Chapter 12
Opinions on Cyber Security, Electronic Health Records, and Medical Confidentiality:
Emerging Issues on Internet of Medical Things From Nigeria

Ibrahim Taiwo Adeleke
Federal Medical Centre, Bida, Nigeria

Qudrotullaah Bolanle Suleiman Abdul
University of Ilorin Teaching Hospital, Nigeria

ABSTRACT

IoMT has helped to improve health safety and care of billions of people and at least, health-related parameters can now be monitored from home in real time. This chapter deployed a cross-sectional design to determine perceptions of Nigerian healthcare providers toward medical confidentiality and cyber security in the wake of electronic health records and IoMT. Participants' opinions on the workings of EHRs in Nigeria include: security of health records (79.4%); aiding effective healthcare data backup (88.2%); enhancement of medical confidentiality (89.2%); speeding up documentation process (93.1%); and that EHRs will generally bring about positive changes in the country healthcare system. Nearly a third (31.4%) of participants have heard about audit trail, which they admitted (43.1%) have the capabilities to facilitate effective medical confidentiality. Healthcare providers in Nigeria have some concerns over security of patient health information on the Cloud, but are hopeful of the workability of IoMT for its promises to improve healthcare quality.

INTRODUCTION

Internet of things (IoT) is a combination of various technologies that empower a diverse range of ap-

DOI: 10.4018/978-1-7998-1090-2.ch012

pliances, devices and objects to interact and communicate with each other using different networking technologies (Kodali, Swamy & Lakshmi, 2015). In the healthcare context, internet of things (IoT) or internet of medical things (IoMT) extends the Web through the deployment of ubiquitous devices with capabilities for embedded identification, sensing, and data exchange features (Miorandi et al., 2012). In IoT-based healthcare, diverse distributed devices aggregate, analyze and communicate real time medical information to the cloud, thus making it possible to collect, store and analyze the large amount of data in several new forms and activate context based alarms (Kodali, Swamy & Lakshmi, 2015). IoMT plays a key role in the growth of medical information systems. IoT has potentials to collect and integrate possibly more precise, relevant, and high-quality data in real time to monitor processes and outcomes (Gupta, Maharaj & Malekian, 2016). With IoMT, patient's health records and related data can be accessed from anywhere in the world using any Internet-enabled device like PC, tablet or smart phone (Kodali, Swamy & Lakshmi, 2015). A healthcare provider can automatically collect information about the patient, applies decision support rules and as such, speed up treatment process (Chacko & Hayajneh, 2018).

The need to cut cost, improve medical care and adopt electronic health record (EHR) is driving hospitals to implement IT solutions that streamlines procedures such as billing, medical imaging and electronic medical record (EMR) processing. EHR is being defined (NAHIT, 2011) as an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization. In other words, EHR is a repository of patient data in digital form, stored and exchanged securely, and accessible by multiple authorized users. It contains retrospective, concurrent, and prospective information and its primary purpose is to support continuing, efficient and quality integrated health (Hayrinen, Saranto & Nykanen, 2008). Electronic health record has evolved to play a major role in healthcare in modern society.

IoMT allows billions of smart devices to communicate and share data, and millions of new devices are connected to the Internet every day (Gartner, 2015). It enables healthcare providers to automatically collect information and apply decision support rules to allow for earlier intervention in the treatment process (Chacko & Hayajneh, 2018). Securing healthcare data requires enforceable security policies and implementing solutions that focus on vulnerabilities, configuration assessments, malware defenses, as well as activity and event monitoring (Chacko & Hayajneh, 2018). There are three main components of information security, which are captured in the CIA Triad of TechTarget (TechTarget, 2015); confidentiality, which limits access to the information in IoT devices; integrity, which ensures that information in IoT devices is trustworthy and accurate and lastly, availability, which guarantees reliable access to the information in IoT devices by authorized people. Traditionally, healthcare organizations have proven to be eminently capable of ensuring the integrity and availability of information within their connected devices.

Yet as cyber security threats intensify, ensuring confidentiality has become increasingly difficult. Storing sensitive information such as EHRs in the Cloud means that precautions must be taken to ensure the safety and confidentiality of the data. Medical confidentiality on the other hand, is the limiting of health information to only those for whom they are appropriate (Adeleke et al., 2011). With the emergence of IoT and Cloud computing, EHR management systems are facing an important platform shift, but such important changes must be approached carefully (Rodrigues, 2013). The adoption of EHRs with information exchange among patients, providers and payers, increased regulation and provider consolidation indicate the need for better information security (Appari, 2010). Although EHRs provide considerable benefits to patients and healthcare providers, there have been concerns (Adeleke et al., 2015; Hoffman, 2007; Taitsman, Grimm & Agrawal, 2013) over confidentiality, integrity, and availability of the data.