International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Securing Telehealth Platforms: Best Practices for Securing Telemedicine Applications and Protecting Patient Data

Richard Aggrey[1], Bright Ansah Adjei[2], Karl Osei Afoduo[3], Nana Adwoa Konadu Dsane[4],

\

[1]Dep. Director, Head of IT, University of Ghana Medical Centre,
[2]Senior Health Research Officer, University of Ghana Medical Centre,
[3]Senior Health Research Officer, University of Ghana Medical Centre,
[4]Dep. Director of Research, University of Ghana Medical Centre,

Abstract

It is imperative to secure telehealth applications since they represent the next generation of healthcare delivery systems and offer remote clinical services and accessibility. Through telehealth, patients are able to see their doctors despite problems of time and distance, congestion, and infection. However, with the increase of telemedicine services, other vices such as ransomware, phishing and data leak are on the rise and are a threat to patients' lives.

The following recommended practices for telemedicine application security were covered in this paper; MFA, HIPAA, and safeguarding the patient information. Preventing cyber threats and gaining patient's trust then require the following measures: encryption of data, safe storage of data, conducting regular risk assessments and compliance with data privacy and protection laws. The following are the recommendations that may help in enhancing telehealth systems: – Telehealth systems should be developed by healthcare delivery organisations, telehealth technology vendors and policymakers.

However, research and improvement in security measures have to be done in order to address current and future risks that telemedicine is exposed to and to enhance the value of telemedicine in light of such advanced technologies such as Artificial Intelligence and integration of electronic healthcare.

1. Introduction to Telehealth Platforms

The usage of telehealth systems to deliver clinical services remotely is growing, by linking professionals and patients worldwide (WHO,2020). These services could potentially reach those who might not otherwise be able to obtain healthcare because of travel challenges or a lack of specialists in urban areas (Smith, et al., 2020). Apart from that, telehealth allows patients to schedule appointments at their convenience. For long-distance clinical health care, patient and professional health-related education, public health, and health administration, telehealth uses electronic information and telecommunication technology. Today, what is popularly known as telehealth is simply a shift from using technology in administering, delivering and receiving health care services (Haleem, A., et al., 2021).

Telemedicine encompasses all uses of information technology for diagnostics, treatments, communications, and health information research that support clinical assistants, patients, and educators

in areas of health management and inter-professional links. Telehealth, through the application of common telecommunications and network technology, could permit the provision of health care services for patients and a care provider that are at distances from each other. The demand for remote provision of a broad range of health services has grown in a surge that was precipitated in large part by the increasing age of the population, complexity of an aging society, workforce shortages, and inaccessibility of health care services. The rapid changes in the practice of medicine will have positive implications for care and distribution of needed health practitioners. The growth of telehealth will also have an impact on health resources, shift responsibility and management of care, health outcomes, cause changes in current practice, administration functions, advocacy, and billing (Kichloo, A., et al., 2020).

1.1. Definition and Importance of Telehealth

Telehealth is the delivery of healthcare services through telecommunication technologies (WHO, 2020). It is a type of telemedicine that expands beyond healthcare to include other services and products (HIMSS, 2021). However, telemedicine refers particularly to services related to clinical services, such as diagnosis and treatment (U.S. Department of Health and Human Services [HHS], 1996). Recent years have distinguished telehealth from telemedicine because the former includes patient education, disease surveillance, research, and administrative activities (Smith, et al., Brown, 2020).

Telehealth services are typically categorised into two main types based on communication methods: the dichotomy of communication strategies, namely synchronous and asynchronous communication (Norris et al., 2019). Synchronous communication is actual time communication where the messages are sent and received at the same time. Synchronous communication is characterised by timely exchange of information between and among patients and healthcare givers and it comprises video medical consultations, telephone consultations, and online chats. Such interactions are usually described as consultations or e- consultations.

Meanwhile the asynchronous communication does not necessarily involve immediate or real time dialogue. This means that messages can be sent and received at different time. For instance, a patient can use a smartphone or computer to scan and upload images, laboratory results, or even ask a health-related question which will be later responded to by a clinician. Such kind of communication is convenient as it is not constrained and can be used where the consultation is not very urgent.

