Chapter 72
Privacy Preserving in Digital Health:
Main Issues, Technologies, and Solutions

Zakariae El Ouazzani
Rabat IT Center, Smart Systems Laboratory ENSIAS, Mohammed V University, Rabat, Morocco

Hanan El Bakkali
Rabat IT Center, Smart Systems Laboratory ENSIAS, Mohammed V University, Rabat, Morocco

Souad Sadki
Rabat IT Center, Smart Systems Laboratory ENSIAS, Mohammed V University, Rabat, Morocco

ABSTRACT

Recently, digital health solutions are taking advantage of recent advances in information and communication technologies. In this context, patients' health data are shared with other stakeholders. Moreover, it's now easier to collect massive health data due to the rising use of connected sensors in the health sector. However, the sensitivity of this shared healthcare data related to patients may increase the risks of privacy violation. Therefore, healthcare-related data need robust security measurements to prevent its disclosure and preserve patients' privacy. However, in order to make well-informed decisions, it is often necessary to allow more permissive security policies for healthcare organizations even without the consent of patients or against their preferences. The authors of this chapter concentrate on highlighting these challenging issues related to patient privacy and presenting some of the most significant privacy preserving approaches in the context of digital health.

DOI: 10.4018/978-1-7998-8954-0.ch072

INTRODUCTION

Nowadays, thanks to recent advances in Information and Communication Technologies (ICT), healthcare related data is more and more collected, recorded, processed and shared electronically allowing a significant enhancement in the health care sector or, let's say, its digital transformation towards the "Healthcare 4.0".

In this context, digital health solutions could offer to the patient better quality of care benefits in terms of both cost and time. However, these solutions increase also the risks of data breaches and privacy violation. In fact, digital health systems involve different technologies and various stakeholders (healthcare providers, Cloud providers, intermediate services such as laboratories, pharmacies...) increasing the number of potential attack vectors with new chances for intruders to gain unauthorized access to personal and sensitive healthcare data.

As stated in (The biggest healthcare data breaches, 2018), e-health systems are a profitable target for hackers. Attacks exploiting ransom ware, human errors and spear phishing emails seem to be the most dominating the last few years. In August 2019, phishing attacks continued to pose serious problems for US healthcare organizations such as with the largest breach on Presbyterian Healthcare Services, which involved more than 150,000 healthcare records breached (Healthcare Data Breach Report, 2019). Such statistics show clearly that more efforts are needed to secure and protect personal healthcare data.

Moreover, healthcare related data require stronger security measures than other types of data. This is due to the nature of the health information that may contain sensitive and private information such as sexual or mental health data, etc. Such measures should prevent disclosure of this sensitive data to any third party without prior and explicit consent of the patient (Gilson, 2012).

But, for the healthcare patricians' point of view, the security policies of the health care organizations should give them the ability to access or to share sensitive patient information(even if it is against the patients' security preferences) in order to make well informed decisions particularly, in critical emergency cases. In this context, it is clear that privacy preserving solutions should take into account all these different and sometimes conflicting needs.

It is also very important to share and publish patients' related data (including, genetic, imaging, patient-centered, etc.) to allow innovation in the healthcare sector. For example, more than 10,000 labeled images on Image Net (Department of Biomedical Informatics, 2018) were shared publicly to allow the training of deep neural networks for image recognition tasks.

Generally, such publicly shared healthcare data is anonymized before being shared, but, it is widely admitted that mitigating the risks of re-identification is still a challenging issue. Other challenging issues are raised regarding the data sharing among different health providers. For instance, the use of mobile apps and IoT devices to collect patients health data, which are then stored on the cloud, etc.

In this chapter, the authors aim to give a clear picture of privacy concerns in digital health. They focus particularly on highlighting the challenging issues related to patient's privacy and present some of the most promising privacy preserving approaches.

Thus, the proposed chapter will be organized in 5 sections. Section 2 presents some related privacy concepts and definitions particularly in the context of digital health. The description of the main e-health stakeholders and the technologies behind the rise of digital health is given in Section 3. Section 4 shows the impact, on the patient's privacy, of potential attacks that could exploit vulnerabilities inside these technologies. Section 5 discusses three kinds of privacy-preserving approaches and techniques that have been proposed recently to mitigate such risks and still need deeper research work.