to protect the integrity and secrecy of information [1]. Laws are usually aimed at liability after the event. The effectiveness of law lies in its enforceability. In comparison, a standard is an expert consensus document that provides a benchmark for a product or service [2]. Standards are practices that are recognized for their quality and can be used as a measure for comparison. Like laws, they need to be monitored and enforced to be effective. Standards provide guidelines for best practice, consistency and interoperability. There are two types of standards: formal and de facto. Formal standards are developed by official industry or even government bodies, whilst de facto standards are established through market use and vendor promotion but have not gained official recognition or sanction. However, it should be noted that in computing de facto standards, such as Microsoft Windows operating systems, are a primary driving force in societal expectation as well as within the industry itself [3].

2 Medical information security standards

The issue of importance of standards in the health environment relate to ensuring quality and accountability. This must be viewed within the context

of existing standards and the application of these standards.

2.1 Importance

Although the security of data *in situ* is important, such security takes on a new complexity with the increased portable nature of technology. This in turn leads to increased mobility in terms of data access. To date, the role of standards in this area has been to promote seamless interoperability between hardware devices and vendor applications. However, as Kokolakis, Gritzalis and Katsikas [4] point out, when dealing with the healthcare environment we need to consider trust and quality assurance when employing such interoperable services. In these circumstances the issues are represented, and indeed measured, by conformance to specified processes and procedure management, rather than by measurement of the specific quality of a data item.

Quality of data is a key factor in good patient care. Data quality in healthcare is problematic in that both the syntactic and semantic characteristics must be assessed. Whilst syntactic assessment can be assisted by existing software tools, assessing the semantics (linguistic meaning) of the words within the context examined is difficult, particularly if this was compounded by incorrect syntax [5]. Currently, this leads to a reliance on standards and conformance to policy rather than specific data quality measurement. Medical practices must be accountable to their patients in order to maintain the basic relationship of trust between doctor and patient. Therefore there is a need to reassure patients that their privacy is not eroded in the electronic environment. This is of particular importance in a consumer driven health market such as Australia.

A lack of formal standards allows a growing diversity in *de facto* standards, which limits interoperability and data conversion between commercial products, and hampers production of a national electronic health record. For the end user this results in a complexity of choice and increased difficulty in assessing quality, compliance with standards or legal requirements.

2.2 Existing standards

Existing principles can be viewed from the legal and standard perspectives. From a legal perspective, there are various standards worldwide that either provide for general or specific scenarios in healthcare. For instance, in Australia the overarching legal regulation is the *Australian Federal Privacy Act 1988* establishing national privacy principles and information privacy principles. This legislation is broad and

required reviewing to include the collection of electronic data, security, quality of data and sensitive information consent. Yet, in the updated version the data security section only lists two items which are general in nature: that “an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure” and that “an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed” [6]. These amendments were subsequently passed in 2000, yet they still do not specifically address the electronic environment. Further, the legislation does not apply to all States and Territories in Australia, some of whom have no other legislation which covers information privacy, and in particular protection of medical and health related data [7].

In contrast, in the United States, the *Health Insurance Portability and Accountability Act (HIPAA)* of 1996 is a legally binding, comprehensive health information protection policy. The HIPAA promoted the development of electronic healthcare transactions and specifically addressed the important issues of privacy and security for health related information. This act is in two parts, covering the privacy of information, and security of information separately. The security element specifically acknowledges the inherent problems in using electronic forms of records keeping and the changing nature of the technology upon which such records are recorded, used and stored. More importantly, the HIPAA identifies requirements and implementation strategies. In 2003 the US congress went further to enact the *Standards for Privacy of Individually Identifiable Health Information*, otherwise known as the *Federal Medical Privacy Rule*. Some argue that such specificity, as is incorporated into the rule, is impossible to comply with given current medical information systems and a lack of understanding of even basic security measures in medical organizations [8].

From a standards perspective, we refer to ISO 17799, which was developed in 2000 to assist in the development of security plans. It is a code of practice focused on high-level security management. It was revised in 2005 to cover current technology and e-business practice. “ISO/IEC 17799:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices” [9]. As a code of practice it cannot be used for certification, so a standard has recently been developed (ISO/IEC 27001 *Information security management system requirements*) which will be certifiable. This new standard specifies the

requirements for security implementation which is customizable for individual organizations [10]. ISO standards are only a starting point as they do not contain comprehensive information on how security measures should be implemented or maintained.