Telehealth can be defined as a service that uses different technologies to communicate with patients and other healthcare providers. Telecommunication networks provide support to the data acquisition process and also support the live video interview link and all secure data transfer. Electronic Health Records (EHRs) are used in storing and accessing patient pertinent information such as patient histories records, laboratory results and images among others (Norris et al., 2019).

Moreover, mobile applications are critical to telehealth by providing technologies for distant patient monitoring, health, and patient involvement. Others are IVR systems that offer information or even connects the call to the right services and video conferencing for actual real-time consultancies.

A number of other technologies exist in parallel with conventional consultation and telemedicine to increase the adaptability, productivity, and effectiveness of the healthcare services delivered to patients. Though telehealth and telemedicine require the use of telecommunications in the improvement of healthcare delivery, their application is not the same thing. Telehealth involves multiple categories of programmes that are medical and nursing and other probable functions like patient instruction, disease tracking, research, and paperwork among others.

Unlike telehealth, which covers a broad range of healthcare technologies and services, telemedicine relates

solely to clinical services where purpose is to diagnose illnesses, treat patient, and perform medical consultation. Telemedicine is usually applied to such specializations as psychiatry, dermatology or other cases when the examination can be made without direct touch and conversation.

Telehealth and face-to-face clinical services extend each other as they present potentialities of health care provision. Telehealth has existed in parallel with the conventional health system for the last 70 years, expanding service delivery opportunities, minimizing transport-related nuisances, and optimizing work. Although telehealth is excellent for many healthcare issues, specific diseases and particular specialties continue to be most useful for in-person visits (Smith et al., 2020).

2. Challenges in Securing Telehealth Platforms

The telehealth industry has long struggled to counteract and safeguard against the numerous security risks that its systems face. This is further impacted by the sector's main offering, which often involves remote monitoring and clinical consultations. Common threats telehealth systems often face include data breaches, data losses or exposures, unauthorized internal or external access, and phishing attacks. Increased frequency of remote consultations presents patients and providers with a host of unique security risks. Significantly, it increases the points of external network connection, thereby creating new opportunities for unauthorized external access to the patient's data or the telemedicine application system. Patients could also potentially be placed in a position whereby any breach of a researcher's telehealth systems could be used to cross-match the patient's data with other repositories or leaked data, posing an unanticipated threat intelligence risk to the patient (AlOsail, D., et al., 2021).

Numerous malware programs, especially ransomware - a type of malware that encrypts the contents of the system and demands money for the files to be decrypted—result in inadvertent data leaving through malicious end systems and attempting to propagate. A range of ransomware attacks have made news headlines and have delved into the unprecedented realm of healthcare infrastructure over the years, including hospitals, city emergency services, and public bank systems. All of these could be translated into telemedicine platforms equally if the appropriate security measures are not put in place. As a result of such significant breaches, around 90% of healthcare organizations reported that they experienced a data breach at some point. It is important to note the potential obligations under the current frameworks for appropriate telehealth data breach management. Optimal cybersecurity measures protect patient privacy and data integrity and are indispensable for patient trust and future decision-making in accepting and negotiating security against risk (McIntosh, T., et al., 2024).

2.1. Understanding Cybersecurity Threats in Telemedicine

Healthcare's shift to digital platforms has enhanced patient-provider engagement and improved remote monitoring. However, the increasing cyberattacks during the global pandemic on numerous telemedicine platforms evidently made this connection feeble. These experiences occurred as a result of threats such as unauthorized access, denial of service, distributed denial of service that interrupted healthcare services and compromised the service and information. Therefore, telemedicine platforms must prioritize data security as it is a crucial component in safeguarding patient information as well as healthcare systems (Chigada, J., et al., 2021).

There are various vulnerabilities that a telemedicine platform can attract. If a patient's personal health record is stolen or misused, it can lead to negative healthcare expectations. In telemedicine, the required facilities are maintained in different locations, and users communicate over a network. This brings additional security and privacy issues into the scope of telemedicine. Cyber threats leading to the violation

of these security and privacy features will have huge implications. Though the general threats to information security are common to both healthcare and telemedicine, the remote nature of telemedicine, with a large number of stakeholders, intensifies these threats. Organisations should follow healthcare data safety regulations to ensure that sensitive patient data does not become accessible to any unauthorised user (Aslan, Ö., et al., 2023). The major privacy act that offers the right to security for an individual's medical records globally is HIPAA, which was enacted and signed into law in 1996 by the US Congress.

