5-5-2022

Exploration of Security Concerns Related to Personal Devices When Accessing Cloud-Based Electronic Health Records

Gargi Nandy
University of Nebraska, Omaha, gnandy@unomaha.edu

Deanna House
University of Nebraska, Omaha, deannahouse@unomaha.edu

Exploration of Security Concerns Related to Personal Devices When Accessing Cloud-Based Electronic Health Records

Gargi Nandy
MS in MIS Student
College of IST
University of Nebraska, Omaha
gnandy@unomaha.edu

Dr. Deanna House
Assistant Professor
College of IST
University of Nebraska, Omaha
deannahouse@unomaha.edu

ABSTRACT

This research explores a relatively unchartered area of electronic health records, patient security concerns related to accessing records stored in the cloud from personal devices. The healthcare industry has had increases in cyberattacks related to data breaches; with nearly two a day occurring on average. Additionally, ransomware attacks for healthcare entities have been at an all-time high. While HIPAA normally provides added protection for patients and healthcare entities, access via personal devices can sometimes fall outside of HIPAA jurisdiction. Additionally, patients are solely responsible for keeping personal devices and home network devices patched and protected. This research will provide more information related to access via unsecured home networks.

Keywords

Electronic Health Records, Cloud, Security, Privacy and Unsecured Home Networks.

INTRODUCTION

Cloud computing is gaining in popularity due to its adaptability, domain compatibility and better service use. It is gaining its popularity among various industries due to low cost and "pay-as-you-go" features (Somani et al, 2017; Rodrigues et al, 2013). Current revenue from the cloud globally is $474 billion, overall increase of $408 billion from 2021 (Gartner, 2021). According to National Institute of Standards and Technology (NIST) special publication, cloud computing can be defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011) . The concept of cloud can be differentiated due to its unique service and delivery models. The burden of on-premise hardware and infrastructure needs are completely taken care of by the cloud providers. Cloud computing generally provides three service models- infrastructure as a service (IaaS); this service provides a complete operating system to the consumers, platform as a service (PaaS); using this service users can use the platform provided by the cloud providers to develop manage and run the applications thus relieving them from creating own infrastructure which will be tedious in terms of cost, time and effort, software as a service (SaaS); using this service users can use the software provided by the cloud service and four deployment models- private, public, community and hybrid. These service and the deployment models together make cloud computing unique and cost efficient for cloud consumers (Issa, Ottom, & Tamrawi, 2019).

Adoption of Electronic Health Records (EHRs) and the need for anytime access have driven many healthcare providers to move to cloud environments. The utilization of cloud for EHR storage acts as a central data repository that provides easy access and flexibility for healthcare providers, patients, and medical facilities. The concept of EHR first started during the 1960's in the United States (Lindrud, 2015). These records typically contain personal details of patients (Personal Health Information – PHI), insurance details, past health records of the patient which includes diagnosis and prescriptions, treating physician, SSN and many more. Nowadays almost every hospital maintains electronic health records (EHRs) of their patients which are

accessible by doctors, nurses, family members (with patient consent) and even sometimes third parties (Carlson & Goldstien, 2020). Despite clear benefits, the security risks and vulnerabilities are great (Barona & Anita, 2017). According to IBM security report, data breaches in a hybrid cloud model cost up to $3.61million (IBM Security, 2021).

Patients use different forms of electronic media to access EHRs such as mobile phones, laptops, desktops and all of them use the internet, which means there is always a chance of falling victim to cyber-attacks (Manworren, Letwat, & Daily, 2016). According to mobile usage statistics, 54.8 percent of global web traffic can be attributed to mobile web traffic and 6.4 billion people are using smartphones worldwide (Lin, 2021). While the case for increases in mobile web traffic can certainly be made, many times access to EHRs often utilize an unsecured home environment or public WIFI (such as those that are accessed by the patients or medical professionals working from home). As mentioned by Hall & McGraw, 2014, home environments are not frequently patched and there is very little awareness of cyber-hygiene among individuals. These conditions increase the risk of attack by cyber criminals.

