Information security assessment tool for digital hospitals

Heitor Neves Gottberg[a], Roberto Silva Baptista[b], Ivan Torres Pisa[b]

[a] *Public Health Program, Dept of Preventive Medicine, Federal University of Sao Paulo, Brazil*
[b] *Dept of Healthcare Informatics, Federal University of Sao Paulo, Brazil*

Abstract and Objective

Information technology security is usually a complex issue, involving international standards to allow public recognition. In healthcare, it gains complexity due the complex nature of operations and also dues country regulations that demand additional controls and accountability for the organizations Information Security Management System. But since the use of Electronic Medical Records and Hospital Information Systems is increasing, the organizations are pushed to face this challenge. This poster shows that we have developed a Web based tool to assess the current status of digital healthcare information security management in a hospital comparing to the recognized standards considering the business processes for confidentiality, integrity, availability and also the software features to provide protection of medical data. With this tool, hospital's IT (Information Technology) managers have a first report to start developing it's Information Security Management System (ISMS) or to check de adherence of the existing one to the standards on this subject.

Keywords:
Health informatics, Information management, Health information security

Methods

Revision of national and international standards in Information Security practices

In order to provide a strong and recognized background to our tool, we needed to be based on official and accepted standards. After revising many international ones (e.g. HIPAA, ISO 27001, ISO 27799) and some Brazilian we have decided to base our evaluation on 3 main documents: For the assessment of the "business processes", we have based on the ISO 27002 [1] and ISO 27799 [2] standards, due the fact that those documents have been developed by international subject matter experts. In terms of information security for the HISs, in Brazil, the Federal Council of Medicine has published the resolution 1827/2007 [3] that determines the rules to accept Electronic Medical records points to a guideline called Manual of security requirements, content and functionalities for Electronic Medical Record Systems developed specifically for the evaluation of healthcare software information security [4].

Development of the questionnaire

The tool we've developed is based on a questionnaire that has 2 parts (Part 1: Processes and Part 2: Systems), both providing an estimated level of 0% to 100% to each question.

Validation

In order to validate if the questionnaire would be correctly understood and well received by potential respondents, we have conducted interviews with experts in several areas as, Information Security in HISs, a Professor in Information Security Management system and a CIO of a reference hospital.

Results

The tool is ready and can be found at:
http://telemedicina6.unifesp.br/projeto/seguranca/entrada.php

The first feedbacks though, show that we may find 2 categories of hospitals, once they are migrating to electronic medical records. Either they are aware that once you convert the patient data to digital, it is necessary to pay attention to new information security threats, or they are not addressing this information security topic at all.

Conclusion

Our perception is that even though Hospital managers are aware of the need of digitalizing the health care information and also aware that the confidentiality, availability and confidentiality is key to health services provisioning, no deep debate and investments (time and money) are taking place at this moment.

We conclude that we have to make efforts to get the responses to our questionnaire and then show how hospitals are currently managing the information security issue.

References

[1] ISO, 2005; ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management. ISO.

[2] ISO TC 215, 2008; ISO/IEC 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002; ISO TC 215 – Health Informatics.

[3] Brazilian Federal Council of Medicine (CFM), 2007; RESOLUÇÃO CFM Nº 1.821/07.

[4] Leão, B; et al (ed); 2004; Manual of security requirements, content and functionalities for Electronic Medical Record Systems; Brazilian Society for Healthcare Informatics.

Address for correspondence
e mail: heitor.gottberg@gmail.com