CERTIFICATION AND SECURITY IN HEALTH-RELATED WEB APPLICATIONS

Iraklis Varlamis
Harokopio University of Athens,
Dept. of Informatics & Telematics
varlamis@hua.gr

Ioannis Apostolakis
National School of Public Health,
Dept. of Health Economics, Athens
gapostolakis@nsph.gr

Anargiros Chryssanthou
Greek Data Protection
Authority, Auditors Dept.
achrysanthou@dpa.gr

ABSTRACT

Healthcare web applications bring together medical experts and patients in a digital space where patients share their personal data and doctors provide consultation and diagnosis. A critical requirement for the success of a web application for healthcare is to be trusted from all participants. In order to build trust, the application should guarantee security, confidentiality, and reliability for people, data and processes. The medical profile of patients must be protected from unauthorized access and the medical advice should come from experts only. Information exchanged between any two parties should be transferred securely, should be preserved for future use and processed in accordance to predefined procedures that take into account all ethical and legal restrictions. All the above state the need for a strict policy-based mechanism, which defines roles, access rights and limitations on information access and a flexible identification mechanism, which allows anonymity of patients, and guarantees the truthfulness of doctors' identity and expertise. This work presents a holistic approach on certification and security in health related web-applications with emphasis on standards, protocols and procedures.

KEYWORDS: certification, security, standards, healthcare

INTRODUCTION

Advance in telecommunications and informatics have provided humanity with the opportunity to provide advanced services to people world-wide. One of the areas that have most benefited from information technology is the health sector. Health-related web applications have provided advanced services, such as telemedicine, to patients and doctors. However, these applications bear with them several responsibilities: to record, process and store medical information by following standard and lawful procedures, to protect medical data from unauthorized access, to ensure continuity and constant availability of healthcare services, etc.

With the use of web-based healthcare applications, such as telemedicine, tele-healthcare, tele-homecare etc, doctors are able to provide medical services to patients in distant and isolated areas. All these applications assume that medical data, such as vital signs and a patient's medical profile, are transferred securely and reliably over the complex infrastructure of the World Wide Web. Moreover, they assume the trustfulness of the source and destination of medical data.

In the case of telemedicine systems, for example, a patient's medical profile and other medical information are transferred over the network from the examination lab to the doctor's office in order the doctor to be able to perform a diagnosis. According to the CIA model (confidentiality,

integrity and availability) model, the medical information transferred across the network should be encrypted, secured and protected until it reaches its final destination. Patients' medical profiles should be accessible by their doctors in order to support diagnosis and care, but must be invisible to other patients, medical companies or individuals who don't have the appropriate privileges. Moreover, medical data should be preserved for future use and must always be available, although protected from unauthorized alterations. The use of standards in the whole process of collecting, transferring, storing and managing sensitive medical data is a requirement and should be accompanied by auxiliary auditing and monitoring services in order to build a trust model between patients and doctors.

In this work, we focus more on the following aspects of security: a) authentication, which guarantees that medical data and consultation are genuine, b) authorization, which assures that medical data are accessed by appropriate right holders, thus reinforcing trust between the partners of a medical transaction, c) non-repudiation, which guarantees that both trustees will fulfill their obligations to a contract and will acknowledge all conducted transactions, thus gradually enhancing the bonds between partners, d) risk management which refers to the ongoing iterative process of assessing web based applications for vulnerabilities, reinforcing them against threats and implementing appropriate security controls, and e) certification, as a means of guaranteeing that medical data are exchanged and processed appropriately. Certification is an addition to traditional aspects of security. It requires auditing and ensures appropriateness of the medical process in terms of information security and compliance to suitable standards and regulations (ISO 27000 series, HIPAA directions and data protection laws).

In the following section we present in more details the aforementioned aspects of security in healthcare. In section 3 we summarize the relative initiatives and established standards with emphasis to recent advances that can be used in favor of the medical community. Finally in section 4 we present our conclusions.

