Privacy and Security Risk Factors Related to Telehealth Services – A Systematic Review

By Shannon H. Houser, Ph.D., MPH, RHIA, FAHIMA; Cathy A. Flite, Ph.D., RHIA, FAHIMA; and Susan L. Foster, EdD, MBA, RHIA, CHPS, CHC, CHPC, CIPP/US, FAHIMA

Abstract

The objective of the study is to identify challenges and associated factors for privacy and security related to telehealth visits during the COVID-19 pandemic. The systematic search strategy used the databases of PubMed, ScienceDirect, ProQuest, Embase, CINAHL, and COCHRANE, with the search terms of telehealth/telemedicine, privacy, security, and confidentiality. Reviews included peer-reviewed empirical studies conducted from January 2020 to February 2022. Studies conducted outside of the US, non-empirical, and non-telehealth related were excluded. Eighteen studies were included in the final analysis. Three risk factors associated with privacy and security in telehealth practice included: environmental factors (lack of private space for vulnerable populations, difficulty sharing sensitive health information remotely), technology factors (data security issues, limited access to the internet, and technology), and operational factors (reimbursement, payer denials, technology accessibility, training, and education). Findings from this study can assist governments, policymakers, and healthcare organizations in developing best practices in telehealth privacy and security strategies.

Keywords: telehealth, telemedicine, privacy, security, confidentiality

1. Introduction

The extended lockdown as a result of the COVID-19 pandemic brought about increased demand for telehealth services.[1] Before COVID-19, telehealth services existed but were not widely used, mainly due to the lack of reimbursement. The use of telehealth services has been viewed as innovative and a solution for improving the delivery of healthcare as well as reducing costs and increasing access to care regardless of location.[2] Prior to the COVID-19 public health emergency (PHE), Mental and behavioral health providers utilized telehealth services most frequently. However, after March 2020, with the declaration of the PHE, the necessity for telehealth services sored in all disciplines, especially with primary care, mental and behavioral health and pediatrics.[1]

In a 2022 telehealth survey of physician participants conducted by the American Medical Association, 60 percent of respondents agreed or strongly agreed that telehealth enabled them to provide high-quality care. More than 80 percent of respondents indicated that with the use of telehealth, patients have better access to care.[3] However, putting telehealth services to use during the pandemic opened the door to multiple issues, including health care disparities.[4] With the increased use of telehealth and virtual care comes a plethora of new services, widening the gap of risks, which now include cyber and technology-related data security and privacy exposures.[7] Also, patients' lack of trust and expertise in using telehealth technology adds to their concerns for privacy and security.[5] The American Telemedicine Association, a leader in telehealth policy, advocates for telehealth and virtual care technology to be built on a foundation of protection of patient privacy, patient data, and the reduction of cybersecurity risks.[6] Despite telehealth being viewed as a valuable resource for providing quality healthcare services, data privacy and security

concerns continue to hinder the perception of benefits and influence the overall adoption and successful use of virtual care services.[2]

Healthcare professionals have become acutely aware of the obstacles to using telehealth technology, such as the performance of physical examinations as well as the lack of reimbursement parity and differences in state licensure and regulations.[8] Vulnerable populations struggle more than others with the use of healthcare technology, which raises privacy and security concerns.[9] Although there have been significant temporary changes in telehealth policies at both the federal and state levels, permanent changes to support telehealth services have been slower to manifest despite the continued demand.[10] To gain a better understanding of the challenges and barriers to the adoption and use of telehealth technology, the authors undertook this study to gather information that can be used to develop best practices and guidelines for telehealth privacy and security strategies.

Study Objectives:

1. Identify challenges and associated factors for privacy and security related to telehealth visits during the COVID-19 pandemic.
2. Categorize challenges into key factors in order to develop best practices and guidelines for telehealth privacy and security strategy.

2. Methods

2.1. Search Strategy

This systematic review was undertaken using a comprehensive literature search to find all published work identifying privacy and security challenges in telehealth. The search strategy was developed with the assistance of a college librarian. The search terms included a combination of Medical Subject Heading (MeSH) and advanced terms such as privacy, security, and telehealth. The six databases of PubMed, Science Direct, ProQuest, Embase, CINAHL, and the Cochrane Library were selected for the search using database-controlled vocabulary terms for telehealth, privacy, and security.

