The Benefits and Risks of Privacy and Security in the Era of Digital Health: Health National Service (SNS) of Portugal

Ana Moreira
Lusofona University of Porto
Porto, Portugal
a21602146@mso365.ulp.pt

Hugo Barbosa
Lusofona University of Porto
Porto, Portugal
hugo.barbosa@ulp.pt

Abstract. This paper intends to address privacy and security issues according to new digital health times, considering all devices available or integrated into the system. The possible risks and benefits of this new era should be known for better risk prevention and more effective use of benefits. As cyberattacks are increasing and increasingly customized, health cybersecurity has become a fundamental issue, but it is a complex process because it involves a large amount of information to be managed by various types of users. To ensure data privacy, integrity and security, protection mechanisms must be implemented, keeping in mind certain precautions and encourage users to modify certain behaviours. Digital Health is continually being improved, especially regarding the use of the current technologies. This paper includes an analysis to the applications of Health National Service (SNS) of Portugal.

Keywords: Digital Health, Privacy, Security, Risks, Benefits, Prevention, Cybersecurity, Cyberattacks, Confidentially.

1 Introduction

The desire to improve health care through timely access to information and decisionsupport aids, the need for simultaneous access to records by doctors, nurses and administrators is accelerating the move to electronic patient records. [1] [2] We have a strong expectation that our patient records will be used only in the context of providing effective care, and otherwise, the information will be kept secret. [2] Our medical records contain much mundane information about us but may contain some of the most sensitive information (about emotional problems, HIV status, substance abuse, genetic predisposition to disease and others). The access to patient records must be controlled because this can affect the life of the patient, for example, causing social prejudice, affecting insurability and the ability to get a job. [2] [3]

The healthcare security allows preserving the confidentiality, integrity and availability of information. We all are responsible for the information security and have the responsibility of protecting your data. [4] The human factor, that is fundamental to healing patients, is critical to healthcare security, the hospital leaders have to recognize it and otherwise all the security could be compromised. [5] The encryption of medical records is essential to keep protected in the event of a breach, that could result in the loss of patient trust if their data are exposed. All the records that is created, stored or transmitted must be encrypted and we must understand how data flows in the organization. According to [6], only 63% of healthcare organizations encrypt patient health information on their work devices.

In that sense and after the study of several data, such as concepts and numbers associated with the privacy and security in the era of digital health process, the analysis of the existing resources allowed the knowledge of the current spectrum of existing systems which in conjunction with the survey conducted in this paper have helped to understand the shortages. Thus, based on this acquired knowledge, some risks and benefits were made.

The rest of the paper is structured as follows. Section 2 presents an introduction to privacy and security in digital health including terminology and concepts. Section 3 introduces the motivation of era of digital health environment. Section 4 introduces some applications that exist in Health National Service (SNS) of Portugal. Finally, in Section 5, conclusions are drawn and referred future work.

2 Privacy and Security in Digital Health

First of all, we must distinguish three concepts involved in protecting health care information: privacy, confidentiality and security. [2] • Privacy, the right of a person to control the disclosure of personal information; • Confidentiality, the controlled release of personal health information to a care provider; • Security, procedures that help maintain the integrity and availability of information systems and control access to their contents. Confidentiality, integrity and availability are widely accepted as the information Security Triad, describing the three core objectives of information security. Availability refers to the guarantee of consistent access to the information by authorized people and is a crucial objective in the healthcare institutions. [7]

Fig. 1. Schema of Information Security Triad. [7]

The most important threats to patient information confidentiality are: [8]

- From inside the patient care institution (accidental disclosures, insider curiosity and insider subornation);
- From within secondary user settings (uncontrolled secondary usage – those who have access rights to patient information for a purpose in support of primary care);
- Outsider intrusion into medical information systems (unauthorized access).

Cybersecurity will be the main challenge for healthcare institutions, as the number of successful threats at these institutions has grown significantly in recent months. It is known that in the United States, more than 110 million individual health records have been targeted by cyber-attacks in hospital institutions, which represents a 3 times superior number of affected individuals when compared to the total threats occurred between 2009 and 2014. The institutions attacked invested a value five times higher than the one applied in the acquisition of hardware, software and services related to Information Security. [9]

3 Era of Digital Health

In this section we will talk about benefits, risks and forms of prevention in this era of Digital Health.