2. CERTIFICATION AND SECURITY IN HEALTHCARE

Methodologically, taking security measures may maintain integrity, ensure availability and protect confidentiality however does not guarantee the "ultimate" level of computer security. In the case of transferring medical data across complex computer networks, it might not suffice to secure the exchanging endpoints. Throughout its lifecycle, medical data is vulnerable to unauthorized access, alteration or manipulation, which without any security checks or presence of auditing procedures can easily go undetected, and weaken its authority. In a secure lifecycle, medical data is managed and protected so that it remains authentic, reliable and useable, while retaining its integrity. These characteristics of data can be preserved by implementing an effective Information Security Management System (ISMS) for Medical Information that ensures all three aspects of the aforementioned CIA model by implementing policies and procedures, allocating human and machine resources for all physical, personal and organizational aspects (Higgins, 2008).

When designing a secure health related application, one should have in mind that the most secure technological solution may become deprecated and that a private transaction can be intruded due to a human mistake, such as losing a password. An information security management system is more than a secure transaction or an authentication process (Williams, 2007). In such a system, any transfer of medical data: a) is performed after an iterative

exchange of credentials between the transacting parties, thus reinforcing authentication, b) is audited, in order to be able to connect any faulty transaction with the exchanging parties and attribute responsibilities. All processes are frequently revisited and tested in order to identify potential risks and provide solutions that strengthen security.

Certification in web applications springs from the need to verify the accurate, impervious and protected exchange of data across the web (Nardelli, Posadziejewski, & Talamo, 2003). The persons accessing medical data, as well as the exchanging parties during transfers of medical data need to be accurately identified. Certifying these issues means that an auditing body can track down responsibilities and identify the culprit responsible for any breach of security, in any of the following areas: confidentiality, integrity, availability, authorization, non-repudiation.

Special focus should be given to medical virtual communities (Ebner, Leimeister, & Krcmar, 2004) and the assistant role they provide to patients who seek for medical help and advice. Researchers, practitioners, medical industry and patients jointly contribute their findings, products and experiences, to the community's knowledge base. The information transferred inside a health related virtual community and the stockpiled knowledge must be carefully protected from unauthorized access or use and validated in order to be qualitative and useful.

Summarizing all the above issues, any health-related web application (tele-medicine, tele-healthcare, tele-consultation etc.) must be examined under the prism of certification, security and confidentiality, but also fulfill authentication and non-repudiation requirements, thus providing a holistic approach in building trust within a health related virtual community. The additional risks from delivering a health related application over the Internet should be assessed carefully under the prism of security. Developers of web based medical applications should also consider how certification applies in their applications. In the following section we depict the critical issues on building, maintaining, securing and certifying health related applications and summarize the available solutions.

3. SECURITY RISKS AND COMPLIANCE TO STANDARDS

As telemedicine applications evolve, the amount of sensitive information that travels through the World Wide Web increases and subsequently more strict security measures need to be taken in order to protect this information from unauthorized access. The measures can vary from simple password encryption policies to advanced cryptographic methods such as elliptic curves. For example, dissemination of medical informative content via mailing lists requires security measures to be taken, to ensure the safe transfer of medical data, while medical RSS feeds require validation and certification concerning their sources. In the former case (website transmission) cryptographic protocols, such as SSL (Secure Socket Layer), can be used by a member to communicate with the community site, whereas in the latter case a respectful healthcare association is required to certify the feed sources. An alternative solution is the use of Virtual Private Network technology as an access control measure for the users of the web application. A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Since the users of the health related web application connect to the application via an encrypted tunnel, any conducted communication is private and therefore secure. However, this is not always sufficient to build trust between the application and the patient and the certification is another step forward.

The ISO 27000 series of standards (ISO 27001 Security Website, 2009) intends to cover all the different levels and aspects of security, such as auditing of the data transfer process, assessment of information security risks, implementation of information security controls and continuous monitoring, maintenance and improvement of system security (see Figure 1). Data protection authorities can associate the level of provided protection with the applied security measures and certify whether an organization is providing adequate level of protection for medical data. It needs to be examined whether an authoritative party, such as a national health association, the world health organization and the EU, is providing specific guidelines for taking appropriate security measures for medical data and achieving an adequate level of protection.

