# Improving Cybersecurity for Telehealth Patients

Written by Kacey Rose

Edited by Eva Nobles
Reviewed by Dr. Keya Sen

The use of technology in the healthcare sector, or telehealth, has skyrocketed, leading to an increased risk of criminals illegally accessing patient medical and personal information. This unauthorized access is predominantly driven by the profit hackers make from accessing patient information. The following paper will focus on some of the main points of weakness that need improvement to prevent cyber attacks, the importance of patient technology education and HIPAA-regulated digital platforms, and the benefits that will arise for both patients and clinic staff by addressing this security issue. I have selected this topic because of my history with telehealth services and interest in protecting patient information. Research on this aspect of the medical field is important because of the increasing use of technology to improve connectivity and efficiency within healthcare organizations.

New technological advancements- and the necessity for these tools during the recent pandemic- has led to technology becoming an integral part of healthcare in the telehealth delivery format. Telehealth can be defined as providing health-related services through telecommunications or other digital communication methods (NEJM Group, 2018). It serves many purposes, such as virtual medical counseling, remote patient monitoring, coordination between medical staff, communication between patients and healthcare providers, as well as electronic database storage of all patient records. With the increase in technology use, the risk of unauthorized access to a patient's medical and personal information also increases. Strong cybersecurity in the healthcare industry is imperative in order to "avoid legal ramifications, medical fraud, and the reputational damage of leaked patient data" (CareersinCyber.com, 2020). This paper investigates why unauthorized access to patient information occurs and how reducing its risk will benefit both patients and healthcare workers.

Digital healthcare leaks occur at a distressing rate due to the incentives for hackers to access patient information. On average, the number of records exposed in a single data leak event is around 25,500 in the United States, but the total number of healthcare records that were exposed, stolen, or illegally disclosed in 2019 was 41.2 million in 505 healthcare data breaches (Seh et al., 2020). The amount of people affected by the healthcare field's ineffective strategies against hackers is growing. A report from Tenable, one of the world's leading cybersecurity firms, describes more than 22 billion records being leaked within approximately 700 data breaches between January and October of 2020 alone (Camarines & Camarines, 2021). Most hackers benefit from these leaks monetarily and are not going to cease their attacks on the healthcare sector any time soon. A 2019 CBS article reports that a single full medical record including date of birth, Social Security, address, etc can bring up to $1,000 because of the multitude of information enclosed (CBS Interactive Inc, 2019). As mentioned previously, if the average number of records accessed in a single leak is 25,000, and full medical records can sell for up to $1,000, then the perpetrator could potentially profit up to $25,000,000. By gaining unauthorized access to personal files, they can sell information like medical identification numbers, credit card numbers, or government issued IDs on the dark web for a high price. If they find a patient's insurance information, hackers can even produce counterfeit insurance claims or illegally obtain their prescriptions (Camarines & Camarines, 2021). The loss of all this information is detrimental not only to patients' livelihood and financial state, but also to the trust they place in their healthcare organizations to protect this vital information. Whenever patient information is being stored or shared online, the utmost priority should be privacy and security.

In order to secure patient information, we must understand how to prevent attacks on telehealth. Ensuring Health Insurance Portability and Accountability Act (HIPAA) compliance is the most important step to prevent cyber attacks. According to the Centers for Disease Control and Prevention (CDC), HIPAA is a federal law that established a standard protocol of protection against the exposure of patient information without their knowledge or consent (CDC, 2022). The use of non-HIPAA compliant platforms poses a threat to the protection of patient information. During the recent state of emergency due to the pandemic, the US Department of Health and Human Services allowed healthcare organizations to use popular video chat platforms such as FaceTime, Google Hangouts, Zoom, or Skype to make access to care easier for patients (Jalali et al., 2020). However, because these applications are not HIPAA compliant, there is no proactive legislation in place to prevent data information leaks through these platforms (Office for Civil Rights, 2022). During the pandemic, there was a reported 25% increase in successful cybersecurity attacks (Ignatovski, 2022). In situations where data breaches are not protected by HIPAA, the Federal Trade Commission has the authority to handle any information compromises, but only after the information has been exposed (Maximus Federal Services, 2012).

The use of HIPAA compliant platforms is more effective because HIPAA is a proactive statute that protects patients' information from vulnerability by deterring violators with the knowledge that they could be punished with both civil and criminal penalties. Civil violations are constituted by three tiers of severity: The first tier is defined by lack of knowledge that the infraction was a violation despite sensible diligence, the second includes reasonable cause for the violation, and the third is specified by willful neglect that resulted in the violation. Civil violators of HIPAA face punishment of up to $1.5 million in fines. In contrast, a criminal violation consists of the illegal access to patient information with knowledge that the act is in violation of HIPAA; criminal violations can then be further categorized into whether the offense was under false pretenses or for personal gain/malicious reasons. Violators can face up to $250,000 in fines and up to ten years in prison ("HIPAA Violations and Enforcement," n.d.). Given HIPAA's proactive nature and hefty punishments for violations of patient privacy, healthcare organizations should only use HIPAA-compliant telehealth platforms to better protect patients.