3.1 Benefits

The health records have the function of continuation of health care, documentation of their processes and communication between health care professionals. [10] As more healthcare facilities, from hospitals to private practices, move from paper charts to electronic medical records, the benefits will increase to physicians and patients: electronic health records can be accessed on demand, and can potentially save lives, time and money. [11]

One major and obvious benefit is legibility, historically, illegible handwriting has been a prime source of medication errors, in one source, more than 60% of medication errors in hospitals were traced to poor handwriting. [12] The use of an electronic medical records helps to reduce medical errors by utilizing computerized prescription entry, predicting drug interactions and displaying a warning for the health-care provider. [13] Some software is designed to integrate with bar code scanning technology, if a nurse scans the wrong medication, an alert pops up alerting to a problem. [12]

The paper charts generate large volumes of documentation that require a lot of storage space, it is difficult to organize and properly store so much information. The search for a paper chart will always be more difficult and time consuming and there is a strong possibility that it is recorded on sheets of paper stored in different compartments. This makes it impossible to locate records quickly and does not allow access to complete health information. Information may become difficult to recover from missing parts or even damages that render handwritten information illegible due to the paper's fragility when stored for a long time. [10]

Another major plus of electronic health records is that patients can be seen sequentially by different providers with up-to-date information immediately available. Other advantages include the fact that the system allows the patient to access their own medical information easily anywhere. [12]

Communication between physicians can be greatly improved with this, allowing each party full access to a patient’s medical history. This access allows for a more indepth evaluation and enables doctors to reach an accurate diagnosis more quickly. In addition, electronic health records can make it easier for doctors to follow up with patients and track continuing care, both under their supervision and that of the patient’s other doctors. The doctors can quickly and

easily pull up test results of their patients and also can verify when they had past exams or procedures. This can save time during a doctor's office visit, and in case of emergency, these records can provide critical and life-saving information to emergency care providers. [11] This can reduce the number of duplicate tests and exams too. Some software can flag each critical value of exams results for clinical staff and can also help physicians determine when to repeat an exam. [12]

Catastrophic events have demonstrated that patients in these situations are often confused and frightened, making it easy to forget personal medical details. Every second counts during an emergency, so having access to a patient's medical history, blood type and allergy information, when the patient is unable to communicate can be the difference between life and death. [11]

The electronic health records can reduce costs through decreased paperwork by reducing the number of employees to do this work and by reducing waste and redundant tests. [14] Facilities can also use these data in more expansive ways, for example, clinical researchers to improve health. Electronic health records have many more benefits than disadvantages, so implementing them is well worth the investment. [12]

3.2 Risks

There is a temptation to use patient health information for business purposes than those initially authorized, for example, to manage risk in insurance or to guide marketing of medical products. According to [2] there are 206 reported cases of direct discrimination from unauthorized use of genetic tests information. At least three companies in health information services industry are members of the "terabyte club" that are organizations with large data warehouses used to collect and analyse data for business applications.

According to [15] a healthcare record that is rich with personal, medical and financial detail, may be 50 times more valuable to a cybercriminal than a stolen credit card information.

Cyberattacks can occur in two forms, one is used to attack data and other is focused on control systems. The first type attempts to steal or corrupt data and deny services, the second type attempt to disable or take power over operations used to maintain physical infrastructure. The clear majority of internet attacks have fallen into the first category, such as important data stealing. [16] [17] According to [18], in 2013 and 2014 healthcare companies saw a 70% increase in cyber-attacks, it's important that everyone acknowledges the situation and understands the risks and impact, an investment in security of the organization will bring down the risk but some risk will always exist.

A cyber-physical attack on building equipment pales in contrast to the damage a determined hacker can do if he gains access to active medical devices. [19] A hospital network controls the diagnostic, treatment and life support equipment on which patient lives depend and these attacks can do a lot more than get information, they can really disrupt the day-to-day operations of your facilities. [20] The active medical devices require wireless communication and internet connectivity for software-based control of therapies and network-based transmission of patients stored medical information, this combination makes active medical devices more vulnerable to cyberphysical attack. [21] [22]

For example, an infusion pump could be controlled remotely by a malicious hacker to cause the machine to dump an entire vial of medication into a patient and the hospital staff member wouldn't notice even if they keep an eye on the pump from a centralized monitoring station. We have read how hackers struck hospitals with ransomware that prevented staff from accessing patient records or scheduling appointments, now that hackers realize the value of the medical networks to the hospital staff, they have seen that hospitals are more likely to pay up without fight because they cannot afford the downtime of restoring patient files from backups. [22] [23]