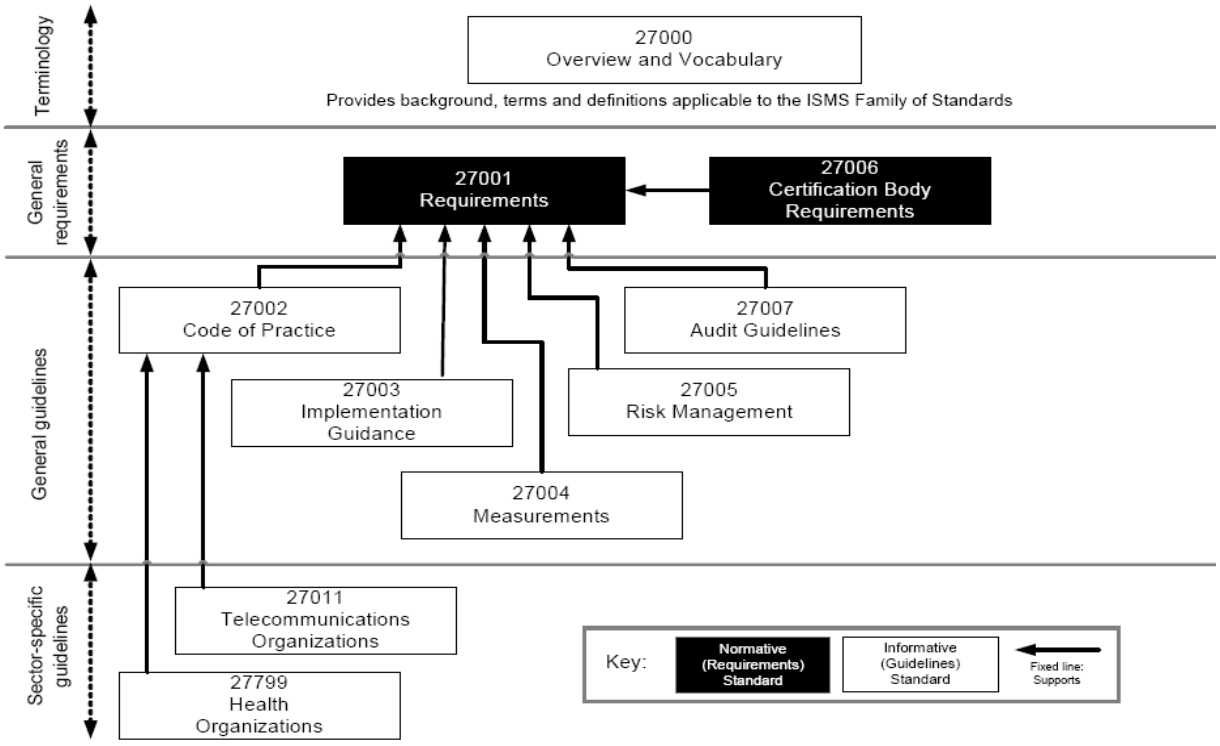

Figure 1. ISO 27000 series of standards (from ISO/IEC, 2009)

Part of the ISO 27000 series, is the ISO 27799 standard (ISO technical committee TC215, 2008), which defines guidelines to support the interpretation and implementation of ISO/IEC 27002 in health informatics. It specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. Healthcare organizations that comply to this standard ensure a minimum level of security and maintain the confidentiality, integrity and availability of personal health information. Although the development of a security management system, which follows the ISO 27799 directives, is a complicated task (Farn, Hwang, & Lin, 2007) it is the first step in providing secure and trustful web based healthcare applications. Defining a clear and concise ISMS policy, which leads to the implementation of information security policies, is the real source pool for hardening the strength of a security management system. These policies can be systemic (e.g. access control policy), data (e.g. privacy policy) or human related (rules of conduct), with all three aspects of

policies being interconnected, as an access control policy will be systemically implemented, will be followed by human users and concerns the use of data. ,

The Health Insurance Portability and Accountability Act of 1996 (HIPAA, 1986) is an attempt to use federal law in order to protect the privacy of medical records. The implementation of the HIPAA privacy regulations proved to be costly, inconsistent, and frustrating to both physicians and patients (Annas, 2003). Moreover, healthcare applications on the web usually cross national borders and as such, they face several legal issues, such as licensing, accreditation, concerns of identity theft and dependency, which are difficult to be properly addressed by legislative entities.

