7-22-2021

Telemedicine Security: Challenges and Solutions

Crystal Fausett
Embry-Riddle Aeronautical University, fausetc1@my.erau.edu

Joseph R. Keebler
Embry Riddle Aeronautical University, keeblerj@erau.edu

Megan C. Christovich
Embry-Riddle Aeronautical University

Jarod M. Parker
Embry-Riddle Aeronautical University

John M. Baker
Embry-Riddle Aeronautical University

TELEMEDICINE SECURITY: CHALLENGES AND SOLUTIONS

Crystal M. Fausett, Megan C. Christovich, Jarod M. Parker, John M. Baker, & Joseph R. Keebler
Embry-Riddle Aeronautical University

The proliferation of telemedicine spurred by the COVID-19 pandemic has come with a variety of human factors challenges. Such challenges include mitigating potential risks associated with the quick transition to virtual care. We identify challenges and solutions related to telemedicine security, and analyze our results using Schlarman's People, Policy, Technology framework (2001). Our systematic literature review synthesizes gray literature (white papers, news articles, and blog posts) in addition to formal (published) literature. This methodology closes the gap between academic research and professional practice and aids in providing timely, practical insights related to cybersecurity and safety in virtual care environments. As the transition from traditional care continues to develop, we seek to better understand emerging vulnerabilities, identify crucial cyber hygiene practices, and provide insights on how to improve the safety of paitent data in virtiual care. Telemedicine is here to stay, and lessons learned from the pandemic are likely to remain useful.

INTRODUCTION

Telemedicine is defined as "a term used to describe any care provided that involves an element of distance from the patient" (World Health Organization, 2020). Telemedicine encompasses all virtual patient care, whether a practitioner is conducting a phone call consultation or performing telerobotic surgery across the Atlantic Ocean. Telemedicine has allowed for patients in underserved rural areas to access quality care, practitioners to collaborate on digital medical records, and granted easier patient access to specialists. These benefits are accompanied by increased risk. The connection and exchange of data with other devices and systems over the internet has can introduce security vulnerabilities. Although telemedicine has been around for centuries, it has gained popularity in recent months as a result of the COVID-19 pandemic. As telemedicine becomes more prominent, it becomes increasingly important to reevaluate the role cybersecurity plays in healthcare.

In 2018, cybersecurity was named one of the greatest challenges in the healthcare industry (Healthcare Executive Group, 2018). Since then, the proliferation of telemedicine during the pandemic has drawn attention to security challenges faced in healthcare. As of 2020, less than half of providers across the healthcare continuum meet standards put forth by the National Institute of Standards and Technology cybersecurity framework (Cynergistek, 2020). With the level of virtual care appointments increasing at a drastic rate, many security measures have failed to catch up to the demand of telemedicine services.

Cybersecurity is typically not a buzz word when discussions around patient safety occur. However, secure cyber behaviors can protect the safety of patient data. Protected health information includes any form of patient data, such as name, medical record number, and email addresses. This data, while seemingly innocuous, is valuable on the black market. This makes telemedicine services and platforms a prime target for cyber attacks. Protected health information, such as patient medical records, are uniquie in that they have a lot of personally identifiable information in one place. While a credit card number might be valuable to hackers, a medical record is more desirable. A recent report names healthcare providers and hospitals, as well as consumers, the most popular targets during the pandemic (Microsoft, 2020). There has been an alarming increase of mentions regarding telemedicine platforms and services on the dark web, a part of the internet not indexed by search engines that is flush with criminal activity (Security Scorecard, 2020). Hackers access the dark web to turn their stolen healthcare data into profit. Medical credentials are far more valuable than credit card data on the black market, sometimes yielding over $1,000 US dollars (Wani et al., 2020).

