DOI: 10.1145/3651223

BY SANCHARI DAS ET AL.

Improving Privacy and Security of Telehealth

Multidisciplinary experts' perspectives on how to strengthen protection of patients' health information in telehealth designs and workflows.

Telehealth is the practice of remotely providing healthcare using electronic communication and information technologies which can potentially increase access to care, especially in underserved or remote regions.[8] In contrast to traditional healthcare, telehealth relies significantly on digital communication technologies such as secure messaging platforms, video conferencing, and mobile applications to facilitate interactions between healthcare providers and patients. The implementation of telehealth enables the utilization of remote patient monitoring as well as virtual visits for regular patient interaction. This proved to be very helpful during the COVID-19 pandemic, when telehealth aided in the distribution and democratization of healthcare services. However, with telehealth use growing in the U.S. by 4% annually and reaching a record 64.3% in 2020, it has revealed significant security and privacy concerns.[a]

Telehealth is especially vulnerable compared to in-person healthcare given the increased complexity and consignment of control over the remote environment. Additionally, the security and privacy of the telehealth depend on several stakeholders such as developers producing secure medical technologies, providers following secure practices, and end users (patients) making secure choices, among others.[6] Moreover, the interacting parties (patients and healthcare providers) often have less control over the technological tools used in the process. However, in this viewpoint we discuss specifically how the obligation under the Health Insurance Portability and Accountability Act (HIPAA) to select and implement tools with appropriate privacy and security falls disproportionately on healthcare professionals and patients in telehealth.

In this aspect, in October 2022, we held a panel at the Human Factors and Ergonomics Society (HFES) annual meeting[b] with experts from academia, industry, and medicine.[c] In this Opinion column, we summarize discussions from this panel on issues surrounding telehealth security to expand the conversation and urge the community to develop secure, usable, and privacy-preserving tools for telehealth.

Practitioner Perspectives on Healthcare Security and Privacy

James T. McElligott, the Executive Medical Director for the Center for Tele health at the Medical University of South Carolina (MUSC), described how the South Carolina Telehealth

[a] See https://www.ahip.org/resources/telehealth-growth-during-covid-19

[b] See https://www.hfes.org/Events/International-Annual-Meeting

[c] Experts contributing to this Opinion column include Faiza Tazi (Ph.D. candidate), Dr. Kapil Madathil (Ph.D., associate professor), Josiah Dykstra (Ph.D., cybersecurity consultant), Prashanth Rajivan (Ph.D., assistant professor), James T. McElligott (M.D., executive medical director), Jiovanne Hughart (Au.D., audiologist), Daniel Votipka (Ph.D., assistant professor), and Sanchari Das (Ph.D., assistant professor).

Association (SCTA) is committed to supporting the development of telehealth and distance care programs in the state. Thanks to the SCTA, telehealth programs in the state registered more than 1.5 million interactions in 2021. These interactions were mainly synchronous video interactions at an average 800 video telehealth appointments per day for MUSC alone. These interactions also included asynchronous interactions and remote patient monitoring. McElligott perceives that when switching between in-person and telehealth appointments, providers need help with workflow adaptation, regulatory compliance, automated security and privacy-focused measurements, as well as educating patients on how to use telehealth platforms.

Jiovanne Hughart, a clinical audiologist, described how some, but not all, types of hearing healthcare services can be provided remotely given the need for direct physical contact in many cases. In practice, the level of privacy and information security in telehealth and in person at a clinic depend on the size and the personal knowledge of the practice owners and clinicians. Furthermore, the security and privacy used during telehealth appointments are often limited to HIPAA training and choosing a technology they can trust that will also enable them to care for patients.

Josiah Dykstra, a cybersecurity consultant for health professionals, described how healthcare providers feel that a lack of time, staff expertise, or funding is their most significant limitation to better cybersecurity.[3] In addition, a need for more adequate resources and targeted education contributes to this perceived inadequacy. Indeed, healthcare providers need a greater understanding of cybersecurity in the context of their work and the threat environment, which complicates their ability to address patient data security measures.

Prashanth Rajivan, who studies how human behavior affects security and privacy, described how a literature survey shows that most research is focused on technology, not human factors.[7] In preliminary research interviewing healthcare professionals, Ph.D. student Faizi Tazi, whose primary researchfocusisenhancingprivacyandsecurityprotocolsoftelehealthservicesforprivatepractices, found that Zoom has been a dominant telehealth platform, and participants perceive the need to internalize risk perception and awareness.

