Data and Knowledge for Medical Decision Support
B. Blobel et al. (Eds.)
IOS Press, 2013

doi:10.3233/978-1-61499-240-0-195

Implementing Healthcare Information Security: Standards Can Help

Andrej OREL[a,1] and Igor BERNIK[b]
[a] *Marand d.o.o., Ljubljana, Slovenia*
[b] *University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia*

Abstract. Using widely spread common approaches to systems security in health dedicated controlled environments, a level of awareness, confidence and acceptance of relevant standardisation is evaluated. Patients' information is sensitive, so putting appropriate organisational techniques as well as modern technology in place to secure health information is of paramount importance. Mobile devices are becoming the top priorities in advanced information security planning with healthcare environments being no exception. There are less and less application areas in healthcare without having a need for a mobile functionality which represents an even greater information security challenge. This is also true in emergency treatments, rehabilitation and homecare just to mention a few areas outside hospital controlled environments. Unfortunately quite often traditional unsecured communications principles are still in routine use for communicating sensitive health related information. The security awareness level with users, patients and care professionals is not high enough so potential threats and risks may not be addressed and the respective information security management is therefore weak. Standards like ISO/IEC 27000 ISMS family, the ISO/IEC 27799 information security guidelines in health are often not well known, but together with legislation principles such as HIPAA, they can help.

Keywords. Information Security, Healthcare information standards, Healthcare information security standards, ISO standards, HIPAA

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 necessary to understand the position of governing laws and standards for different type of business. To position this within healthcare, the approach information security in medicine and discussion of some current health information standards is presented further on.

Standards are an essential feature of any industry in order to ensure levels of quality [1]. This is vitally important in the field of computing, where a multitude of hardware, software and data formats have resulted from an industry where per-se a lack of standards is omnipresent. In such an environment, creating necessary and sufficient legislation is difficult. As a result, legal requirements are often incorporated in formal

[1] Corresponding Author. Andrej Orel, Marand d.o.o., Koprska ulica 100, SI-1000 Ljubljana, Slovenia; E-mail: andrej.orel@marand.si

standards, rather than by specific regulation. It is therefore useful to understand the difference between laws and standards within the computing scenario.

Laws regulate the use, collection, development and ownership of data being used to protect the integrity and secrecy of information [2]. Laws are usually aimed at liability. 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 [3]. Standards are practices that are recognized for their quality. 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 [4].

1. Elements of Information Security in Healthcare

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security is achieved by ensuring the confidentiality, integrity, and availability of information. In healthcare confidentiality, integrity, and availability generally mean the following [5]:

- *Confidentiality* – the property that electronic health information is not made available or disclosed to unauthorized persons or processes.
- *Integrity* – the property that electronic health information have not been altered or destroyed in an unauthorized manner.
- *Availability* – the property that electronic health information is accessible and useable upon demand by an authorized person.

Assessing electronic health information confidentiality, integrity, and availability requires the medical professional first to understand health IT environment of a hospital, private practice or some other medical institution. This includes technologies used for both clinical and administrative purposes. It is important that those technologies are physically used and located, and to know how they are used during various healthcare processes. When evaluating health IT environment one should think about situations that may lead to unauthorized access, use, disclosure, disruption, modification or destruction of electronic health information.

Every IT action is associated with risks. Therefore it’s important to have a collection of those risks, to understand them, to recognise possible impact on business – in our case patients’ healing process, and of course possible influence on patients. To mitigate risk impact two important steps can be performed [5]:

- Reviewing existing health information security policies (if already in place) and develop new policy statements to address new risks to electronic health information provoked by ever changing technologies. These new policy statements could require usage of certain technology for example encryption of data on mobile computing equipment such as laptops, tablets and smartphones which includes a list of personnel within healthcare organisation authorised to view and administer electronic health information. It should be also clarified how and when electronic health information is provided to patients or other healthcare entities outside the organisation itself.

- The updated health information security policies should be implemented into the healthcare organisation day-to-day work to mitigate new risks to electronic health information. This step helps to keep security policies current, and decreases the likelihood and/or impact of electronic health information being accessed, used, disclosed, disrupted, modified or destroyed in an unauthorized manner.

Safeguards (solutions and tools used to implement security policies) can be administrative, physical, or technical. It is important to note that the types of safeguards that can be chosen may be either limited/prohibited or required by law. Once the scope of those safeguards applicable to healthcare processes is identified, there is flexibility in determining which are appropriate for the identified risks. Performing an analysis of the benefits received from implementing safeguards versus the cost of implementation is probably the best way to make this determination. Two possible adverse outcomes:

- Healthcare organisation may not be able to justify purchasing an expensive technology to mitigate a risk to electronic health information. Alternatively personnel can be required to monitor new administrative safeguards which equally mitigate the risk.
- Healthcare organisation may not be able to accept the additional burden of administrative safeguard put on staff, and may decide to purchase a technology instead.

2. Security in Healthcare Based on Existing Standards

Although security of data with fixed data equipment is important, it proceeds with a greater complexity when taking into account increased portable nature of technology. The traditional role of standards in this area was lying in promoting interoperability between various platforms, systems and applications. However when dealing with healthcare environment one needs to consider trust and quality assurance when putting such interoperable services in place [6].

Quality of data is a key factor in good patient care. A lack of formal standards allows a growing diversity in de facto standards, which limits interoperability and data conversion between commercial products, and obstructs 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 [7]. 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.