More profitable and more dangerous attacks on the healthcare industry can occur. Ransomware is a malicious software program that demands you pay a fee in order for your systems to work again. At least 92 healthcare ransomware attacks occurred in 2020, involving the compromise of protected health information of at least 18,069,012 patients (Adler, 2021). Exact figures are often unknown, but between 2016-2020, the overall cost of ransomware attacks on the healthcare industry are estimated to be $31 billion (Adler, 2021). Ransomware attacks can also be deadly. The University Hospital Düsseldorf (UKD) in Germany suffered a ransomware attack on September 10, 2020. This event caused a patient with a life-threatening illness to be diverted to a more distant hospital, as the University Hospital of Dusseldorf was deregistered for emergency services during the attack (Ralston, 2020). The additional hour's travel may have been the cause of the patient's death, which would make this the first known death caused by hacking. More than ensuring the security of patient data, enhanced cybersecurity measures in the healthcare industry can save patient lives.

Cybersecurity can be seen as a human factors problem, as people are often implicated as the weakest link in cybersecurity (Schneier, 2000). While this statement has been controversial, it does exemplify that many investigations of how to improve seucrity often ignore the human element. The implementation of successful security measures cannot be done through technology alone, and necessitates involvement from those who use the technology (Talib et al., 2010). Human factors specializes in areas where humans interact with virtual environemts, such as cyberspace. Telemedicine falls into this category, as does cybersecurity. Here, we offer solutions grounded in human factors to the People, Policy, and Tech-

nology (Schlarman, 2001) challenges of telemedicine cybersecurity.

Meager cybersecurity progress combined with a surge of telemedicine practices and valuable patient data ensures that the healthcare industry will remain easy prey, unless serious preventative measures are taken. As the transition from traditional care continues to develop, this work seeks to better understand emerging vulnerabilities, identify crucial cyber hygiene practices, and communicate prescriptive guidance to the healthcare community. Below we outline our systematic literature review, coding process, and results.

Research Design

Our team conducted a two pronged systematic literature search that incorporated formal literature and gray literature. Formal literature is academic in nature, typically characterized by evidence-based, peer-reviewed journal articles that are found in scientific databases. Systematic literature reviews have been used widely in the domain of human factors, but have been critique for their failure to providing a complete picture. This is likely because systematic literature reviews usually ignore "gray literature," which is often produced by practitioners outside of typical academic settings. With the incorporation of gray literature, we reduce the gap between academia and industry, incorporate perspectives that may be missing from peer-reviewed research, and provide practical insights about telemedicine and security that are immediately applicable.

Gray Literature. Gray literature can be further classified into tiers based on Garousi et al. (2019). Tier 1 literature is described as being ranked the highest in terms of outlet control and expertise, housing literature such as books, government reports, and white papers. The 2nd tier is less rigorous in terms of expertise and outlet control, housing annual reports, news articles, and presentations. The 3rd tier of gray literature is comprised of elements with unknown expertise and outlet control such as blogs and tweets. Only 1st and 2nd tier literature were chosen to be included in this review.

For this review, we first instituted a traditional systematic literature review process, which involved searching multiple databases with predetermined keyword searches. The selected articles from these databases were then combined, and analyzed for viability against our predetermined inclusion and exclusion criteria. Articles were excluded in three phases. The first phase, a title elimination phase served to weed out articles that were immediately irrelevant to the topic at hand (such as mental health). The second phase consisted of eliminating items based on abstracts that did not align with inclusion criteria. The third phase, full-text elimination, removed articles that initially appeared relevant, but did not meet some aspect of inclusion criteria. Following full-text review, remaining articles were analyzed deductively to answer research questions in the qualitative synthesis phase.

Qualitative Synthesis. A qualitative synthesis was chosen as the method for analyzing data from our gathered articles. The research team used the Policy, and Technology (Schlarmann, 2005) to identify and classify the challenges and solutions of telemedicine security.

METHODS

Inclusion and Exclusion Criteria

Articles were included form 2017-2020 to ensure practical relevance. Articles reviewed were only in English. Further, our search was limited to security issues related to telemedicine for hospitals and private practices. Articles were excluded if they pertained to the efficacy of telemedicine as a practice. In addition, articles were excluded if they sought to compare the efficacy of different telemedicine methods such as different watermarking or cryptography forms. Exclusion criteria also included articles with a focus on things other than security as it pertains to telemedicine, such as bandwidth structure.

