Healthcare Security and Protection in Electronic Patients' Consent: Information System SONHO case

Fernando Daniel Rocha Castro

Lusofona University of Porto, Portugal
fernandodrcastro@gmail.com

Abstract. Cybersecurity is the practice of protecting computers, networks, programs and electronic information there is against intruders or any type of virus. It also consists of recovering and fast action after an attack to avoid additional loss of information. In the medical area, all citizens that have healthcare have their personal information yielded to the hospital. Many patients don't know how they process this data and who can access it and what type of exposure they will have with a security breach.

The study of the information systems in the healthcare has the objective of understanding how electronic data of the patients are treated, used and how often the security of the systems are updated, also if the patients give the permission to use their information with another goal then what they know. To achieve this objective will be analyzed a hospital's computer system, through the research of information about this subject. System failures and possible solutions will also be presented.

Keywords: Cybersecurity, Hospital, Information, Patients, SONHO

1 Introduction

Nowadays, it is almost impossible to live without some kind of technology, which is used daily. As for health services, they have begun to evolve and adopt new technologies to make their work more practical and efficient, eliminating various problems associated with old methods (e.g., paper). However, the ease of access to some type of technology and the possibility of connecting with other devices in a network has brought several advantages, such as greater ease of obtaining, storing and sharing information, but it has also brought disadvantages, such as cybercrime attacks.

10.11228/dpsc.03.01.009

To protect a network or system it is essential to know the threats and attack techniques used by the attackers, to then implement the measures and tools needed to protect these resources. Information security is the protection of the integrity and privacy of data in databases and when they are in transit over networks. In order to use digital media in the best way and in security, it is necessary to develop and ensure their security. Digital security can be summarised in three principles [1]:

- Confidentiality of data, i.e. information is only accessed by those authorised to do so.
- Integrity, data cannot be modified and altered in an unforeseen way and the truthfulness of the information is guaranteed.
- Availability, access to information must be available to those authorised and accessible whenever requested.

Due to the little knowledge by health care users about how their personal data are treated, this work aims to understand how the information and security of health care systems in Portugal are handled. To this end, this work is composed of an analysis of security and data protection in health care facilities, as well as the Integrated Hospital Information System (Sistema Integrado de Informação Hospitalar - SONHO), which is one of the most widely used hospital information systems by the National Health System (Sistema Nacional de Saúde - SNS) in Portugal.

In addition to the present introduction section 1, the work will have 6 further sections, divided as follows:

Section 2 - discusses the concept of "Cybersecurity" and its relationship with the health institutions, reflecting on cybercrime and the ways it is celebrated in these institutions.

Section 3 - focuses on information systems and their security, emphasizing the importance of authentication, access control, standards and auditing and patient consent.

Section 4 - presents the SONHO and SONHO V2 system, its features and functionalities.

Section 5 - then identifies problems related to the SONHO system, as well as proposals for its improvement.

Section 6 - is composed of the conclusions and reflections obtained after the work was carried out.

Section 7 - presents all the references used and consulted for the present work.

2 Cybersecurity

Cybersecurity is concerned with protecting computer networks and the information they contain from accidental or malicious penetration and disruption. There is a growing concern that health information security is not sufficient, and this has already resulted in the lack of confidentiality of medical information and data integrity [2]. The Academy of Shared Services of the Ministry of Health (Serviços Partilhados do Ministério de Saúde - SPMS) with the help of the Coimbra Hospital and University

Centre (Centro hospitalar e Universitário de Coimbra - CHUC) initiated a protocol for the creation of the Centre for Development and Training in Cyber-security in Health. This is intended as an important basis for research on the safety of clinical devices, both in software and hardware. It is expected to contribute to the dissemination of all cybersecurity trials with the NHS, cybersecurity best practices, promote knowledge and training of health professionals on cybersecurity and innovation and development of cybersecurity in relation to risks to health systems. Thus, SPMS and the CHUC will establish a cooperation network, with the aim of improving the qualification of health professionals integrated in the NHS and increasing the competitiveness of the services provided [3].

2.1 CyberCrime

Cybercrime attacks range from identity data theft to more serious threats to health infrastructure and even patient security, so these attacks do much more than steal data, even hindering the daily operations of hospitals [4]. Cybercrime against health issues has manifested itself in four specific threats: data loss, theft of money, attacks on medical devices and attacks on health infrastructure. Many of these criminals are motivated by financial issues, hacking, obtaining intellectual property or consumer information to damage the institution's reputation [5]. So the best way to protect ourselves from cyber-attacks is to invest and work on the security services of healthcare institutions with robust security architectures.