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) 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 [8]. In 2003 the US congress enacted 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 the given current medical information systems and a lack of understanding of even basic security measures in medical organizations [9].

From a standards perspective, one can take into account the ISO/IEC 27002:2005, which was originally developed as ISO 17799:2000 to assist in the development of security plans. It is a code of practice focused on high-level security management. In its current revision (the ISO/IEC 27002:2005) it tries to cover current technology and e-business practice. This standard intended to be the common basis and practical guideline for developing organisational security standards and effective security management practices [10]. As this is only code of practice it cannot be used for certification, so the leading standard for “Information Security Management Systems (ISMS) requirements” is the ISO/IEC 27001:2005. This standard specifies the requirements for security implementation which is customizable for individual organizations. Unfortunately “certifiable” ISO standards are only a starting point as they do not contain comprehensive information on how security measures should be implemented or maintained.

However, there is a general opinion especially in some countries (Australia & New Zealand leading in this domain) that there was a need for more specificity in the area of health information security than for other business entities. Subsequently the ISO 27799:2008 “Health informatics — Information security management in health using ISO/IEC 27002” was developed specifically to assist health organizations interpret the original standard ISO/IEC 27002:2005 [11]. In addition, other standards specifically addressing health information domain with both patients and health providers have been developed. Guidelines for the security and use of electronic medical records can be found in there. Among others, the ISO/TR 18307 “Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics” [12], and ISO/TS 18308 “Health informatics — Requirements for an electronic health record architecture” [13] can be mentioned.

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 [14]. HL7 has been predominantly based on the HIPAA guidelines. Significant effort is put into development of healthcare information systems security in Europe by the European Committee for Standardization (CEN).

3. Conclusion

The ISO/IEC 27000 family (ISO/IEC 27001, ISO/IEC 27002…) of standards are designed to encompass security in a general sense and with a possibility to be used in every industry. The controls discussed are not prioritized and should not be viewed as a definitive or a contextual solution. Some researchers have suggested that such standards should be viewed as reference frameworks for security governance rather than guidelines [15]. This is rather unfortunate, as most of the people are looking for possible guidelines when trying to implement the health security system. This reflects the high level nature of such standards, and it has been suggested that a lack of international standards has been an important factor in medical information systems in Europe [6], resulting in limited interoperability. Standards are written for specialists in the field and in the case of (healthcare) information security, for security specialists. But to the contrary in many cases the healthcare organisation management expects those standards to be read and implemented by non-technical healthcare staff.

Standards are imperative to ensure benefits to the patient and healthcare providers in information interoperability whilst allowing for diversity and creativity to be promoted [5]. What we need is a comprehensive set of standards that define practical guidelines, or standards that are written in conjunction with practical guidelines for the healthcare community. Healthcare is an area with diverse group of organizations for instance hospitals, specialists and general practitioners, working either in public or in private sector. We can only wish that specific standards targeted to the most common security issues will be developed also for the protection of sensitive health information.

References

[1] Williams PAH. The Role of Standards in Medical Information Security: An Opportunity for Improvement. School of Computer and Information Science Edith Cowan University Joondalup, Western Australia, 2006; http://ww1.ucmss.com/books/LFS/CSREA2006/SAM8149.pdf (last accessed 10 September 2012).

[2] Pfleeger CP. Security in computing, 2nd ed. Upper Saddle River, NJ: Prentice Hall; 1997.

[3] Health Information Standards Organisation. Why standards?; http://www.hiso.govt.nz /whystandards.htm (last accessed 10 September 2012)

[4] Dennis A. Networking in the internet age. Hoboken, NY: John Wiley & Sons; 2002.

[5] Blobel B. Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems. Series "Studies in Health Technology and Informatics" Vol. 89. Amsterdam: IOS Press; 2002.

[6] Orel A, Bernik I. Priporočilni standardi SUVI in dopolnitve za področje varnosti v zdravstveni informatiki. In: BERNIK, Igor (ed.), MEŠKO, Gorazd (ed.). Zbornik prispevkov. Ljubljana: Fakulteta za varnostne vede, 2012; http://www.fvv.uni-mb.si/KonferencaIV/zbornik/Orel_Bernik.pdf (in Slovenian)

[7] Pharow P, Blobel B. Von eHealth zu mHealth – die Sicherheitsanforderungen in der mobilen Welt. Proceedings of GMDS 2007. http://www.med-ges-2007.de/ (in German).

[8] HIPAA. "Health Insurance Portability and Accountability Act", HHS Summary of the HIPAA Privacy Rule; http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last accessed 1 September 2012).

[9] Lederman R. The medical privacy rule: can hospitals comply using current health information systems?, in Proc. 17th IEEE Symposium of Computer Based Medical Systems 2004, 2004, 236-241

[10] ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. Geneva: International Standards Organization (ISO); 2005.

[11] ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002. Geneva: International Organization for Standardization (ISO); 2008.

[12] ISO/TR 18307 Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics. Geneva: International Organization for Standardization (ISO); 2001.

[13] ISO/TS 18308 Health informatics — Requirements for an electronic health record architecture. Geneva: International Organization for Standardization (ISO); 2011.

[14] Health Level Seven International (HL7). Introduction to HL7 Standards; Introduction to HL7 Standards http://www.hl7.org/implement/standards/ (last accessed 1 September 2012)

[15] von Solms B. Information Security governance: COBIT or ISO 17799 or both?. Computers & Security 2005 March; (24):99-104.