A terrorist hacker, on the other hand will not ask for money, he will simply hack active medical devices to deliver fatal doses of drugs or he will change pharmacological databases so drug to drug interactions go undetected until it is too late for hospital staff to notice. Unless hospitals take the steps necessary to secure their active medical devices they will be targeted for cyber-physical attack and possibly with lifethreatening consequences. [22]

According to [24] there are some statistics from the year of 2017:

- 1 in 13 Web requests lead to malware Up 3% from 2016;
- Percentage spam rate 55% in 2017 in email;
- 5.4B WannaCry attacks blocked;
- 600% increase in attacks against Internet of things devices;
- 24,000 Average number of malicious mobile apps blocked each day.

This numbers remind us that is very important prevent our devices from being attacked. Many users continue to make life of the attackers easier, by continuing to use older operating system versions. [24]

Ransomware is a type of malware that takes control over a computer system by encrypting all the data on the drive, the data is then held at ransom until a predetermined cost is paid. Due to the use of cryptocurrencies for payment it is difficult to track those demanding the ransom making it tough to prosecute. Ransomware can be transmitted by emails as legitimate business or tempting links, trojans acting as update requests, gaining access by exploiting known network or security software vulnerabilities. [25]

A rapid increase in the computerization of health care organizations, many without the capacity to keep up to date with the extensive privacy and security measures required, has made them targets for cyber-criminals. Health care organizations may be perceived as more vulnerable targets by cyber-criminals due to a potentially smaller IT staff and older set of IT infrastructure. [20]

3.3 Prevention

To prevent and secure your system from threats you need to know exactly what happens to patient health information after it enters your environment. It is your job to ensure it is stored, transmitted or destroyed in the most secure way possible. To do this you must record all the hardware, software, devices, systems and data storage locations that can access information, you

should find gaps in your security and then properly encrypt all the information when it enters in your environment. [6]

There are three common data handling processes often confused: masking, hashing, and encrypting.

- Masking is hiding part of the data from view, it is still there in clear text, you just can't see all of it on the screen. [6]

- Hashing is running the data through a mathematic algorithm to change it into something indecipherable. The best hashing algorithms are designed so that it's impossible to turn a hash back into its original string.

- Encrypting turns data into a series of unreadable characters, that aren't of a fixed length. The key difference between encryption and hashing is that encrypted strings can be reversed back into their original decrypted form if you have the right key. [26]

Over 100 organizations since 2009, according to [6], have had patient health information stolen because of inadequate email encryption, due to the nature of this mean of communication and the struggles to properly secure it through encryption, consider avoiding the transmission of health information via email whenever possible. The use of patient portals is preferred for sending information to patients and it's a way to reduce risks.

According to a study by [27] 36% of healthcare organizations and 55% of business associates that have been breached point to unintentional actions by their employees as the cause. This needs to change and for this they need introductory training sessions for new employees and partners to regular updates and refreshes. Julian M. Goldman says that physicians respond best when they understand why something is important, what the outcome could be and what the risks are. Then they become partners in the solution. [5] Security and privacy of health care information is a "people" problem to, if it is known that the system will record the identities, times and circumstances of all users accessing information and that these records are reviewed regularly, ethical users will think twice about abusing their privileges. Of course technology can help to make sure that only personal authorized access information and that information gets from one place to another accurately and securely, but technology can do very little to ensure that the person receiving the information will handle it according to confidentiality standards. It is unthinkable that we would impose system security constraints so tight that they would prevent an emergency room doctor from accessing the records. [2]

According to [20] there are some primary prevention methods like employee security training and awareness, confirm that backup routines are actively deployed and can be effectively restored, anti-virus programs, firewalls and network access control.

4 Applications of the Health National Service (SNS)

In this section we will talk about the applications that exist in Health National Service (SNS) of Portugal and some measures that helps protect the data of the users.