While security concerns related to cloud-based EHRs and the use of personal devices to access EHRs have been previously explored, research has focused mainly on health care providers and hospitals rather than patients. There is a need for an information systems and security lens to explore security concerns and vulnerabilities where personal devices are involved from the patients' endpoints. The challenges of the push to move to cloud EHR paired with patient record access with personal devices have increased the risk of data breach/data leakage of patient data.

LITERATURE REVIEW

Security data breaches in the healthcare industry are a matter of great concern. According to the data breach statistics report there has been an exponential rise in data breaches over the past 10 years and from 2018 to 2021 the rate of data breach incidents involving 500 or more users compromised has doubled from 1 per day to an average of 1.95 per day (HIPAA Journal, n.d.). Cost of PII (Personally Identifiable Information) per lost or stolen record amounts to $180 with an overall increase of $34 since 2020 (IBM Security, 2021). There has been a significant rise in the average cost of data breach in US in healthcare industry, from $7.13 million in 2020 to $9.23 million in 2021 and also ranks first among other industries (IBM Security, 2021).

In June 2019, an Indiana based Methodist hospital had a data breach that affected the medical records of 68,000 patients. Upon investigation it was discovered that an unauthorized individual gained access to one of the employee's email accounts which happened as a result of employees responding to phishing emails. It was reported that along with the patient names other information that was potentially compromised included address, date of birth, Social Security Number, driver's license number, state ID number, passport number, medical record number, CSN number, HAR number, Medicare number, Medicaid number, diagnosis information, treatment information, health insurance subscriber, group, and/or plan number, group identification number, financial account number, payment card information, electronic signature, username, and password (HIPAA Journal, 2019). Cybercrimes in the health field are unique because of the kind of data it deals with (Coventry & Branley, 2018). There are many concerns related to the maintenance of electronic health records and devices. Additionally, there is a high cost associated a data breach, with the U.S. at $8.19 million, the Middle East ($5.97 million), UK ($4.88 million), Germany ($4.78 million), - Ponemon Report, 2019 (Rathod, 2019).

As the majority of the workforce moved to remote work to remain productive during the COVID-19 pandemic, the need for cloud-based systems increased drastically. Many physicians and nurse practitioners were working remotely and accessing EHRs using personal devices to diagnose patients (American Medical Association, 2020). These networks are either provided by the local internet service providers or the mobile networks and hence they have their own set of security and privacy protocols (Mandal & Khan, 2020) and hence are not HIPAA (Health Insurance Portability and Accountability Act) compliant. On the patient side, this is even less regulated and monitored with patients left to determine their own secure practices for EHR access. As mentioned by (Davis, Mason, & Anwar, 2020) there is an urgent need to focus strongly on the security infrastructure provided by these third-party vendors who are often less monitored and regulated.

HIPAA is a governing authority in the US that protects sensitive patient health information from being disclosed. It was established in the year 1996. According to HIPAA, only covered entities (includes health plans, health care providers, health care clearing house) fall under HIPAA by signing a Business Associate Agreement (BAA). This agreement assures that any violation of the law will be subjected to criminal penalties (HHS.gov, n.d.) and when the patients' personal devices are involved there are some grey areas that still need to be sorted out.

Use of untrusted networks in the health care sector can cost more than expected. There is always a chance of Man-in-the-middle attacks where an intruder can easily intercept the entire data that patient browses (Sombatruang, Onwuzurike, Sasse, & Baddeley, 2019). Many home users are in the false belief that their home network is either too small to be targeted or is secure

enough that it cannot be attacked (Cybersecurity & Infrastructure Security Agency, 2020). Digital literacy among people living in remote areas is very limited, which leads to a less secure home network (which includes weak/no WIFI password) (Wang & Alexander, 2021). The chances of cyberattacks like ARP spoofing, IP spoofing, MAC spoofing, Cache spoofing and DDoS attacks increases. Some of the attacks like Cache spoofing are easily spread through network connection and can compromise the entire system (Mandal & Khan, 2020).

