Chapter 77
Cyber Hygiene in Health Care Data Breaches

Jomin George
Namibia University of Science and Technology, Windhoek, Namibia

Aroma Emmanuel
Namibia University of Science and Technology, Windhoek, Namibia

ABSTRACT

This article describes how data breaches have become the norm, as highlighted by the significant number of breaches experienced by healthcare providers. These breaches have led to the scrutiny of cybersecurity technologies, protocols and strategies applied in the health care sector. As such, this article will explore the cyber security available in health care that is used and can be used to deter data breaches. Health care sectors are currently looking on different technologies and strategies to prevent and secure the patient information from data hackers. But some of these techniques have been effective, and some have not.

INTRODUCTION

Cyber hygiene plays a serious role in various health care systems; it provides the foundations for protecting the patient confidential information from any cyber threat. Its importance is recognized by various institutions in health care sector and has developed various cyber security strategies to make the best out of the technology, its main aim is to improve the way health care institutions can protect themselves from cyber threats. Previous studies have noted that the world today is affected by the immense flow of technology. The digital information flow creates a complex economic and societal interrelation. The explosive use of the computer in data management has reinvented how data is stored and processed in almost all sectors, healthcare is one of the institutions greatly affected by the new development. With every step towards the realization of wholly interconnected virtual systems, additional risks also come into play.

DOI: 10.4018/978-1-7998-2466-4.ch077

Technology has enabled the health sector to generate and store patient data in computer systems, the aim is to improve efficiency and safety during care since practitioners can exchange information more rapidly and accurately as compared to the older approaches. However, recent developments show increased rate of attack on systems believed to be secure, hackers are giving more attention to EHR, mostly for the purposes of extortion. Although different approaches to protecting patient information have been developed over the years, attackers evolve at the same pace, they continue to device new orthodox styles of violating cybersecurity. This paper is an investigation into modern cyberspace, including what makes it so challenging authorities to completely lock out cybercriminals from accessing private data.

Despite its assumed unimportance to cybercriminals over the years, the healthcare sector has now become a prime target for cybercriminals. Data breaches have become the norm, as highlighted by the significant number of breaches experienced by healthcare providers like Banner Health, Newkirk Products, Inc. and the Los Angeles Health and Mental Department among others in 2016. In total 16,471,765 healthcare records were exposed in 2016, a large number despite falling short of the 113,267,174 records exposed in 2015 (HIPAA, 2017). Nevertheless, 2016 data breaches were some of the worst in health plan member's records, and in-patient records revealed. These breaches have led to the scrutiny of cybersecurity technologies, protocols and strategies applied in the healthcare sector (Thomson, 2012). As such, this paper will also explore the cyberhyeine techniques available in health care that can be used to deter data breaches.

Health care entities are currently utilizing different technologies and strategies to try stopping the menace of cyber insecurity (Michael & Jason, 2017). Some have been effective, and some have not. Normal practices like password protection, encryption and firewalls have been deemed ineffective in the past few years because the healthcare industry is now plagued with the problem of insider breaches especially because of the vulnerability of cloud services that 91% of health providers are using but 47% are not protected (Martin, 2015). Despite regulatory bodies like the FDA recognizing the enormity and seriousness of the issue and offering recommendations on how to control cyber risks, the attacks continue to increase. Consequently, it has become necessary for the healthcare industry to devise new methods of cybersecurity.

Abbreviations

- EHR – Electronic Health Record
- HIPAA- Health Insurance Portability and Accountability Act
- COBIT -Control Objectives for Information and Related Technology
- DDoS - Distributed denial of service
- HTTPS - Hyper Text Transfer Protocol Secure

PROBLEM STATEMENT

A problem with online data storage relates to providing security to the information stored in the online platforms. One of the challenges of cloud storage of patient information is providing an easy and convenient access to the patient data while ensuring that such an access will not amount to a violation of owner privacy. A concerned voice cites activists relates to clearance of access to such information by the practitioner. Recent studies show that privacy violation in healthcare touches even the practitioner