In Australia, the AS/NZS 17799 is the Australian Standards version of the ISO17799. A complementary standard to the original ISO17799 guidelines called AS/NZS 4444 was superseded by AS/NZS 7799.2:2003 *Information security management - Specification for information security management systems* in 2003. However, it was acknowledged that there was a need for more specificity in the area of health than for other business entities. Subsequently the HB174-2003 *Information security management – implementation guide for the health sector* was developed specifically to assist health organizations interpret the original standard [11]. In addition, other AS/NZS standards specifically addressing health identification of both the patient and health providers have been developed, as have guidelines for the security and use of electronic medical records [12].

It should also be mentioned that other standards exist for specific aspects of health information, particularly for use in e-health information exchange. HL7 is one such standard, which has been developed as a principal standard for clinical information exchange [13]. HL7 has been based predominantly on the HIPAA guidelines. In addition, significant effort is being put into development of healthcare information systems security in Europe by the European Committee for Standardization (CEN). However, as with Australia, this has resulted in a diverse range of standards being developed for specific instances of technology use. Finally, many standards do not include sufficient security-related provision and given the complex nature of standards, has resulted in a large number of companies selling security management solutions for the interpretation of the standards and how to put them into practice.

3 Role of standards

Security standards are a necessity because they serve as rigorous objectives to quality, and if followed they increase the effectiveness of security practices. However if they are too general and difficult to put into practice without significant interpretation, then perhaps there is a need to review the construction of standards. In order to do this we should consider the benefits and limitations associated with them.

3.1 Benefits

The portability of data, resulting from the use of mobile computing devices, means improved workflow capability and increased quality of care [14]. Indeed, mobility and the use of small devices such as personal digital assistants (PDAs) allow scalability in technology infrastructure with minimal disruption to the user and at lower cost [15]. Benefits such as these are not in contention. Compatible and secure information exchange using message formats such as HL7 are an obvious advantage to interoperability. Less obvious is that certification, and standards, can cement consumer confidence as it implies high reliability and quality. The role of standards has been identified by various national health policies as important because of this drive for increased connectivity and information sharing.

There is also a distinct need for standardized reporting and information collection to improve patient care and to support the global shift to make primary care the coordination point for healthcare [16]. Indeed, standards for the design of health information systems and electronic information sharing have been the reason for the development of Health Informatics groups worldwide. Such groups have also recognized the need for development of more understandable and specific guidelines for security implementation and assessment, due to the generic nature of the existing standards.

3.2 Limitations

The ISO 17799 and 27001 standards are designed to be overarching and encompass security in a general sense. The controls discussed are not prioritized and should not be viewed as a definitive or a contextual solution. Undeniably, some researchers have suggested that such standards should be viewed as reference frameworks for security governance rather than guidelines [17]. This reflects the high level nature of such standards, and it has been suggested that a lack of international standards has been a factor in the over customization of medical information systems in Europe [4], resulting in limited interoperability. As Allaert [18] points out, whilst there is a considerable amount of development resources for new information systems for the medical arena, those responsible do not want to spend either the time or the money on essential or desirable security measures. Standards are written for specialists in the field and in the case of information security, for security specialists, yet we expect them to be read and implemented by non-technical healthcare staff.

Standards exist to ensure a secure system and provide associated minimum technical specifications.

Ultimately, the translation of a standard into policy and then procedures, specific to the environment of use, is a necessity. Yet, this is where the application of standards into use by the medical profession fail. Policy derived from standards must be singular and continually monitored if it is to be effective [15]. It is a cost overhead, which whilst reducing risk to data does not overtly contribute to patient care and is therefore frequently underestimated. This points to a lack of understanding of the importance of security at the management level. It also highlights the issue that in order to implement effective security you must first understand what is being protected, and the associated risks and vulnerabilities. The healthcare environment demands physicians and other health care professionals are not only medical personnel but social workers, administrators and now security specialists. This has been clearly identified as an issue for primary care in Australia [19]. Current standards do not assist in this aspect of application at all. The Australian HB 174-2003 handbook features best practice control measures for information security and is designed for a non-technical readership. This goes a long way to making the implementation of original standards more understandable. However, like other guidelines it does not cater for specific types of health providers or organisations and therefore contains a more complicated picture for those with minimal security knowledge.

4 Discussion

Standards are only one part of the security protection package.