Formal Literature Search

A search in December 2020 was conducted in abstract and citation databases PubMed, Scopus, and Web of Science. The following selection of 2 keywords was used: "telemedicine" and "security." These searches identified a total of 1,612 articles. Of these, 527 articles were found to be duplicates and discarded, leaving 1,085 unique articles. A consensus procedure was developed to eliminate articles based on titles that did not relate to telemedicine or security. Inter-rater reliability agreement among 4 raters was 83.1 percent. Differences among raters were discussed until a 100 percent consensus was achieved. Using this method and exclusion criteria, 654 articles were found to not be suited for this study and removed, advancing 431 articles for abstract review. The same consensus procedure was applied to abstract elimination, with inter-rater reliability reaching. Differences among raters were discussed until a consensus was achieved. Upon elimination, 330 articles were removed, advancing 101 articles forward for full text review. Based on full text review, only 35 formal literature articles were determined to reach inclusion criteria. These 35 articles were included in the qualitative synthesis.

Gray Literature Search

Our gray literature search employed the same criteria as our formal literature review, conducted in January 2021. First, Xtelligent Healthcare Media and HIMSS, both specialized and credible health information technology resources, were searched. Second, literature resources searched from Google that fit quality assessment were considered. This included white papers, national healthcare department guidelines, and frameworks from reputable resources and organizations. Only the first 100 Google results were included as they provided a sufficient sample, and a noticeable saturation of concepts occurred beyond this. Our initial search captured articles from Xtelligent Healthcare Media (n = 200), HIMMS Media (n = 407), and Google (n = 100). Articles were first assessed for relevance based on title, following the same methodology as the formal literature. 531 articles were eliminated based on title. This left 134 articles for full text eligibility. Quality assessment was conducted to ensure that gray literature sources were credible. 6 pillars of quality were examined for each

piece of literature, including authority (is this from a reputable source?), methodology (does the source have a clearly stated goal?), objectivity (is the source as unbiased as possible?), data (Does the source have a clearly stated date?), novelty (does the source enrich or add something new to the discussion?), and related sources (have related formal or gray literature sources been discussed or linked?) (Garousi et al., 2019). Of the 134 relevant articles, 30 were found to be irrelevant, 7 were duplicates, and 3 were removed for failure to meet strict quality guidelines. This led to the ultimate inclusion of 94 pieces of gray literature in qualitative synthesis.

Qualitative Synthesis

We evaluated selected articles using a systematic approach, codebook, and spreadsheet. A consensus on how to extract information was reached by the team coding a small sample of articles together. Schlarman's People, Policy, and Technology (2001) model allowed us to break down the security process within a healthcare setting into its core elements: 1) people responsible for supporting the security process, 2) policy used to provide direction for ideal security behavior, and 3) various technologies used including products and tools that support the security process. Gray literature documents were further assessed for quality by authority of source, method, date, objectivity, novelty, and impact (Garousi et al., 2019).

RESULTS

People Challenges

Lack of training. Employees are often the weakest link in cyber network defense (Davis, 2020a). Ideally, this would prompt organizations to conduct frequent employee trainings. Unfortunatley, many organizations place an emphasis on technology-centric solutions while ignoring the human element of cybersecurity.

Social engineering attacks. Social engineering is the art of convincing someone to act in a way that is not in their best interest (Hadnagy, 2018). Social engineering attacks are aimed at humans, generally geared towards convincing them to give access to restricted systems or secure information. Attacks such as malicious links, ransomware attacks, and phishing emails have played a role in many healthcare data breaches.

Use of personal devices. The COVID-19 pandemic has caused a rise in the number of people working from home. The use of personal devices on a home network makes security more vulnerable, as there is a lack of network infrastructure support that we would typically see in a hospital setting.

Lack of physical security. It is possible that information is shared on different devices and accessed by different employees (Jumreornvong et al., 2020). Threats to patient privacy may exist if the physical device security is compromised.