Cyber-attacks, in the hospital context, can occur from several vectors [6]: 1) Internet access, if there is an Internet connection; 2) wireless network, if active wireless medical devices are used; 3) internal threat; 4) direct access attack, through physical access to a medical device; 5) removable slides such as USB, CD, PEN; 6) E-mail (e.g., phishing, Trojans); 7) other networks, access to medical slides through connection to corporate network; 8) installation or improper use, as deliberate or inadvertent activity.

3 Information System

After defining the requirements and what the institution's system should do, a number of security steps need to be taken to ensure a smooth functioning and prevent threats in the future.

3.1 Authentication

Authentication serves to identify the user and restrict access to his/her information by unauthorised persons. It is the first step in accessing the system. Authentication is essential to promote and strengthen the security of information systems. It refers to the successful identification, by some means and in some system, of a user and certifying this same identification, i.e. the system, in a controlled way, proves that the user

is who he says he is [7,8]. In most cases, the identity is proven by a cryptographic entity using a user password, which should only be known by the user. For this purpose, the security of a hospital information system is mainly based on cryptography and its authentication [9]. Thus, the computational complexity of using cryptography is used to ensure the security of all stored information is very large [9].

3.2 Access control

Another process to prevent unauthorised third-party access is to establish an access control policy. It consists of a logical entity that identifies the user who is trying to access a certain resource in the system and whether or not to allow access based on its attributes in the system. This point is central to health care information systems in order to prevent access to privileged and private information for users.

3.3 Standards and Auditing

An audit consists of a thorough analysis of the functioning of a company or organisation, assessing performance and identifying possible shortcomings that compromise its operation. In information systems, the audit goes beyond the computer function, focusing on all the information systems that belong to the organisation, whether they are computerised or not. In this way, the audit focuses on the analysis and evaluation of planning processes, developments, tests and system applications, and also examines the logical, physical, environmental, organisational, data protection and security structure [10].

ISO 27000 is a code of practice for information security and also provides security for human resources [11]. This standard address information security vocabulary and is where the ISO 270001 standard is inserted. The ISO 270001 standard is the international reference standard for Security and Information management. This standard aims to address information security management and has been improved over the years. In this way, the adoption of the ISO 27001 standard leads organisations to adopt an appropriate model for establishing, implementing, operating, monitoring, reviewing and managing an Information Security Management System, with the aim of appeasing and adequately managing the organisation's risk. Some organisations therefore require their suppliers to hold ISO 27001 certifications, as a guarantee of compliance with the principles established by ISO 27001, providing security for their customers and partners [12].

3.4 Patient consent

When a patient enters the hospital, an electronic clinical record is made, which will contain their personal data as well as data on their health status. This information can be changed and visualised by health care providers such as doctors and nurses. Clinical information systems can, for example, assist in health care delivery, clinical decision making and assess the quality of care provided. It also helps in health care man-

agement and planning. It is important to emphasise that patients have power over their access data, and thus need to give permission to access, and that they need to give their consent to those who are allowed and entitled to access that information. Patients can access their data, and health professionals, in order to securely accept patients' medical records, must use their professional identification card, and must have the patients' consent [7].

4 SONHO System

4.1 Concept

In health care in Portugal, a system was needed to store patient data and manage the financial accounting of income during their stay in hospital. To meet this need, a software was uniformly adopted in 1994 to manage the administrative data of patients, this system is called Integrated Hospital Information System (SONHO) [13], and the Central Administration of Health System (ACSS) is the institution responsible for it [14]. SONHO is the dominant information system in public hospitals in Portugal, as it has been used in a major part of SNS institutions over these years. This system is now responsible for the production control, invoicing and management of administrative data that includes clinical data such as clinical history, diagnosis and benefits. It should be noted that it is possible to export the system information for statistical indicators and to share clinical information between hospitals or even with health centres, provided they use the same information system [15]. However, in a gradual manner, SONHO is being replaced by SONHO V2, this version being more up to date according to current needs [16]. Thus, the SONHO V2 is being created as an updated and improved form of the SONHO, in order to respond to technical problems experienced by hospital units and to improve the quality and accessibility of users, health care and the improvement of working conditions for health professionals [17]. The System is connected to RIS (Rede Informática de Saúde – Health Informatics Network), a private network that interconnects several public health institutions to allow the exchange of information and services between them.

4.2 How it works

According to Pedro, V. [18], a hospital information system is developed to support administrative and clinical management with the aim of improving the equity of care provided to the user. SONHO consists of 8 modules: integrator, emergency, outpatient, inpatient, operating theatre, day hospital, archive and billing. This system incorporates three main functionalities: 1) Clinical register; 2) International classification of the patient; 3) Homogenic Diagnostic Group. At a structural level, its main objective is to create the minimum infrastructure to encompass new modules/applications interconnected with existing ones and also to ensure that the implemented standardisation criteria are naturally taken over by the new applications. On a functional level, this system focuses on controlling the flow of hospital patients. All data is collected at

hospital care points when the user accesses the entity for any type of medical act (e.g. emergency, examination) [14].