The following cyberattacks are highly probable on telemedicine systems. Phishing attacks are targeted towards new telemedicine users; hackers send URLs of lookalike web pages on the telemedicine platform. As new users usually don't have a clear picture of the original telemedicine service web pages, they are often victims of such attacks. In addition to lookalike webpages, other phishing methods include sending emails, calls, or messages asking for telemedicine website credentials or other confidential information. Ransomware also occurs when the telemedicine system lacks encryption for files or during transaction progress. The unavailability of patient data due to a ransomware attack can cause health or financial loss to certain patients. Another likely attack on telemedicine systems is denial of service or distributed denial of service attacks. Such attacks temporarily make the telemedicine platform unavailable, resulting in server crashes or system overload while handling high traffic. Spoofing attacks is also prominent as it a form of fraud orchestrated to misrepresent oneself as someone else. These activities are often noticed during video conferencing or diagnostic sessions. In this situation, the attacker may act as a patient or a doctor, misleading others in treatment discussions or compromising group therapies. Any information shared during this time can be misused in society or for personal gain (Alawida, M., et al., 2022).

3. Best Practices for Securing Telemedicine Applications

Strong patient authentication protocols are considered to be an effective way of preventing unauthorised parties from connecting to a telemedicine platform. Multi-factor authentication is considered an effective strong authentication method. A user account recovery process is needed in case the user is unable to use the multi-factor authentication. In addition, users must be provided training regarding how to use the telemedicine application securely. They should also know how to recognise different types of threats. User awareness, if not adequately developed, can hinder the full potential of the secure telemedicine application. All data transmitted by telemedicine systems should be protected by strong encryption. Sensitive data stored on intermediary systems should also be encrypted to protect against defamation. Access by insiders should also be controlled through different authentication protocols (Wenhua, Z., et al., 2024).

Regular updates of the telemedicine application are equally essential to reduce vulnerabilities due to software bugs or other problems. This applies to the various devices, software platforms, and network equipment used in the telemedicine system. One effective way of ensuring the ability of a healthcare organisation to reduce the risks that go with the widespread use of telemedicine applications is the construction of written security policies. This policy should reflect the unique design, infrastructure, workflow, personnel, and other related topics of the telemedicine initiative or programme. To get an accurate configuration of the telemedicine application's organization, a professional in information assets or cybersecurity should be involved in the development of the policies. Furthermore, getting expertise in evaluating system security performance is more important for an independent cybersecurity professional or a professional from one's own team (Ahmad, R. W., 2021).

3.1. Implementing Multi-factor Authentication

A 2-factor or multi-factor authentication (MFA) method normally includes at least one or more of the

following components for proving the user's identity: something the user knows, such as a password, PIN, or security question/answer; something the user has, such as a token, smart card, or code sent via text message; and something the user is, such as a biometric. The major advantage of MFA is that adding more than one proof of identity makes unauthorised access much less likely (Suleski, T., et al., 2023).

Adding one more layer of identity proof to authenticate a user significantly improves overall system security. For any organisation using or preparing to offer telehealth services, implementing MFA is a meaningful step to reduce the risks of unauthorised access to patient records and maintain compliance with privacy laws. MFA can be integrated with nearly any login setup, from simple username/password-based systems to more advanced solutions involving smart cards, thumbprint readers, facial recognition, and gait analysis. Text messages containing one-time codes are the most commonly used form of MFA because they give users flexibility through any cell phone with text capabilities. Other common methods include sending a phone call to the user with the one-time password or setting up an application on a smartphone for periodic code generation. Device tokens generating a time-limited passcode can also satisfy the 'something the user has' requirement. Another popular 'something you have' method is the push notification sent to a dedicated application on a user's smartphone. Push notifications enable biometric verification in the smartphone app to be completed without the need to leave the system access page because it is now a background process (Lawson, H., 2020).

4. Protecting Patient Data in Telehealth Platforms

Healthcare organisations making the move to remote care are making patient data protection a top priority in telemedicine applications. As healthcare organisations and providers have adopted the Health Insurance Portability and Accountability, they must establish safeguards to exclude the unauthorised use and disclosure of sensitive health information. HIPAA sets requirements to prevent breaches and to beef up consumer confidence in telehealth by establishing a floor of privacy and security measures (Hall, J. L., et al., 2014).