It is not just the telemedicine platforms themselves that must be more secure. The healthcare sector should take the next step and model its entire digital infrastructure after other high-risk industries, like financial or government institutions. Nevertheless, implementing effective protection against cyberattacks on telemedicine platforms is complicated and must be multifaceted to be successful (Kim et al., 2020). In the financial sector, all banks must file suspicious activity reports that indicate possible criminal intent within 30 days of "initial detection of facts that may constitute a basis for filing" ("Suspicious activity reports [SAR]," n.d). The healthcare sector could use these reports as the first line of defense, which should then be followed up on by a specific department within the organization or further investigated by a federal bureau, like the Department of Health and Human Services or the Federal Trade Commission. A second possibility in building a better defense is to generate multiple layers of protection against a cyber attack. In fact, the National Institute of Standards and

Technology describes in-depth defense as the "application of multiple countermeasures in a layered or stepwise manner" and as the basis of an efficient security system (Stouffer et al., 2017). Finally, the system should then be put through consistent tests to search for potential weaknesses (Scott, 2022). A few additional measures could include encrypting data, keeping software updated, and requiring two-factor authentication prior to granting database access. Overall, healthcare technologists have many options to consider as they build a strong defense against hackers and cyber attacks.

The healthcare industry already educates both patients and staff on how to identify and correct weaknesses in their interactions with the digital world. Studies dating back to the early 2000s mention the potential risks we see today (Parimbelli et al., 2018). Some steps have been taken to mitigate the risk of serious legal implications related to non-consensual sharing of patient information. For example, patients are required by law to give informed consent prior to participating in telehealth medical counseling, though the laws vary in these circumstances. Other common requirements include educating patients on ensuring their privacy by recommending that they step into a separate room or use headphones to reduce the risk of eavesdropping. Physicians are also required to disclose the presence of any observers and receive the patient's permission for these observers to remain during the appointment ("Obtaining informed consent," 2021). These requirements ensure that a patient is aware of and accepts the possibility that their personal or medical information could be shared with outside parties on purpose or by accident.

While the healthcare industry and physicians try their best to educate patients on the potential risks, patients' lack of overall digital knowledge still creates problems. The quickening evolution of technology makes it increasingly difficult to efficiently use one's devices. As technology becomes more complex, people's inexperience with these new devices could increase the risk of their information being accessed without their knowledge (AHIMA Foundation, 2022). For instance, this knowledge deficit leads patients to use weak passwords, click on phishing or spam emails, or even lose a device used for medical purposes with information still stored in it (Kim et al., 2020). Many patients may use simple passwords that include personal information or common sequences to make them easy to remember; however, this simplicity allows hackers to quickly determine the password. Additionally, if a patient clicks on spam/phishing emails, the hackers can access the information stored on the device and circumvent the need for passwords all together. Another major weakness area is the use of unprotected Wi-Fi networks. Unprotected networks give access to all devices that are connected and allow hackers to effortlessly steal information stored on these devices (Hall & McGraw, 2014). Stronger device and network security is an integral aspect of improving protection of patient information. A recent poll showed most people are in favor of stronger device security and are willing to sacrifice user-friendliness for this increased protection ("4 Challenges Facing the Health Care Industry," n.d.). Increasing patient knowledge on how they can prevent their information from being obtained could be provided through learning courses or awareness announcements distributed by their healthcare organizations.

Improving telehealth security will have multiple important implications since data leaks jeopardize the patient's identity and financial information when it is not sufficiently protected. While there are some laws regarding patient information and informed consent, these laws are not enough to prevent cyber attacks. The keys to reducing the risk of unauthorized access to patient information are recognizing motivations for hackers, detecting areas of weakness, and formulating digital defense strategies. Some of these strategies could include filing suspicious activity reports, developing layered cyber attack defense plans, running frequent tests on the defense plans, encrypting sensitive data, keeping software updated, using 2-factor authentication, and strictly using telehealth platforms that comply with HIPAA regulations. Most notably, patients will feel safer and more comfortable when using telehealth for medical counseling. Additionally, the proper protection of patient information ensures the information is not tampered with as this could have "serious effects on patient health and outcomes" (Riggi, n.d.).