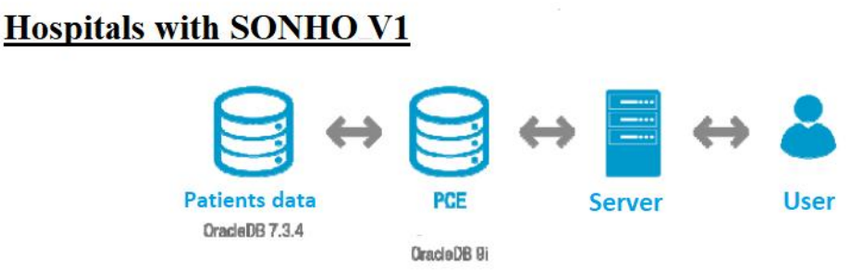

Fig. 1. Example physical architecture SONHO + PCE [16]

The first version of the SONHO revealed some difficulties in its handling, the SONHO V2 was created with the aim of combating these limitations and expanding its functionalities. The new version of SONHO V2 presents several improvements and functionalities compared to the previous version, namely [19]: a) Online help, which is a help tool that allows the user to have support in using the system; b)Upload / Download documentation, which makes it unnecessary to archive paper documentation and allows better administrative management; c) The creation of reminders for treatment, which ultimately improves the care process, d) The access to global information of each user, and the search for it quickly, e) Management of Moderator Fees, which allows access to information on the payment of moderator fees of each user; f) Use of the citizen card, which allows the identification of the user more quickly; g) Generation of Daily Maps and Statistics, h) Simultaneous scheduling of appointments, examinations and analysis; i) Consultation of several agendas simultaneously (consultations, exams and analyses); j) Visualization of a calendar with the vacancies for appointments and appointments made; k) Colour coding to identify the situation of the interned user.

4.3 LIGHT middleware

Middleware is software that is placed between an operating system and the applications that run on it. Functioning essentially as a hidden translation layer for information, middleware enables communication and data management for distributed applications. The SNS uses LIGHT (Local Interoperability Gateway for Healthcare) to mediate the exchange of information between SPMS products and external customers. It is a solution that goes beyond integration: it is an open source interoperability platform that addresses the 4 layers - legal, organisational, semantic and technical - rewarded and developed for SONHO [20]

Fig. 2. LIGHT platform [20]

5 Proposals for improvement and safety for the SONHO system

5.1 Problems

As the SONHO V1 System is old, it encounters several problems:

- maintenance level as each hospital has its own autonomous system and is checked one by one.
- It uses the same interface from the day of its creation, little oriented to the medical activity
- Poor ability to communicate with other systems which compromises the exchange of information with other health establishments using another system.
- Allows for the creation of WEB shortcuts which may compromise patient data

The personal data of the patients in the hospital information system are a fundamental and most important part, and all this information is stored in its database. As the SONHO system is an information system, it is more prone to computer attacks of the disclosure type that have the objective of stealing information. Disclosure is the unauthorised access to the information contained in the systems, and this can be divided into three types: 1) exposure, where a user or software discloses personal data to unauthorised persons; 2) interception, where a device connected to the same network can create a copy of the data when it is sent, or else have access to data transfer

traffic and intercept the information (eavesdropping); and finally, 3) intrusion, i.e. obtaining the data while ignoring the access protections to the system.

5.2 Possible solutions

To make the SONHO system more secure an authentication system could be implemented so that only authorized persons can access it. One method would be through a username and password with different access to the system depending on the status of the user in the healthcare entity.

Carrying out regular audits, this practice aims to evaluate the performance of the system and propose improvements to it, as well as possible security flaws and how to avoid them.

Protect the hardware from any possible intruder, for example by using a dedicated server room with current surveillance.

Verify the usability of the system with questionnaires to health workers using the system, with your help it is possible to orient its interface to be more interactive and easier to use, making it even more efficient. Despite all the aspects mentioned as positive in relation to SONHO V2, there are aspects that could be interesting to consider in order to further enrich and improve this new hospital information system. SONHO V2 has developed a colour coding system that allows access to the situation of hospitalized patients, however, in order to make this system more inclusive, it is important to develop other identification methods, such as the use of symbols, as there may be colour blind users with difficulties in identifying colours. Another aspect to be improved is the impossibility to digitise documents, which would be quite relevant as this would not require reference documents to be made available in several services.