Beyond data breaches, patient data in telehealth platforms is also prone to loss, manipulation or exposure given improper controls. The need for secure data storage and transfer capabilities in healthcare organisations must exist, for example, to encrypt data stored in the cloud and to have strong security controls for accessing and transferring patient data (Bassan, S., 2020).

Healthcare organisations should be doing regular risk assessments, as required under HIPAA, to cover all the ways data can become compromised. The same goes for third-party providers — electronic health record vendors, telemedicine platforms, and billing and scheduling services — who are also required to conform to HIPAA and its components. Finally, no matter what regulations are put in place to secure patient data, the only way to create and sustain a space of trust among patients to use telehealth platforms for their care is to put the security and privacy of their data first (Yadav, V. 2024).

4.1. Compliance with HIPAA Regulations

HIPAA outlines the requirements and standards for keeping a patient's health information confidential. It includes several acts, all regulating a different aspect of patient data. Primarily, however, HIPAA contains the Privacy Rule and Security Rule. The Privacy Rule established policies for the protection of individuals' medical records and other personal health information. It also identified patient rights concerning their PHI, such as the right to examine their medical records. The Security Rule outlines the safeguards to protect Electronic Protected Health Information (ePHI). It is designed to handle the security of the health

information, which includes assessing the threats to the healthcare organisation's management, as well as physical and technical safeguards of information (Theodos, K., et al., 2020).

HIPAA-compliant entities can be divided into covered entities and business partners. HIPAA requires covered businesses to meet certain duties, while business associates ensure that they will be able to do so. Each covered entity and business associate may have different roles, but they share one goal: ensuring that all PHI remains secure and private. One fundamental concept that you will notice throughout the acts is that patients hold the rights to their health records and certain information on how they are used. It only makes sense, then, that a large part of the policies in these acts centre around informing patients of their rights. Another critical aspect of the acts is managing a security breach. If there is a chance that insecure health records are accessed, shared, or dealt with in a fashion that violates their confidentiality, then the HIPAA Breach Notification Rule mandates that individuals are informed. Furthermore, the Breach Notification Rule contains the instructions that surround the effective date for breached entities. Another integral requirement is the training of all staff with access to protected health information. Organisations are required to provide additional follow-up training for staff who have flouted the security policies and procedures (Oakley, A. (2023).

4.2. Strategies for Achieving and Maintaining HIPAA Compliance

In addition to having healthcare leadership prioritize compliance from the top down, organisations must also possess operational systems in place to ensure that they abide by data protection, privacy, and security laws. Organisations must develop a sanctions policy against workforce members who disclose data that privacy regulations protect. Organisations can also be audited. As a result, some organisations have developed multifaceted approaches to ensure compliance. One possible strategy is to incorporate penalties into the workforce member's agreement to access electronic health records without a legitimate purpose. Another possible approach is for organisations to educate their workforce members about the potential penalties they may encounter for accessing electronic health records without a legitimate purpose (Ameen, N., et al., 2021).

Regardless of whether or how these generally available compliance approaches are adopted, healthcare organisations require documented compliance programs that must be constructed on the basis of numerous factors, including but not limited to organisational structure and size. Organisations can achieve this by creating a list of compliance requirements from various sources of healthcare legal frameworks. Also, healthcare organisations should ensure that they do proper risk analysis from time to time to determine any possible threat that could be present in their privacy security and data protection frameworks. Such a risk analysis and assessment would aid in identifying the policies and procedures that agencies enforce through a variety of enforcement means, including reviews and audits (Malenfant, S., et al., 2022).

5. Conclusion and Future Trends

Patient data, verification, and consent are becoming vital issues in ensuring the security of telemedicine and telehealth. Due to telehealth's ability to offer care to patients at a lower cost and promptly, it is probable that additional healthcare and related organisations will aid in advancing it. During this transition time, it would be wise for telehealth systems to adopt existing best practices for data protection and practice areas in securing patient consent and ensuring that the person sending the data is the person they claim to be. We identified some of these best practices and those needs at the start. The healthcare industry is seeing the opportunity to provide effective remote care to patients using telehealth and telemedicine services.