According to [28] the security and protection of their user data is taken seriously. They seek to comply with good international safety practice as well as with the "EU guidelines on assessment of the reliability of mobile health applications" and the code of conduct and privacy for mobile health applications. They have a page dedicated to cybersecurity but there are still many topics that are under construction. [28]

Mobile health applications have a strong potential to bring important benefits to citizens and society, however, data concerning health is highly privacy sensitive. Therefore, mobile health apps must be planned in such a way that the privacy of the users is protected. [29]

According to [29] you must obtain informed consent as users install the app to process their data for the purposes you've described to them. You must carefully consider what data is strictly necessary for your app and don´t collect or process more data for a longer duration than strictly necessary. The developers should ensure the confidentiality, integrity and availability of the personal data processed via their apps. Is required to implement appropriate measures to protect personal data against destruction, loss, alteration, disclosure, access and other unlawful forms of processing. Processing of personal data must be compatible with the purposes for which you first collected the personal data, as communicated to the users of your app. Secondary processing of the data for scientific research purposes is however still considered as compatible with the original purposes if it is done in accordance with EU level rules adopted. [29]

4.1 MySNS

The app MySNS allows you to consult news, your health information, provide a list and a map of health institutions, evaluation of the quality and satisfaction of the SNS by the citizen, consultation of the SNS Contact Center 24 and you will also receive notifications such as heat alerts and others associated with your location. [30]

Fig.2. Screenshot of the app MySNS. [30]

4.2 MySNS Tempos

Mobile application that allows you the consultation of the average waiting time in the hospitals of the National Health Service. The user can consult, per institution, the average time of attendance in the emergency room. The application also allows to obtain more data about the

hospital institution, such as address, telephone contacts and geographical location, through the use of the GPS of the mobile device. [30]

Fig. 3. Screenshot of the app MySNS Tempos. [30]

4.3 MySNS Carteira

Through the SNS user number and validated with information in the National Register of Users, the electronic health portfolio allows the citizen to associate specific "cards" with informative components of interest. [30]

Fig. 4. Screenshot of the app MySNS Carteira. [30]

4.4 MyADSE

This application allows you to save the ADSE beneficiary card digitally, receive messages when a refund is made, apply for the European sickness insurance card, allow you to update beneficiary and family members data, also allow you to make refund simulations and know the values and applicable rules. [30]

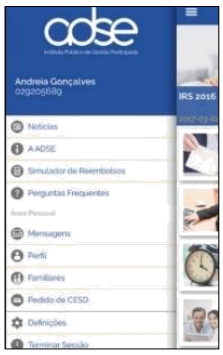

Fig. 5. Screenshot of the app MyADSE. [30]

4.5 Dador CHVNG

With the app of the Blood Service of the Hospital Center of Vila Nova de Gaia/Espinho you will be able to access your personal page and obtain all the essential information as donor, namely the records of previous harvests, analysis results, personal notifications, among many others. [30]

Fig. 6. Screenshot of the app Dador CHVNG. [30]

4.6 Dador S João

This app is identical to the Dador CHVNG but it is destined to Hospital S. João. [30]

Fig. 7. Screenshot of the app Dador S João. [30]

4.7 Dador.pt

The application is intended to promote blood donation, the user will have real-time access to information on where and when to give blood. [30]

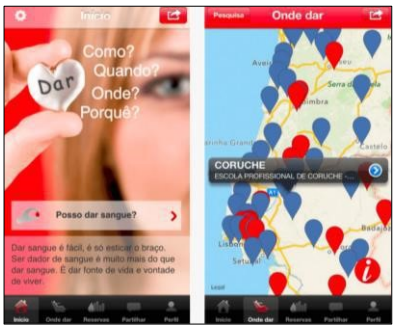

Fig. 8. Screenshot of the app Dador.pt. [30]

4.8 eMed.pt

INFARMED provides a mobile application that facilitates users access to cheaper drug prices. This tool allows that, during the moment of the choice or the acquisition of a certain drug, the user identifies another drugs equivalent, but economically cheaper. The application also provides information about the information flyer and allows you to create a drug consumption plan. Lastly, the application provides the location of the pharmacies closest to the point where the user is. [30]

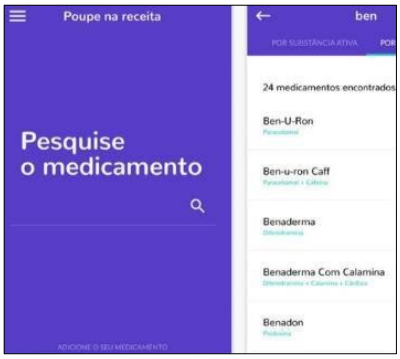

Fig. 9. Screenshot of the app eMed.pt. [30]

5 Conclusion

Today's society is turning into a digital society, with the growing influence of the technology in our daily lives. It is present in so many places, sometimes without people realizing it, that being already frequent is considered natural. This society increasingly directs its attention to new technologies, fostering their development and reaching a closer approximation of knowledge, making it increasingly accessible to all.