It is common for people to use cell phones for both official and personal use, as it is very convenient and handy. As mentioned by Freidman & Hoffman, 2008, mobile devices are very vulnerable to cyber-attacks similar to a computer or laptop. External agents can gain unauthorized access to one's cell phone using sophisticated spyware and it will be enough to conduct any nuisance activities (both at the personal and political level). When an individual uses the same cell phone to access their health records using their credentials, the bad actors can have a complete control of the patients' activity. There are possibilities that the hacker can use privileged account information to send an email appearing to originate from a health care provider with a malicious attachment. Once the attachment is opened, the hacker can have a complete control of the machine without the patient knowing. As mentioned by (Thompson, McGill, & Wang, 2017), personal devices pose a greater threat as the patients either have limited technical knowledge or lack of self-awareness on security risks. While policies such as Bring Your Own Device (BYOD) are in place in healthcare organizations, these typically focus on the expected use for healthcare providers, not patients. Therefore, patients are left to fend for themselves for security and protective matters.

RESEARCH QUESTIONS

Much of the research surrounding e-health and cloud computing that has been previously explored mainly focused on finding different security vulnerabilities due to flaws in cloud security infrastructure. The research is very limited related to security challenges from the patients' end when using personal devices to access confidential medical records. For the purposes of this research, we are focusing on the patient.

Therefore, our research questions are as follows -

RQ1 – What are the current policies (including guidelines, regulations, and laws) in place for patients using personal devices to access Electronic Health Records?

RQ2 – What are the security vulnerabilities associated with using unsecured networks to access confidential PHI data (in our case EHRs)?

RQ3 - What are minimum recommended cyber-hygiene practices that a patient should utilize to prevent from falling victim to cyber-attacks?

METHODOLOGY

The researchers have explored data surrounding healthcare data breaches and data leakage in cloud environments to understand the challenges faced by healthcare providers. While this is important information to take into consideration, the patients' perspectives are missing from the HIPAA mandated reports.

The researchers plan to collect survey data to determine risks that consumers take such as accessing secure information over public Wi-Fi, having unpatched systems, and not using multi-factor authentication. The survey questionnaire will be distributed via Qualtrics and will focus on items such as: demographics, technology use, security utilization, security knowledge, type of hardware and security incidents. This will help to determine how patients utilize home devices for electronic health record access.

EXPECTED CONTRIBUTIONS

The research will provide insights surrounding EHR cloud-based access utilizing home devices and focus on finding the root cause of attacks to determine where security and policy gaps may exist. The research helps us provide key areas to focus mitigation efforts and to predict better risk assessment and risk management strategies to understand vulnerabilities. Many cyber-attacks are related to the inability of an individual in understanding and maintaining cyber-hygiene. Hence, this study will also demonstrate cyber awareness of patients and work to define better strategies for preventing attacks and protecting patient EHR data.

REFERENCES

Ambrose, P. J., & Basu, C. (2012). *nterpreting the Impact of Perceived Privacy and Security Concerns in Patients' Use of Online Health Information Systems*, *8*(1), 38-50.

Barona, R., & Anita, E. M. (2017). A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats. *2017 International Conference on circuits Power and Computing Technologies [ICCPCT]* (p. 2). IEEE Xplore.

Carlson, J. L., & Goldstien, R. (2020). Using the Electronic Health Record to Conduct Adolescent Telehealth Visits in the Time of COVID-19. *Journal Of Adolescent Health*, 157-158. doi:https://doi.org/10.1016/j.jadohealth.2020.05.022

Coventry, L., & Branley, D. (2018). *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward*, *113*, 2-4. Retrieved from https://doi.org/10.1016/j.maturitas.2018.04.008

Cybersecurity & Infrastructure Security Agency. (2020, Nov 03). Security Tip (ST15-002) Home Network Security. Retrieved from CISA: https://www.cisa.gov/uscert/ncas/tips/ST15-002

Davis, B. D., Mason, J. C., & Anwar, M. (2020, Oct 10). Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. Internet of Things Journal, 7(10), 10102-10109. doi: 10.1109/JIOT.2020.2983983

Fernandez-Aleman, J.L., Senor, I.C., Lozoya, P.A.O., & Toval, A. 2013. Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics*, (46), pp. 541 – 562.