New frameworks and public policies are now introduced and implemented to regulate and govern the use

and deployment of telemedicine platforms. However, despite its effectiveness and efficiency, its security is still a concern. In addition, the increasing reliance on emerging technologies, such as AI integration and the integration of electronic healthcare systems with telehealth services, has opened up new research prospects. Improving the security measures for these telehealth platforms could also be an enticing course for future work. Nevertheless, as cyber threats are advancing daily, researchers and stakeholders should continue exploring effective strategies to enhance telehealth platforms' overall resiliency and effectiveness.

References

1. Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. International journal of medical informatics, 148, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399
2. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences, 34(10), 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003
3. AlOsail, D., Amino, N., & Mohammad, N. (2021). Security issues and solutions in e-health and telemedicine. In Computer Networks, Big Data and IoT: Proceedings of ICCBI 2020 (pp. 305-318). Springer Singapore. https://doi.org/10.1007/9
4. Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114, 106531. https://doi.org/10.1016/j.chb.2020.106531
5. American Medical Association (AMA). (2019). Telehealth utilization during the pandemic.
6. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
7. Bassan, S. (2020). Data privacy considerations for telehealth consumers amid COVID-19. Journal of Law and the Biosciences, 7(1), lsaa075. doi:10.1093/jlb/lsaa075
8. Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23(1), 1-11. https://doi.org/10.4102/sajim.v23i1.1277
9. Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. Sensors international, 2, 100117. https://doi.org/10.1016/j.sintl.2021.100117
10. Hall, J. L., & McGraw, D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. Health Affairs, 33(2), 216-221. https://doi.org/10.1377/hlthaff.2013.0997
11. Health Insurance Portability and Accountability Act (HIPAA), 1996.
12. Healthcare Information and Management Systems Society (HIMSS). (2020). The future of telehealth security.
13. HIMSS. (2021). Telehealth Security Best Practices.
14. Kichloo, A., Albosta, M., Dettloff, K., Wani, F., El-Amir, Z., Singh, J., ... & Chugh, S. (2020). Telemedicine, the current COVID-19 pandemic and the future: a narrative review and perspectives moving forward in the USA. Family medicine and community health, 8(3). doi: 10.1136/fmch-2020-000530.

15. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248
16. Lawson, H. (2020). AI-Driven Multi-Factor Authentication: Enhancing IAM Security in Healthcare Systems. DOI: 10.13140/RG.2.2.10636.32645
17. Malenfant, S., Jaggi, P., Hayden, K. A., & Sinclair, S. (2022). Compassion in healthcare: an updated scoping review of the literature. BMC palliative care, 21(1), 80. https://doi.org/10.1186/s12904-022-00942-3
18. McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., ... & Halgamuge, M. (2024). Ransomware reloaded: Re-examining its trend, research and mitigation in the era of data exfiltration. ACM Computing Surveys, 57(1), 1-40. https://doi.org/10.1145/3691340
19. National Institute of Standards and Technology (NIST). (2018). Cybersecurity Framework.
20. Norris, T., Hart, G., & Larson, E. (2019). Telehealth and Rural Health Care Delivery. Rural Policy Research Institute.
21. Oakley, A. (2023). HIPAA, HIPPA, or HIPPO: What Really Is the Heath Insurance Portability and Accountability Act? Biotechnology Law Report, 42(6), 306-318. https://doi.org/10.1089/blr.2023.29329.aso
22. Smith, J., & Brown, R. (2020). Cybersecurity in Healthcare: Emerging Threats and Solutions.
23. Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Digital health, 9, 20552076231177144. https://doi.org/10.1177/20552076231177144
24. Theodos, K., & Sittig, S. (2020). Health information privacy laws in the digital age: HIPAA doesn't apply. Perspectives in health information management, 18(Winter), 1l. PMCID: PMC7883355 PMID: 33633522
25. U.S. Department of Health and Human Services (HHS). (1996). Health Insurance Portability and Accountability Act.
26. Wenhua, Z., Hasan, M. K., Jailani, N. B., Islam, S., Safie, N., Albarakati, H. M., ... & Khan, M. A. (2024). A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications. Computers in Human Behavior, 153, 108134. https://doi.org/10.1016/j.chb.2024.108134
27. World Health Organization (WHO). (2020). Telehealth: Opportunities and Challenges.
28. Yadav, V. (2024). Cybersecurity Protocols for Telehealth: Developing new cybersecurity protocols to protect patient data during telehealth sessions. North American Journal of Engineering Research, 5(2). http://najer.org/najer/article/view/51