When the risk to patient information leaks are less likely, patients feel more confident in using telehealth platforms, and in turn, providers are more willing to use digital methods to communicate with them As the number of patients physically visiting a clinic decreases, the physical demands for clinic staff will also decrease, helping to alleviate some of the stress in working in healthcare. Since telehealth options are so flexible, these changes could also reduce provider burnout rates. Finally, should another emergency situation like the recent pandemic arise, the changes needed to protect a patient's medical and personal information will already be in place. Overall, reducing the risk of unauthorized access to patient information by profit-seeking hackers will result in a more trustworthy and accessible healthcare industry on the patient side, while also revamping the work environment for medical staff.

References

*4 current issues in health care and what administrators can do: Regis*. Regis College Online. (2022, October 23). Retrieved March 30, 2023, from https://online.regiscollege.edu/blog/4-challenges-facing-the-health-care-industry/

AHIMA Foundation. (2022, June 15). *Digital Health Literacy as a Social Determinant of Health*. AHIMA Foundation. https://ahimafoundation.org/understanding-the-issues/digital-health-literacy-as-a-social-determinant-of-health/

Camarines, T., & Camarines, J. (2021, July 16). *Discussing data security and telehealth during the COVID-19 pandemic*. National Library of Medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8344833/

CareersinCyber.com. (2020, December 17). *The importance of cyber security in healthcare*. ISACA. https://www.isaca.org/membership/membership-benefits/benefits-partner-content/career-guidance-articles/the-importance-of-cyber-security-in-healthcare

CBS Interactive Inc. (2019, February 14). *Hackers are stealing millions of medical records – and selling them on the dark web*. CBS News. https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/

Centers for Disease Control and Prevention. (2022, June 27). *Health Insurance Portability and accountability act of 1996 (HIPAA)*. Centers for Disease Control and Prevention. https://www.cdc.gov/phlp/publications/topic/hipaa.html

Hall, J., & McGraw, D. (2014). *For telehealth to succeed, privacy and security risks must be identified and addressed*. Health Affairs. https://journalofethics.ama-assn.org/article/privacy-and-security-concerns-telehealth/2014-12

*HIPAA Violations and Enforcement*. (n.d). American Medical Association. https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement

Ignatovski, M. (2022, October 1). *Healthcare breaches during COVID-19: The effect of the healthcare entity type on the number of impacted individuals*. Perspectives in health information management. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9635044/

Jalali, M. S., Landman, A., & Gordon, W. (2020). Telemedicine, privacy, and information security in the age of COVID-19. *Journal of the American Medical Informatics Association, 28*(3), 671-672. https://doi.org/10.1093/jamia/ocaa310

Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Risk management-based security evaluation model for telemedicine systems. *BMC medical informatics and decision making, 20*(1), 106. https://doi.org/10.1186/s12911-020-01145-7

Maximus Federal Services. (2012, December 13). *Non-HIPAA covered entities: Privacy and security policies and practices of PHR vendors and related entities report*. HealthIT.gov. https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf

NEJM Group. (2018, February 1). *What Is Telehealth?* NEJM Catalyst. https://catalyst.nejm.org/doi/full/10.1056/CAT.18.0268

*Obtaining informed consent*. (2021, April 21). Telehealth.HHS.gov. https://telehealth.hhs.gov/providers/preparing-patients-for-telehealth/obtaining-informed-consent/

(OCR), O. for C. R. (2021, June 28). *Notification of enforcement discretion for telehealth*. HHS.gov. Retrieved March 30, 2023, from https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

Parimbelli, E., Bottalico, B., Losiouk, E., Tomasi, M., Santosuosso, A., Lanzola, G., Quaglini, S., & Bellazzi, R. (2018). Trusting telemedicine: A discussion on risks, safety, legal implications and liability of involved stakeholders. *International Journal of Medical Informatics, 112*, 90–98. https://doi.org/10.1016/j.ijmedinf.2018.01.012

Riggi, J. (n.d.). *The importance of cybersecurity in protecting patient safety*. American Hospital Association. Retrieved 30 June, 2022 from, https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

Scott, J. (2022, March 4). *Tips for healthcare organizations to prevent and respond to data breaches*. HealthTech Magazine. https://healthtechmagazine.net/article/2022/03/tips-healthcare-organizations-prevent-and-respond-data-breaches

Seh, A., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare, 8*(2): 133. https://doi.org/10.3390/healthcare8020133

Stouffer, K., Zimmerman, T., Tang, C. Y., Lubell, J., Cichonski, J., & McCarthy, J. (2017, September). *Cybersecurity framework manufacturing profile*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

*Suspicious activity reports (SAR)*. OCC. (2019, March 4). Retrieved March 30, 2023, from https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html