People Solutions

Security culture. Ensuring that individuals employed in a healthcare setting have access to resources regarding policies, procedures, and their role in keeping patient data secure and their organization resilient against cyber attacks are important. Another important piece of security culture is fostering improvement over blame. Incident reporting should be encouraged, as this will help organizations to better prepare for and anticipate adverse events that may occur as a result of telemedicine care.

Awareness and training. Individuals across different roles in a hospital setting should be thinking about what actions they would take in incident response and the possible impact a cyber attack could have on patient care. This can be accomplished by having individuals within a healthcare setting participate in tabletop exercises and other simulations of cyber attacks (CITE). In addition, healthcare providers should receive training and demonstrate proficiency with the technology systems in use (including but not limited to telemedicine platforms).

Policy Challenges

Lack of direction. There is a lack of ground covered by existing ethical, legal and regulatory guidelines when it comes to virtual care (Kluge et al., 2018). Telemedicine curriculum should train future providers to deal with the ethical, legal, and regulatory implications of telemedicine (Jumreornvong et al., 2020).

Data protection. Policies often aim towards protecting the confidentiality of patient information. However, increased virtual care during the COVID-19 pandemic could dramatically increase privacy and security risks.

Data ownership. Who owns healthcare data, and what occurs to that data throughout it's lifecycle is a point of contention. As data travels from collection, storage, use, disclosure, and disposal, who is responsible for ensuring its protection and security?

Policy Solutions

Strategy and governance. Healthcare organizations and professionals shall comply with both state and federal regulatory guidelines (i.e, HIPAA) (Richmond et al., 2017). Robust privacy and security plans should not only be implemented, but disclosed to patients.

Implementing and updating telemedicine protocols. Guidelines and policies regarding patient and provider interactions should be transparent (Spagnuelo & Lenzini, 2017). Patient health information has been accumulated, especially during the pandemic, and a variety of different entities may have access to it: health providers, medical device vendors, health insurance companies, pharmaceutical companies, telemedicine platforms, and advertisers (Bassan, 2020). Patients should know what happens to their health data, the circumstances under which is is shared, and how it is secured.

Technology Challenges

Personal Devices. During the pandemic, we have seen an increase in working from home. However, without the network infastructure that would normally exist in a larger hospital setting, many personal devices can become easy targets for attackers to infiltrate the larger network.

Network security. Inappropriate or unauthorized access to secured networks can be devastating for patients and costly for healthcare providers.

Insufficient security controls. Without encryption, login redundancies (such as multi-factor authentication), and intrusion detection tools, telemedicine portals may be left vulernable to malicious actors (Davis, 2020a).

Technology Solutions

Multi-factor authentication. A key way that the healthcare community can mitigate security vulnerabilities is by implementing multi-factor authentication on all endpoints across the network (Davis, 2020a). Multi-factor authentication provides another level of security beyond typical login credentials. After entering a passcode, users of the virtual care system (patients and providers alike) would also have to provide an additional verification mechanism, such as phone number or fingerprint. Even if a users device, username, or passcode are compromised, multi-factor authentication can help protect the healthcare organizations network.

Performing regular assessments. Mechanisms shall be put in place to scan for any vulnerabilities, ensuring that equiptment is safe to support the needs of patients and physicians while securely transmitting their data (Richmond et al., 2017). Ensuring data security, privacy, and integrity within virtual care systems should be a priority for healthcare organizations.

Secure and encrypted platforms for communication. Even with the best technology, systems can still be unsafe (Langarizadeh et al., 2017). Telemedicine portals, such as those where patients view medical reocrds and renew perscriptions, are trusted to be secure. Maintating this security by monitoring patient and provider logins, double-checking suspicious activity, and responding quickly to compromises are essential.

