Chapter 74
Patient Privacy and Security in E-Health

Güney Gürsel
Gülhane Military Medical Academy (GATA), Turkey

ABSTRACT

In the digital era, undoubtedly, e-health is a major contributor for decision support, education, research and management activities in healthcare. It provides tremendous benefits by easy store and access to data. This easiness brings a big problem together with the benefits. Users have easy access to vast amount of sensitive health data about patients. This may give way to misuse and abuse. That is why the concepts of privacy and security becomes very popular and point of major concern. This chapter is a descriptive study aimed to give principles of these concepts and invoke awareness about.

INTRODUCTION

Electronic health, E-Health, is in the intersection of medical informatics, public health and business, can be defined as the use of information and communication technologies to improve health care (Eysenbach, 2001). E-Health has grown and developed rapidly. From primary care institutions to big healthcare centers, every healthcare organization uses an information system and records every piece of patient data electronically. As the amount of data increases, using it helps improve not only the quality of services given in healthcare, but also healthcare education, research etc. Easy access to huge amounts of healthcare data brings some problems and dangers together with the benefits. One of the biggest dangers is the violation of Patient Privacy and Security. Patient Privacy and Security is becoming a popular issue as the e-health continues to improve. With the electronic storage and access of patient health data, staff has the opportunity to access huge amounts of data that they would never have when they are in paper forms. The electronic patient data also lures many organizations, who are big actors in healthcare business such as drug companies, medical device companies, insurance companies etc. Many people are in a competition to use this huge amount of patient data for legal or illegal purposes with legal and illegal access.

Patient Privacy and Security is a challenge for every e-health application and healthcare organization using e-health technologies. E-health has many advantages and benefits to both patients and caregivers,

DOI: 10.4018/978-1-5225-3926-1.ch074

healthcare managements take advantage of these benefits, but the possibility of misuse and abuse of patient health data emerges.

This chapter is a descriptive study that examines the concepts and issues related to Patient Privacy and Security and techniques used to protect it. The purpose of the study is to take attention to the importance of the Patient Privacy and Security and invoke awareness of the students, academics, researches having studies and works related to healthcare and patient data.

The chapter is organized as follows: In Background section, the definition and description of patient Privacy and Security will be given. The main part is in the heading of "Patient Privacy and Security" comprising the seriousness of the situation, Patients' Rights and Healthcare Providers' Responsibilities, Privacy and security trends that affect healthcare, Laws and Regulations on Patient Privacy and Security, Security and Privacy Auditing in E-health. In the end are the future research directions and conclusion parts interpreting the chapter.

BACKGROUND

Health data is the most private data of a person. It is so sensitive that it can make a person ashamed and upset. There may be some details even the person himself wants to forget. Because of these assets of patient health data, the notion of Patient Privacy and Security has arisen.

Although privacy and security are two different things, they are used together as a repetition for patient data. In healthcare, these two terms are used together as a concept, in which one refers to what is going to be protected, privacy, and the other refers to how it will be protected, security. In this section, to avoid misusage and confusion, brief descriptions about what is intended with patient privacy and security, will be examined. Exact description of health information is going to be given to clarify what to protect.

Health Insurance Portability and Accountability Act (HIPAA, 1996) defines health information as "whether oral or recorded in any form or medium, that

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."

HIPAA (1996) defines i*ndividually identifiable health information as "*a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    - That identifies the individual; or
    - With respect to which there is a reasonable basis to believe the information can be used to identify the individual."