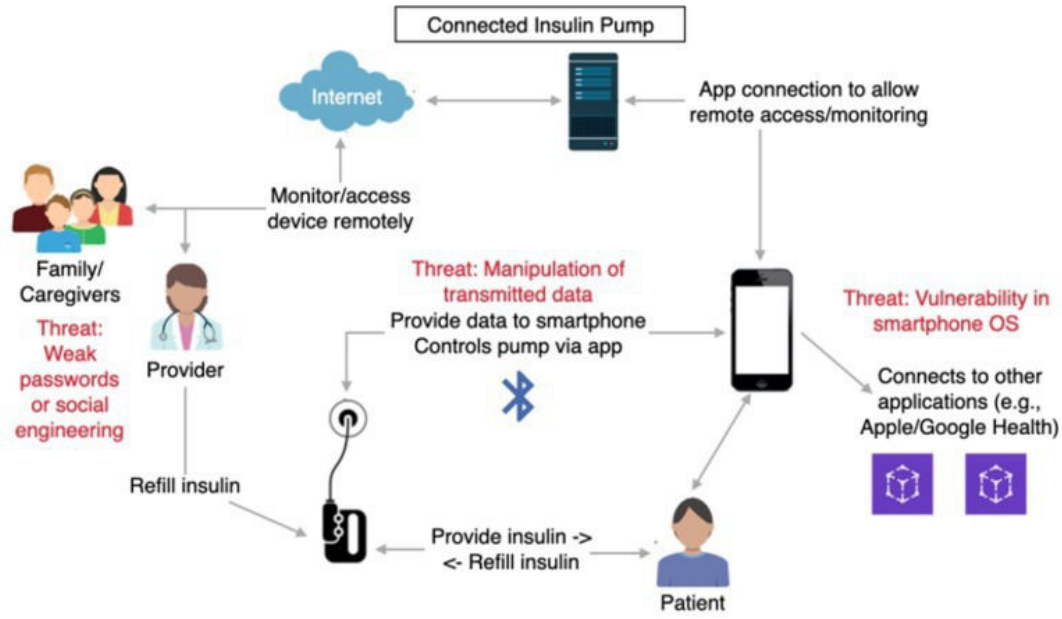
Threat Models and Medical System Security

Digital systems are essential to the efficient operation of any healthcare facility and the provision of quality care. However, these systems also store private health information (PHI); thus, ensuring that these systems are as secure as possible is crucial. Daniel Votipka, who has studied secure development and human-computer interaction, described how these systems must be prepared to face attacks from malicious actors, including internal and external threats. These attacks can range from identity attacks such as identity loss, sharing, theft, misuse, impersonation, or spoofing Electronic Health Records (EHR), to unauthorized access or disclosure, data and log file tampering, weak access control, elevation of privileges, and potential data repudiation.[5]

Threat models have been widespread and required in U.S. healthcare recently.[1] The accompanying figure represents a system model for a telehealth interaction: remote patient monitoring specifically for a connected insulin pump. The model depicts the various stakeholders when a patient interacts with medical Internet of Things (IoT) devices. The model also includes example annotated threats, such as threats to data integrity as it is transferred to and from the patient's smartphone, the threat of device manipulation if an attacker is able to compromise the patient's smartphone, and the threat of other actors' (care givers and providers) accounts being compromised due to insecure authentication (weak passwords or stolen credentials) or social engineering attacks. While threat modeling and the inclusion of security and privacy mitigations are required by law and regulations, there is not always a clear standard regarding how they should be applied in practice, or even how regulators should assess security. Currently, medical device developers rely on a range of best-effort practices and depend on a few skilled security practitioners with domain expertise. This approach does not scale well—especially problematic for small startups producing cutting-edge technology.

Prior research also found that the security and privacy of telehealth hinge on decisions often made by administrative personnel who rarely interact with the tools, creating a complex threat model.[8]

Figure. System model for an Internet-connected insulin pump with annotated threats.



Data Collection and Protection

The patient's medical history, diagnoses, medications, treatment plans, and other crucial healthcare and personal data are commonly contained in EHRs. By integrating EHR with telehealth, healthcare professionals can access patients' medical history, lab results, and treatment plans, enabling them to make informed clinical decisions and provide personalized care remotely. However, the integration of telehealth platforms with EHRs also brings significant risks to patient confidentiality. There are three main types of data workflows that occur at the intersection of telehealth platforms and EHR systems[9]: collection and transfer of vital sign data from medical devices for care management; collection and transfer of patient-reported outcomes (symptoms, functional status, and quality of life); and patients' general interactions with healthcare professionals during synchronous telehealth sessions. Security measures, such as encryption, authentication protocols, and secure data transmission channels, must be developed to mitigate threats introduced by the adoption of telehealth systems and to maintain the integrity of data workflows associated with telehealth practices. Such measures ought to place a strong emphasis on safeguarding the confidentiality of a patient's medical records which has been noted by the panel moderator Kapil Madathil, whose research focuses on the knowledge base of human factors engineering to the design and operation of sustainable human-computer systems.

HIPAA compliance requires these security measures to be implemented, for both providers and their business associates such as software developers related to the medical technology. Each panelist spoke about how crucial it is for covered entities to ensure EHR systems are HIPAA-compliant to safeguard patient information's security and privacy. HIPAA violations are punishable by fines and legal action. Patients rightfully expect that their private medical records will be kept secure and confidential, and HIPAA attempts to make sure this happens. However, it is crucial to understand that HIPAA compliance does not ensure EHR systems are completely secure.[4]

Therefore, healthcare providers must be vigilant but medical practitioners who are not technical experts are compelled to trust third-party software accounts about HIPAA compliance.