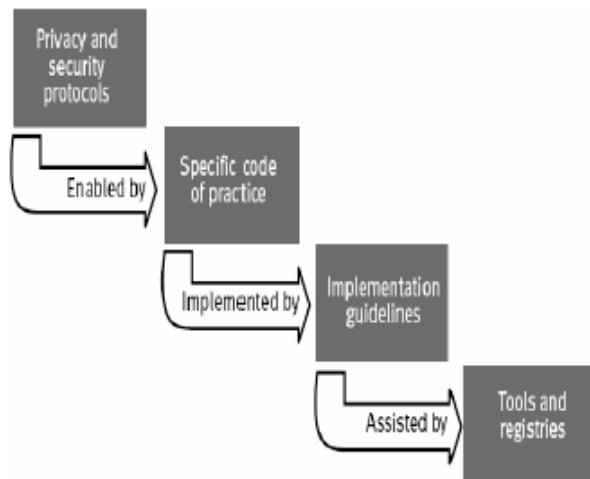


Figure 1: Privacy and security guide framework [16]

As the New Zealand health strategy group [16] suggests in figure 1: security standards (protocols) are enabled by codes of practice, which are implemented by guidelines and assisted by tools. For the package to be effective it should not be left to separate organizations to provide each component, particularly since the originating expertise in standards development is then interpreted by others for codes of practice and implementation guidelines. Further, security frameworks need to be context specific. Whilst technical controls will come and go, the work processes and information they are protecting in healthcare remain constant. It is the processes of protection and control that are important. These are not reflected in any standard and omit reference to enforcement or quality assurance of the standard.

Since the quality of medical information is dependent on assessing process rather than the data itself, as discussed previously, then it is necessary to have a framework to support this assessment. One such model which may be applicable to the health area in assessing their security abilities is the Systems Security Engineering – Capability Maturity Model (SSE-CMM).

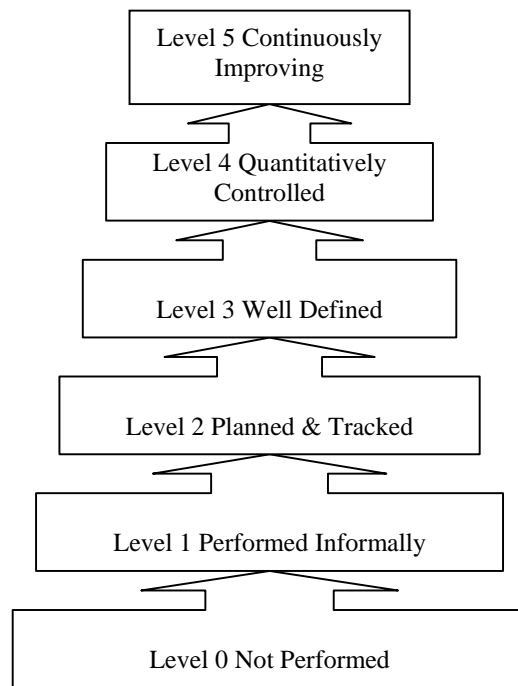


Figure 2: Capability maturity levels

SSE-CMM is a model for evaluating security processes; evaluating the capability of the organization in regards to security; and as a basis for improving security in an organization. The model uses a capability scale as shown in figure 2. Whilst this model has been used in

various business settings it has not yet been applied to the health field, although various organizations are considering it [20]. However, since information security is a people, and therefore capability, based activity, and given that healthcare is an area of national importance, it seems logical to use this model to create an information security capability based framework for implementation and assessment [21].

In 2002, the SSE-CMM was adopted as the standard ISO/IEC 21827:2002 *Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)* [22]. The standard, whilst aimed at the software development, is based upon generic security risks assessment which is consideration of threats, vulnerabilities and impact. It also includes a set of security base practices from which to assess current security capability. The purpose of developing the model into a standard is to establish a comparison metric, whilst providing a process for improvement in security practice. However, as with other standards, the generality of the content relies on the reader to understand and interpret the specifications.

5 Conclusions

Standards are imperative to ensure benefits to the patient and healthcare providers in information interoperability whilst allowing for diversity and creativity to be promoted. They are a necessity for consistency of information collection and sharing, for establishing secure infrastructure over which to share this information, and for providing guidelines for the consequent information governance procedures. What is needed is a comprehensive set of standards that define practical guidelines, or standards that are written in conjunction with practical guidelines for the healthcare community. Given that this is an area with a diverse yet homogenous group of organizations for instance hospitals, specialists and general practitioners, specific targeted standards should be developed for the protection of sensitive information, and not left to individual interested parties to develop.