Another improvement would be to integrate the Light middleware into all SNS information systems, since during the month of January 2017, around 1,932,619 events passed through LIGHT, with 97.82% of success cases [20].

6 Conclusion

The evolution of technologies and their great impact, influence and importance in information has become indispensable for many organizations and services provided today. However, the ease with which everyone can access the Internet has increased the number of hackers trying to obtain private information by illegal means, often for money. Since the beginning of the year, more than thirty public bodies have been targeted by hackers [21]. As a result, healthcare establishments that have personal data on their users in information systems databases may be the target of computer attacks from someone trying to obtain this information.

In order to prevent this loss or theft of information, it is necessary to be vigilant and carry out risk analyses periodically in order to keep up with the best solutions and improve the security of the systems. In this paper, I have explained how the SONHO, an information system used by SNS, is used to help hospitals in their administrative

part as well as to make clinical records of patients. Is also made up of a billing part that includes the costs of patients during their passage in the clinical establishment. I have presented some of its features and flaws, as well as possible improvements to make it more efficient and interactive for users, such as the use of symbols in addition to colours in the identification of patients in order to facilitate the visualisation of these for people with colorblind vision. I have had the opportunity to research and learn how healthcare institutions store their patients' information and share it among other facilities, for example, the RIS network. This has been a very important work, as it allows to know and explore a hospital information system, to identify its possible problems and to develop solutions to them, as well as to highlight the importance of personal data and the care that should be taken with them.

7 References

1. Cunha, D., & Fenato, M.: A Segurança da Informação e a sua importância para a Auditoria de Sistemas (2013)
2. Coventry, L., & Branley, D.: Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas, pp.48-52 (2018)
3. Academia SPMS: Protocolo de Cooperação em Cibersegurança na Saúde. https://academia.spms.min-saude.pt/notice/chuc/, last accessed 2020/12/15
4. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A.: Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, pp.1-10 (2020)
5. Perakslis, E. D.: Cybersecurity in health care, pp.395-397 (2014)
6. Ayala: Cybersecurity for hospitals and healthcare facilities (2016)
7. Araújo, S. C.: Segurança na circulação de informação clínica. [Master's dissertation, Faculdade de Engenharia do Porto] (2007)
8. Figueiredo, D. S., Pizzol, L. C. D., & Junior, A. F. F. B.: Infraestrutura de segurança para comunicação, autenticação e autorização transparentes em hospitais federados, pp.58-63 (2011)
9. Kuang, L. Q., Zhang, Y., & Han, X.: Watermarking image authentication in hospital information system, pp.1-4 (2009)
10. Silva, P. M. G. D.: A função auditoria de sistemas de informação: modelo funcional e de competências [Doctoral dissertation, Universidade do Minho] (2008)
11. Sansigolo: A importância da série ISO 27000. Faculdade de Tecnologia de São José dos Campos (2015)
12. ISO 27001, https://www.27001.pt/index.html, last accessed 2020/12/15
13. Lameirão, S.: Gestão Hospitalar e o uso dos Sistemas de Informação: Aplicação ao CHVR-PR [Master's dissertation, Universidade de Trás-os-Montes e Alto Douro] (2007)
14. Diretório de Informação em Saúde: Sistema Integrado de Informação Hospitalar (SONHO), http://dis.dgs.pt/2010/09/30/sistema-integrado-de-informacao-hospitalar-sonho/, last accessed 2020/12/16
15. Ávila, C. I. M. D. J.: Interface para a exportação de sumários de utentes do SONHO em openEHR (2011)

16. SPMS: SPMS - Serviços Partilhados do Ministério da Saúde, www.spms.min-saude.pt, last accessed 2020/12/16
17. CHSJ Portal: SONHO V2. https://portal-chsj.min-saude.pt/pages/865, last accessed 2020/12/17
18. Pedro, V.: Adaptação do sistema de gestão de doentes do Centro Hospitalar de Leiria ao sistema integrado de gestão hospitalar SONHO V2 [Doctoral dissertation, Instituto Politécnico de Leiria] (2015)
19. Marto, V. M. A.: A Gestão da mudança em sistemas de Informação: a migração do sistema de gestão de doentes para aplicação SONHO V2 no Centro Hospitalar de Leiria, EPE V2 [Doctoral dissertation, Instituto Politécnico de Leiria] (2017)
20. SPMS: SPMS - Serviços Partilhados do Ministério da Saúde, https://www.spms.min-saude.pt/2017/02/um-ano-luz/, last accessed 2021/01/15
21. JN: Hackers sequestraram mais de 30 organismos públicos só neste ano. https://www.jn.pt/justica/hackers-sequestraram-mais-de-30-organismos-publicos-so-neste-ano-11431269.html, last accessed 2020/12/17