Electronic Health Records: A Literature Review of Cyber Threats and Security Measures

Donna S. McDermott, Robert Morris University, Moon, USA
Jessica L. Kamerer, Robert Morris University, Moon, USA
Andrew T. Birk, Robert Morris University, Moon, USA

ABSTRACT

Electronic health records (EHRs) pose unique concerns for administrators and information technology professionals with regard to cybersecurity. Due to the sensitive nature and increasing value of personal health information, cyber risks and information protection should be a high priority. A literature review was conducted to identify potential threat categories and best practices in protecting EHR information. Potential threats were identified and categorized into five areas: physical, portable devices, insider use, technical, and administrative. Government policies have created administrative, physical, and technical safeguards to keep EHR information safe. Despite these efforts, EHRs are being targeted by cyber-criminals due to flaws in personal and organizational management of protected healthcare information. This paper aims to educate, inform, and advocate for the proper handling of EHRs to alleviate the burden caused by compromised electronic documents.

KEYWORDS

cyber security, cyber threats, EHR, electronic health records, medical records, private health information, safeguards, security threats

INTRODUCTION

The healthcare industry has adopted the widespread use of electronic health records (EHRs) in an attempt to streamline patient information, improve medical workflow, and ease communication between caregivers and patients. EHRs are an electronic version of a patient’s medical history that is maintained by a healthcare provider or agency over time (Centers for Medicare & Medicaid Services, 2012). These records tend to be very inclusive and contain personal health information (PHI) with details such as health history, financial and billing details, social security numbers, and medical reports. Due to their sensitive nature, agencies need to be diligent in maintaining their cybersecurity (Kruse, Smith, Vanderlinden & Nealand, 2017). With the passing of the Health Insurance Portability and Accountability Act (HIPAA) by Congress in 1996, the medical community has been mindful of patient privacy and protecting patient sensitive information; however, the introduction of EHRs has presented new concerns for healthcare information security. Issues such as network security, viruses, and electronic data breaches have become important considerations for healthcare providers and patients (Brott, 2012). Cybersecurity of EHRs presents new challenges for healthcare organizations and medical personnel. This paper will present the risks to EHR security and provide recommendations from the literature to address and prevent these risks.
BACKGROUND

According to the U.S. Department of Health and Human Services, health information technology involves the electronic exchange of health information to improve health care and reduce costs, prevent medical errors, increase efficiency, and expand access to affordable health care (HHS, 2017). In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed and highlighted the importance of reporting data breaches. With the proliferation of EHR use, HIPAA required healthcare organizations to address three pillars to safeguard patient information: 1) administrative safeguards such as policies and procedures, 2) physical safeguards such as limiting access to records and workstation security, and 3) technical safeguards such as access control, encryption, and virus checking (Kruse et. al., 2017).

At the same time, the prevalence of cybercrime in healthcare was increasing at a rapid rate. One study found that 94% of healthcare organizations reported being victims of a cyber-attack (Luna, Rhine, Myhra, Sullivan, & Kruse, 2015). In the first half of 2015 alone, the healthcare sector was victim to 187 reported breaches that compromised the personal information of eighty-four million patients. These healthcare breaches also accounted for 21.1% of all the cyber security breaches worldwide (McCarthy, 2015). The rise of data breaches each year in the healthcare industry highlights the failure of existing safeguards (Heald, 2016). As the general public becomes more aware of cybersecurity risks such as data breaches, virus attacks, and ransomware, it is imperative that healthcare and information technology personnel work together to ensure that all measures are being utilized to safeguard sensitive patient information and reassure patients that their information is being protected.

METHOD OF LITERATURE REVIEW

The databases of PubMed (Medline), CINAHL, and ProQuest were used to conduct literature searches regarding cybersecurity concerns related to electronic health records (EHR) with various inclusion and exclusion criteria. Search criteria were limited to blinded peer reviewed scholarly articles published in English since 2011.

Key terms used in the search were: electronic health record, cybersecurity, security, electronic medical record, and private health information. The search yielded an initial sample of 67 articles. Each article was screened by the authors for relevance to the objective. Since very little research has been conducted on this subject, a decision was made to also include informational articles and position papers. Twenty-two papers were reviewed by the research team to determine the top threats to EHR security and literature based recommendations to address or prevent cyber threats.

EVOLUTIONS OF EHR SECURITY THREATS

In the early years of EHRs, the primary sources of security threats were related to improper employee use or insider employee misconduct, as well as physical theft of data storage devices like hardware and computers (Blanke & McGrady, 2016). As the sophistication of cyber criminals have increased in more recent years, newer security concerns and methods of stealing private health information have evolved. Threats and breaches are commonplace in healthcare organizations. Cyber security threats are an unfortunate reality in this era of innovation, digitization, and technology based communication (WMA, 2016).

The healthcare industry has not kept up with the evolving cyber threats digitalization has brought to their organizations as well as their peers in other industries. Healthcare organizations also do not tend to invest in cybersecurity measures as much as their counterparts in other industries such as banking or retail (Parikh, 2017). This lack of follow-up and investment has led to increased targeting and vulnerability to cyber threats.

Cyberattacks can manifest as external or internal threats. An external threat may be incidents carried out by cyber-terrorists, while an internal threat may be from disgruntled former or current
Detecting the Use of Anonymous Proxies

[www.igi-global.com/article/detecting-the-use-of-anonymous-proxies/201537?camid=4v1a](www.igi-global.com/article/detecting-the-use-of-anonymous-proxies/201537?camid=4v1a)