This paper advocates that a more holistic approach be adopted in relation to development of standards, particularly at a national level. Whilst we operate in an expanding and diverse industrial environment, within healthcare there is a uniformity of purpose. There exists an opportunity to help practitioners in a practical sense by using a standardized approach to information security. Research is currently being undertaken in this area to adapt the SSE-CMM for a non-technical, non-security oriented medically specific context, to create a usable set of guidelines that meet both the security standards and legal requirements, and are positioned at

a practical context specific level allowing for the capability of the environment in which it is used.

6 References

- [1] C. P. Pfleeger, *Security in computing*, 2nd ed. Upper Saddle River, NJ: Prentice Hall, 1997.
- [2] Health Information Standards Organisation. (n.d.). *Why standards?* [Online]. Available <http://www.hiso.govt.nz/whystandards.htm>
- [3] A. Dennis, *Networking in the internet age*. USA: John Wiley & Sons, 2002.
- [4] S. Kokolakis, D. Gritzalis, and S. Katsikas, "Why we need standardisation in healthcare security," in *Security standards in healthcare information systems: A perspective from the EU ISIS MEDSEC project*, vol. 69, F.-A. Allaert, B. Blobel, K. Louwerse, and B. Barber, Eds. Amsterdam, Netherlands: IOS Press, 2002, pp. 7-12.
- [5] T. Welzer, B. Brumen, I. Golob, and M. Druovec, "Medical diagnostic and data quality," in *Proc. 15th IEEE Symposium on Computer-Based Medical Systems CBMS 2002*, pp. 97-101, 2002.
- [6] Officer of the Privacy Commissioner. (2000). *National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000)*. [Online]. Available <http://www.privacy.gov.au/publications/npps01.html#d>
- [7] P. A. H. Williams, "Where are the policies for PDA usage in the Australian healthcare environment?," in *Proc. 4th European Conference on Information Warfare and Security*, University of Glamorgan, Wales, UK, 2005, pp.401-408.
- [8] R. Lederman, "The medical privacy rule: can hospitals comply using current health information systems?," in *Proc. 17th IEEE Symposium of Computer Based Medical Systems 2004 (CBMS 2004)*, 2004, pp. 236-241.
- [9] *ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management*, International Standards Organization, 2005.
- [10] *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management*

systems – Requirements, International Standards Organization, 2005.

[11] *Information security management—Implementation guide for the health sector*, Standards Australia HB 174—2003, 2003.

[12] *Health Informatics—Requirements for an electronic health record architecture* Standards Australia ISO/TS 18308:2004, MOD, 2005, pp. 32.

[13] J. S. Hooda, E. Dogdu, and R. Sunderraman, "Health Level-7 compliant clinical patient records system", in *Proc. 2004 ACM symposium on Applied computing*, 2004, pp. 259-263.

[14] E. Terado and P. A. H. Williams, "Securing PDAs in the healthcare environment," *Journal of Information Warfare*, vol. 4, pp. 61-68, 2005.

[15] 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.

[16] Health Information Strategy Steering Committee. (2005). *Health Information Strategy for New Zealand 2005*. [Online]. Available [http://www.moh.govt.nz/moh.nsf/0/1912064EEFEC8EBCCC2570430003DAD1/\\$File/health-information-strategy.pdf](http://www.moh.govt.nz/moh.nsf/0/1912064EEFEC8EBCCC2570430003DAD1/$File/health-information-strategy.pdf)

[17] B. von Solms, "Information Security governance: COBIT or ISO 17799 or both?", *Computers & Security*, vol. 24, pp. 99-104, 2005.

[18] F.-A. Allaert, B. Blobel, K. Louwarse, 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.

[19] P. A. H. Williams, "Information security awareness of medical practitioners", in *Proc. Developing Partnerships. 1st Colloquium of Information Systems Security Education - Asia Pacific (CISSE-AP)*, Mawson Lakes, SA, 2005, pp.32-42.

[20] URAC.org. (n.d.). *NIST/URAC/WEDI Health Care Security Workgroup*. [Online]. Available http://www.urac.org/committees_sworkgroup.asp

[21] J. E. Goldman and V. R. Christie, "Metrics based security assessment," in *Information security and ethics: social and organizational issues*, M. Quigley, Ed. Hershey: IRM Press, 2005, pp. 261-288.

[22] *ISO/IEC 21827:2002 Information technology – Systems Security Engineering –Capability Maturity Model (SSE-CMM)*, International Standards Organisation, 2005.