The opt-out policy adopted by the U.S. Government defines that companies cannot collect consumer's data if the consumer asks for it. Concerning medical information, U.S. laws (USHHS, 2003) assume total confidentiality in several issues (i.e. abortions, contraception or psychological diseases) but delegate decisions to the state laws in others. European Union has adopted an opt-in model for all personal data, which assumes that all personal information is classified until their owner grants access on them. According to the EC directive for medical data protection (95/46/EC) (EU, 1995), only health professionals can access medical information and are responsible for protecting confidentiality. According to the Recommendation (97) 5 (EU, 1997), medical data can be collected without user consent, only for preventing a real danger or in the case of a criminal offence. Moreover, if the law provides for this, data may be collected and processed in order to preserve vital interests of the data subject, or of a third person. In the case of genetic data this includes the members of the data subject's genetic line.

4. CONCLUSIONS

The main aim of this work was to enlighten the path for building secure and trustful healthcare applications for the web, which is expected to serve patients' and practitioners' aims. This holistic approach comprises several actions, such as:

- To alert patients and practitioners in regards to security issues, and more specifically,
- To raise the level of security awareness of: a) IT professionals, who develop, maintain or contribute to health related communities, b) patients that reveal their privacy to a doctor over the web and make use of medical advices shared by other patients, c) doctors that use web based applications and may not understand the special issues that arise when accessing medical data across huge and potentially unsecured computer networks,
- To propose a set of technologies, which can under circumstances ensure that patients and doctors benefit from using community services while minimizing the risk of phishers, spammers, hackers and crackers exploiting potential security holes,
- To form a methodology for certifying the validity of exchangeable medical data, exchanging parties and the exchange process.
- To review the certification and security procedures through collaboration, to identify open threats and emerging needs and to provide solutions.
- To cover as many security and certification issues as possible and provide practical solutions and case study applications.
- To frequently revise security plans and assess risks in order to update the overall security.

This holistic solution (Apostolakis, Chryssanthou, & Varlamis, 2009) can be summarized to a flexible security management system, that complies to standards, takes into account all the restrictions imposed by law and continuously evolves and strengthens against potential risks. The gains from a certified security management solution are many for patients and professionals: (1) the availability of healthcare information is valuable for the effective operation of healthcare organizations, (2) the protection of the personal and healthcare information, promotes the trust among patients and the healthcare professionals, (3) minimizing risk from the medical law point of view protects healthcare enterprises and organizations from legal sanctions – penalties and reduces negotiation overhead between the healthcare organization and the patient.

REFERENCES

Annas, G. J. (2003). HIPAA Regulations — A New Era of Medical-Record Privacy? *The New England Journal of Medicine , 348* (15).

Apostolakis, I., Chryssanthou, A., & Varlamis, I. (2009). A Holistic Perspective of Security in Health Related Virtual Communities. In L. &. eds., *In Handbook of Research on Distributed Medical Informatics and E-Health.* IGI Global.

Ebner, W., Leimeister, J. M., & Krcmar, H. (2004). Trust in Virtual Healthcare Communities: Design and Implementation of Trust-Enabling Functionalities. *37th Annual Hawaii international Conference on System Sciences (Hicss'04) - Track 7. 7.* Washington, DC: HICSS. IEEE Computer Society.

EU. (1995). *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* . European Parliament, EU Council.

EU. (1997). *Explanatory Memorandum to Recommendation (97) 5 on the Protection of Medical Data.* European Council.

Farn, K.-J., Hwang, J.-M., & Lin, S.-K. (2007). Study on Applying ISO/DIS 27799 to Healthcare Industry's ISMS. *WSEAS Transactions on Biology and Biomedicine , 8* (4).

Higgins, S. (2008). The DCC Curation Lifecycle Model. *The International Journal of Digital Curation , 3* (1).

HIPAA. (1986). Retrieved 6 1, 2009, from Full text of the Health Insurance Portability and Accountability Act: http://www.legalarchiver.org/hipaa.htm

ISO technical committee TC215. (2008). ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002.

ISO/IEC. (2009). Retrieved 06 01, 2009, from ISO 27001 Security Website: http://www.iso27001security.com

ISO/IEC. (2009). *ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary.* ISO/IEC.

Nardelli, E., Posadziejewski, S., & Talamo, M. (2003). *Certification and Security in E-Services* (From E-government to E-business, Series ed., Vol. 127). (I. I. Processing, Ed.)

USHHS. (2003). *Standards for privacy of individually identifiable health information.* US: U.S. Department of Health and Human Services, Office for Civil Rights.

Williams, P. A. (2007). Medical data security: Are you informed or afraid? *International Journal of Information and Computer Security , 1* (4), 414-429(16).