There are numerous advantages of using technologies in healthcare institutions, nevertheless it is necessary to reflect that there are vulnerabilities. There is no system totally safe, however attacks can be prevented and damage reduced, considering all the prevention measures as mentioned in this paper.

References

1. IOM: “The computer-based patient record: An essential technology for health care”, Institute of Medicine, National Academy Press, Washington, DC, (1991).
2. Rindfleisch, T. C.: “Privacy, information technology, and health care”, pp.1-10, (1997).
3. Rothfeder, J.: “Privacy for Sale”, New York, Simon and Schuster, (1992).
4. Portuguese Republic - Ministry of Health: “República Portuguesa - Ministério da Saúde, SNS, SPMS: A segurança da informação”, (2017).
5. AT&T: “Physicians & Cybersecurity Risk: A Cybersecurity Handbook for Healthcare CEOs”, pp.3-14, (2018).
6. SecurityMetrics: “Medical data encryption 101”, (2015).
7. OpenText, https://www.opentext.com/products-and-solutions/business-needs/informationgovernance/ensure-compliance/information-security-and-privacy, last accessed 2018/12/20.
8. NRC: “For the Record: Protecting Electronic Health Information”, National Research Council, National Academy of Sciences, (1997).
9. Information Security, http://spms.min-saude.pt/seguranca-da-informacao/, last accessed 2018/12/10.
10. Leal, M.: “Avaliação da Qualidade do Registo Clínico Eletrónico”, University of Minho, Master's Dissertation, (2013).
11. USF Health, https://www.usfhealthonline.com/resources/healthcare/benefits-of-ehr/, last accessed 2018/12/10.
12. Hoover, R.: “Benefits of using an electronic health record”, Nursing2016, (2016).
13. Alpert, J.: “The electronic medical record in 2016: Advantages and disadvantages”, Digital Medicine, (2016).
14. HealthIT, https://www.healthit.gov/faq/what-are-advantages-electronic-health-records, last accessed 2018/12/10.
15. Medscape: “Stolen EHR Charts Sell for $50 Each on Black Market”, (2014).
16. Bogdanoski, M.; Petreski, D.: “Cyber terrorism - global security threat”, (2014).
17. CCRC, http://www.crime-research.org/library/Robert1.htm, last accessed 2018/11/29.
18. Gomes, R.: “Health sector Cybersecurity Strategic Plan”, pp.10-21, (2016).
19. Reel, M.; Roberson, J.: “It’s Way Too Easy to Hack the Hospital”, Bloomberg, (2015).
20. Johnson, C.; Zapotosky, M.: “Under pressure to digitize everything, hospitals are hackers’ biggest new target”, Washington Post, (2016).
21. Kramer, D.; Baker, M.; Ransford, B.; Molina-Markham, A.; Stewart, Q.; Fu, K.; Reynolds, M.: “Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance” PLOS One, (2012).
22. Ayala, L.: “Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention”, Apress, New York, (2016).
23. Leetaru, K.: “Hacking Hospitals and Holding Hostages: Cybersecurity in 2016” Forbes, (2016).
24. Symantec: “ISTR Internet Security Threat Report”, vol.23, pp.7-50, (2018).
25. HITEQ: “Ransomware Guidance For Health Centers”, (2017).
26. Security Innovation Europe, https://www.securityinnovationeurope.com/blog/page/whatsthe-difference-between-hashing-and-encrypting, last accessed 2018/12/04.
27. Ponemon Institute: “Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data”, (2016).
28. SPMS, https://comunidade.mysns.pt/seguranca.html, last accessed 2018/12/15.
29. European Commission, “Draft Code of Conduct on privacy for mobile health applications”, (2016).
30. SPMS, https://www.sns.gov.pt/home/apps-da-saude/, last accessed 2018/12/14.
31. Capelão, F.; Barbosa, H.: “Cybersecurity in Healthcare: Risk Analysis in Health Institution in Portugal”, International Journal for Research & Development in Technology (IJRDT), vol. 9:3, pp. 25 -31, (2018).