Gartner. (2021, November 10). *Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences*. Retrieved from Gartner: https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences

Hall, J. L., & McGraw, D. 2014. "For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed", *Health Affairs, (33*:2), pp. 216-221. doi:10.1377/hlthaff.2013.0997

HHS.gov. (n.d.). *Your Rights Under HIPAA*. Retrieved from HHs.gov Health Information Privacy.

HIPAA Journal. (2019, Oct 9). *68,000 Patients of Methodist Hospitals Impacted by Phishing Attack*. Retrieved from 68,000 Patients of Methodist Hospitals Impacted by Phishing Attack: https://www.hipaajournal.com/68000-patients-of-methodist-hospitals-impacted-by-phishing-attack/

HIPAA Journal. (2020). *2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape*. Retrieved from https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

HIPAA Journal. (n.d.). *Healthcare Data Breach Statistics*. Retrieved from HIPAA Journal: https://www.hipaajournal.com/healthcare-data-breach-statistics/

IBM Security. (2021). *Cost of Data Breach Report 2021*. Retrieved from https://www.ibm.com/downloads/cas/OJDVQGRY

Issa, Y. A., Ottom, M. A., & Tamrawi, A. (2019, September 3). eHealth Cloud Security Challenges: A Survey. *Journal of Healthcare Engineering*. Retrieved from https://doi.org/10.1155/2019/7516035

Koonin, L. M., Hoots, B., Tsang, C. A., Leroy, Z., Farris, K., Jolly, B. T., . . . Harris, A. M. 2020. Trends in the Use of Telehealth During the Emergence of the COVID-19 Pandemic — United States, January–March 2020. MMWR Morb Mortal Wkly Rep 2020, (69:1), pp. 595–1599

Lin, Y. (2021, June 20). *10 MOBILE USAGE STATISTICS EVERY MARKETER SHOULD KNOW IN 2021 [INFOGRAPHIC]*. Retrieved from Oberlo: https://www.oberlo.com/blog/mobile-usage-statistics#:~:text=There%20are%206.4%20billion%20smartphone,apps%20on%20their%20mobile%20devices.

Lindrud, S. D. (2015). The Evolution of the Electronic Health Record. *Clinical Journal of Oncology Nursing*, *19*(2), 153-154. doi:10.1188/15.CJON.153-154

Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. *IEEE Xplore*. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9215374

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *BUSINESS LAW & ETHICS CORNER*, 262-266. Retrieved from http://dx.doi.org/10.1016/j.bushor.2016.01.002

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Special Publication 800-145. pg. 6. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-145/final

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A Comprehensive survey on security in cloud Computing. *110*, 465-472. doi:10.1016/j.procs.2017.06.124

Rathod, L. (2019). *Cost of a Data Breach: Ponemon Institute Report*. Retrieved from https://diligent.com/en-gb/blog/cost-of-a-data-breach-ponemon-institute-report/

Rodrigues, Joel JPC., de la Torre, I., Fernandez, G., Lopez-Coronado, M. 2013. Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems. *Journal of Medical Internet Research*, 15(8), pp. 1-9.

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, 30-48. doi:http://dx.doi.org/10.1016/j.comcom.2017.03.010

Sombatruang, N., Onwuzurike, L., Sasse, M.A., & Baddeley, M. 2019. "Factors Influencing Users to Use Unsecured Wi-Fi Networks: Evidence in the Wild", in *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19),* May 15 – 17, Miami, FL.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 376-391. doi:http://dx.doi.org/10.1016/j.cose.2017.07.003