DISCUSSION

The following are initial results regarding people, policy, and technology challenges and solutions for telemedicine security. People-related challenges associated with telemedicine are plentiful, including human error and system misuse. These challenges can be mitigated by implementing standard cyber hygiene practices, education and training, and instilling a sense of security culture. Policy-related challenges include a lack of clarity regarding data ownership, data protection, and maintaining legislative compliance. Solutions include defining telemedicine protocols and updating them regularly, reporting incidents and breaches, and performing regular risk assessments. Technology-related challenges include weak authentication mechanisms, vulnerable devices, and data storage. Solutions include multi-factor authentication, network monitoring, and using secure communication platforms. Results from our literature review provide guidance on how we leverage human factors to ensure the safety of patient data and cybersecurity in virtual care environments.

Limitations

Gray literature selected for review in this paper underwent a rigorous quality assurance process. Included gray literature majorly consisted of credible experts writing for well known media publications. While incredibly useful for the purpose of identifying challenges and solutions in real-time, these articles do not meet criteria for being sources of the highest quality as do their formal counterparts. In addition, gray literature searches often yield a much larger number of items to review in comparison to formal literature searches. Limiting the number of items analyzed was unavoidable, authors acknowledge this may mean that important sources were neglected.

CONCLUSION

Increased telemedicine in light of the COVID-19 pandemic has patients and providers alike exploring new technologies and virtual care. However, as the healthcare communities digital footprint grows larger, cybersecurity is not often highly prioritized. Future research could further investigate patient perceptions of healthcare cybersecurity. One source of inquiry would be to investigate how patient willingness to use telemedicine is influenced by privacy and security concerns. Another source of inquiry would be assessing the effect of improved cybersecurity training and awareness programs. Knowledge regarding cybersecurity and patient safety in virtual environments is likely to remain valuable, and better understanding the current challenges and proposed solutions through a socio-technical framework can provide useful insights towards this end.

REFERENCES

Cynergistek (September 17, 2020). Moving forward: Setting the direction. 2020 Annual Report.

Adler, S. (2021, March 11) Cost of 2020 US Healthcare Ransomware Attacks estimated at $21 Billion. https://www.hipaajournal.com/cost-2020-us-healthcare-ransomware-attacks-21bn

Davis, J. (2020a, March 20) Best practice cybersecurity methods for remote care, patient portals. https://healthitsecurity.com/news/best-practice-cybersecurity-methods-for-remote-care-patient-portals

Davis, J. (2020b, October 30). Rapid threat evolution spurs crucial healthcare cybersecurity needs. https://healthitsecurity.com/features/rapid-threat-evolution-spurs-crucial-healthcare-cybersecurity-needs

Healthcare Executive Group (2018) HCEG top 10. https://hceg.org/hceg-top-ten/

Hadnagy, C. (2018) Social Engineering (COMPLETE)

Garg, V., & Brewer, J. (2011). Telemedicine security: a systematic review. Journal of diabetes science and technology, 5(3), 768-777.

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology, 106, 101-121.

Microsoft (2020). Microsoft digital defense report. https://www.microsoft.com/en-us/security/business/security-intelligence-report

Ralston, W. (2020, November 11). The untold story of a cyberattack, a hospital, and a dying woman. https://www.wired.co.uk/article/ransomware-hospital-death-germany

Security Scorecard (2020). Listening to Patient Data Security: Healthcare Industry and Telehealth Cybersecurity Risks Report. https://securityscorecard.com/resources/healthcare-industry-telehealth-cybersecurity-risks-report

Schlarman, S. (2001). The people, policy, technology (PPT) model: core elements of the security process. Information systems security, 10(5), 1-6.

B. Schneier, Secrets and lies. Indiana: Wiley Publishing, Inc., 2000.

Talib S, Clarke NL, Furnell SM. An analysis of information security awareness within home and work environments. In: Proceedings of the International Conference on Availability, Reliability, and Security; 2010. pp. 196–203. doi:10.1109/ARES.2010.27.

Wani, T. A., Mendoza, A., & Gray, K. (2020). Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. JMIR mHealth and uHealth, 8(6), e18175.

World Health Organization. (2020, March 19). Rational use of personal protective equipment (PPE) for coronavirus disease (COVID-19): Interim guidance, 19 March 2020 (World Health Organization Publication No. WHO/2019-nCoV/IPC PPE_use/2020.2).