Risks from Third-Party Access to Data

A complex issue that raises significant privacy and security concerns is third-party access to healthcare data.[2] For legitimate reasons, including healthcare delivery, third-party technology providers routinely have access to protected health information. For example, a technology firm may be hired to support EHRs, or a research organization may be given access to de-identified data to study trends in disease prevalence. However, there is also a chance that unsavory parties will gain access to healthcare data for reasons like profit or to abuse PHI.

Healthcare organizations must also obtain patients' consent before sharing their data with third parties and be open about how they share patient data. For legitimate reasons (including research and to assist telehealth providers), third parties may occasionally be given access to telehealth data. For example, a technology company might be hired to support a telehealth platform, or a research organization might be given access to de-identified data to study telehealth usage trends.

Suggestions to Strengthen Telehealth Security and Privacy

Our panel surfaced several recommendations for enhancing telehealth privacy and security, which have been consolidated by the panel moderator, Sanchari Das, whose research focuses on enhancing the privacy and security of daily digital interactions of the understudied populations.

Continuous Training and Awareness for Providers. The HIPAA security rule requires implementing "a security awareness and training program for all members of its workforce," and the Privacy Rule states that training must be "as necessary and appropriate for the workforce members to carry out their functions." Our panelists shared that telehealth providers and staff require more continuous training on privacy and security best practices by experts to ensure that they are aware of their responsibilities and capable of protecting PHI.

Patient Informed Consent. Patients need help making security-informed choices. They need more insight today into the HIPAA compliance practices of their healthcare providers. They need more choices about telehealth platforms and guidance about how to use them safely. While they may be asked for consent before a telehealth appointment, they have few options or alternatives, even if they are concerned about security and privacy. Before using or disclosing PHI for treatment, payment, or healthcare operations, telehealth providers should obtain the patient's consent.

Implement Robust Security Measures. Telehealth providers should implement strong security measures to guard against data breaches and other online dangers. This may entail secure login protocols, data encryption, and ongoing security measure updates. One security measure that can be used to improve the security of telehealth records is the implementation of multifactor authentication (MFA), which was a recurring theme among the panel's security experts.

References

1. Bochniewicz, E. et al. Playbook for threat modeling medical devices. *MITRE and the Medical Device Innovation Consortium (MDIC) 1*, (2021); https://bit.ly/3zFfhRs.
2. Chen, D. and Zhao, H. Data security and privacy protection Issues in cloud computing.In *Proceedings of the 2012 Intern. Conf. on Computer Science and Electronics Engineering, 1*. IEEE Computer Society, 2012.
3. Dykstra, J., Mathur, R., and Spoor, A. Cybersecurity in medical private practice: Results of a survey in audiology. *Proceeding of the 2020 IEEE 6th Intern. Conf. on Collaboration and Internet Computing (CIC)*. IEEE Computer Society, 2020.
4. Koch, D.D. et al. Is the HIPAA security rule enough to protect electronic personal health information (PHI) in the cyber age? *J. Health Care Finance 43*, 3 (2016), 1–32.
5. Muthuppalaniappan, M. and Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *Intern. J. for Quality in Health Care 33*, 1 (2021).
6. Smith, A.C. et al. Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19). *J. Telemedicine and Telecare 26*, 5 (2020), 309–313.

7. Tazi, F. et al. SOK: Evaluating privacy and security vulnerabilities of patients' data in healthcare. In *Proceedings of the Intern. Workshop on Socio-Technical Aspects in Security*. Springer, Copenhagen, Denmark-Virtual, 2022.
8. Tazi, F. et al. Privacy, Security, and Usability Tradeoffs of Telehealth from Practitioners' Perspectives. In *Proceedings of Human Factors and Ergonomics Society HFES 67th Intern. Annual Meeting*. SAGE Publications, Washington D.C., 2023.
9. Zhang, X. et al. Impact of electronic health record interoperability on telehealth service outcomes. *JMIR Medical Informatics 10*, 1 (2022).

Faiza Tazi (faiza.tazi@du.edu) is a Ph.D. candidate at the University of Denver, Denver, CO, USA.

Josiah Dykstra (josiah@designersecurity.com) is a cybersecurity consultant Designer Security, LLC, USA.

Prashanth Rajivan (prajivan@uw.edu) is an assistant professor at the University of Washington, Seattle, WA, USA.

Kapil Chalil Madathil (kmadath@clemson.edu) is an associate professor at Clemson University, Clemson, SC, USA.

Jiovanne Hughart (abizwhiz@icloud.com) is an adjunct professor at Salas at Drexel University in Philadelphia, PA, USA.

James T. McElliot (mcellig@musc.edu) the executive medical director at the Medical University of South Carolina, in Charleston, SC, USA.

Daniel Votipka (dvotipka@cs.tufts.edu) is an assistant professor at Tufts University, Boston, MA, USA.

Sanchari Das (sanchari.das@du.edu) is an assistant professor in the Department of Computer Science in the Ritchie School of Engineering and Computer Science at the University of Denver, Denver, CO, USA.

A research award from Cisco partially supported this work. We also want to thank HFES for helping us organize the Privacy and Security of Telehealth Services panel. Any opinions, findings, conclusions, or recommendations are solely those of the authors.