Chapter 79
Compliance of Electronic Health Record Applications With HIPAA Security and Privacy Requirements

Maryam Farhadi
Kennesaw State University, USA

Hisham Haddad
Kennesaw State University, USA

Hossain Shahriar
Kennesaw State University, USA

ABSTRACT

Electronic health record (EHR) applications are digital versions of paper-based patients health information. EHR applications are increasingly being adopted in many countries. They have resulted in improved quality in healthcare, convenient access to histories of patient medication and clinic visits, easier follow up of patient treatment plans, and precise medical decision-making process by doctors. EHR applications are guided by measures of the Health Insurance Portability and Accountability Act (HIPAA) to ensure confidentiality, integrity, and availability. However, there have been reported breaches of protected health identifier (PHI) data stored by EHR applications. In many reported breaches, improper use of EHRs has resulted in disclosure of patient's protected health information. The goal of this chapter is to (1) provide an overview of HIPAA security and privacy requirements; (2) summarize recent literature works related to complying with HIPAA security and privacy requirements; (3) map some of the existing vulnerabilities with HIPAA security rules.

DOI: 10.4018/978-1-5225-7113-1.ch079

BACKGROUND

In 2009, the American Reinvestment & Recovery Act (ARRA) was enacted with the aim to modernize Health Information Technology in USA. Notably, Health Information Technology for Economic and Clinical Health (HITECH) Act founded the concept of meaningful usage having five pillars. One of the pillars is to ensure adequate privacy and security protection of personal health information ("Center For Disease Control and Prevention," 2007). The HITECH act provided incentives to health care providers to adopt Electronic Health Record (EHR) applications. The act mandated all healthcare providers to adopt EHRs when dealing with patient data by 2015. Otherwise, there are penalties for not complying. As of today, most hospitals, clinics, and affiliates have adopted Electronic Health Record (EHR) applications ("HITECH Act Summary," 2009).

Health Insurance Portability and Accountability Act (HIPAA) was established in 1996 (later revised in 2013) to establish specific privacy and security requirements for safeguarding health information. The information is created or received by various covered entities such as health care providers, health plan providers or insurance companies, employers, and health care clearing houses ("What is Protected Health Information," n.d.). Healthcare professionals and covered entities (e.g., insurance companies, business associates such as laboratories) collect, store and transmit data while providing healthcare related services to patients ("Health Professional," n.d.). Over the lifetime of a person, healthcare data is being collected in the form of electronic records (*The Importance of Data in Healthcare*, n.d.).

HIPAA identifies a set of personally identifiable information as Protected Health Information (PHI). Some examples of PHI include names, social security numbers, medical record numbers, addresses, dates (birth date, admission date, discharge date, date of death), phone and fax numbers, e-mails, health plan beneficiary information, certification/license numbers, vehicle identifiers or license plate numbers, device identifiers and serial numbers, names of relatives, biometrics (fingers and voice prints), and full face photographic images or any comparable images ("Examples of PHI Identifiers Health information :," n.d.).

As health care application becomes more and more evidence-based, storing health data is becoming more important. Weak health data protection may lead to identity theft, obtain medical care at the expense of others, order expensive drugs for resale, and claim of fraudulent insurance (*The Importance of Data in Healthcare*, n.d.). Moreover, health care data hacks may threaten patient's health due to the change of patient's medical history. For example, if health records do not contain a correct listing of allergies, the patient could suffer serious consequences or death due to wrong prescription (Smith et al., 2010).

Compare to banks and financial institutions, patients' data has less protection. Banks are mostly equipped with two-factor authentication while healthcare applications are not. Two-factor authentication is an extra protection which includes not only username and password, but also some unique information that only the user has, such as a physical token. Furthermore, unlike bank accounts that can be locked and changed for protection, it is completely impossible to get back the compromised and disclosed health data (Oliynyk, 2016; *What is 2FA? An extra layer of security that is known as multi factor authentication*, n.d.).

In 2017, Emory Healthcare's appointment system was hacked compromising almost 80,000 patients PHI information such as names, birth dates, internal medical record and appointment information. The appointment related information was stored into local databases unencrypted, which opened the door for hackers to obtain plain text information. According to a report (Arndt, 2017), this incident is the largest breach in 2017 across USA. The HIPAA Meaningful Usage act requires that any data security