A protocol was established before the search, data gathering, and analysis using the Population, Interventions, Comparison, and Outcomes (PICO) Framework. This protocol outlined the search strategy, selection process, and data collection. This approach allowed the reviewers to frame this research based on the PICO methodology, which include the following:
- Population: Includes all providers using telemedicine; all consumers of healthcare using telehealth, excluding insurance companies
- Interventions: Includes all types of telehealth services such as live video, store-and-forward, remote monitoring, and mobile health; excludes face-to-face encounters
- Comparison: Privacy and security challenges 2020-2022 with challenges prior to 2020
- Outcomes: Best practices for privacy and security

2.2. Inclusion and Exclusion Criteria

Inclusion Criteria
- English-language only
- Peer-reviewed empirical studies
- January 2020 to February 2022
- Search terms: telehealth, telemedicine, privacy, security, confidentiality

Exclusion Criteria
- Studies conducted outside of US
- Study design issues: non-empirical studies (systematic review, literature review, commentary)
- Non-telehealth related studies (mobile health, eHealth)

2.3. Review Process

The selection strategy of abstracts for full review was divided among three reviewers. First, each reviewer independently reviewed abstracts for inclusion. Then, each reviewer presented their findings to the full group, and all discrepancies were reconciled.

A total of 1,224 study abstracts were identified through online databases. Upon review, 47 studies were duplicates; the reviewers eliminated 750 studies based on inclusion criteria dates; and 122 were eliminated due to wrong study design. A full-text review was selected for 305 articles. Upon examination, 77 studies were excluded due to wrong study design, 29 were mobile health, 10 did not include privacy and security, 31 were foreign studies, and 140 studies were wrong publication type. Eighteen studies were found acceptable for analysis, as decided by the three reviewers. A summary of the selection process is shown in **Figure 1**.

3. Results

3.1. Study Design and Data Collection Methods

Eighteen studies were identified and included in this study. Quantitative studies were the most cited study design (n=8), followed by qualitative study (n=5), four mix-methods (n=4), and one pre-post design (n=1). The collection methods included a host of approaches from interviews (both semi-structured and focus group) to surveys eliciting both qualitative and quantitative measures. **Table 1** contains the study design and data collection methods in the review.

3.2. Participant Types and Characteristics

The characteristics of the 18 studies, including the participant level, participant types, and a sample description, are summarized in **Table 2**.

Ten studies (56 percent)[9,11-17,25,26] included patients, parents, or consumers, with the most common participant type being patients or parents utilizing telehealth services in an outpatient setting[9,12,13,15,16,26] such as ambulatory surgery, clinics, or physician practices. Two studies[11,17] included participants from the community while one study[16] examined remote monitoring.

Overall, a total of 3,324 patients, parents, or consumers of telehealth were included in the 10 studies.

Six studies (33 percent)[18,19,21,22-24] included a range of provider types from athletic training, emergency room providers, pediatricians, and mental health. A total of 626 participants were providers of telehealth services.

Two studies (11 percent)[4,25] included both provider (clinical personnel, physicians, and nurses) and parent types as participants. A total of 24 providers or parents were participants.

3.3. Privacy and Security Challenges and Risk Factors

Table 3 summarizes all papers analyzed for telehealth's privacy and security challenges and risk factors. Three risk factors associated with privacy and security in telehealth practice include: environmental factors (lack of private space for vulnerable populations, difficulty sharing sensitive health information remotely), technology factors (data security issues, limited access to internet and technology), and operational factors (reimbursement, payer denials, technology accessibility, training, and education).

Unsurprisingly, most cited challenges included privacy and security. Twelve studies[4,9,11-17,20,25,26] cited patient privacy and confidentiality challenges, seven studies[18-21,22-24] cited provider privacy and confidentiality challenges, and age-related patient challenges were mentioned in four studies. The presence of parents during a pediatric/adolescent telehealth visit was an example of an age-related privacy concern. Additionally, the elderly population sometimes presented with limited digital literacy. However, age-related challenges were not noted for providers.

Seven studies identified the use of technology as a risk to telehealth.[9,11,13-15,20,25] The technology risk includes health/digital literacy (language, medical terminology), patient awareness and communication, patients experiencing technical errors, perceived information incompleteness, lack of interest and comfort in using internet-capable devices, and the need for patient assistance with technology. Five studies[19-21,23,24] included technology issues for providers, such as limited access to the internet and telehealth-specific technology, financial cost of technology, implementation of technology, staffing, information technology personnel to implement and support technology, reliability of internet connections to support telemedicine, access to video services, lack of digital devices, cellular data, or Wi-Fi.

The patient's environment as a privacy risk was identified in five studies[4,9,12,15,20]. For example, being overheard in the patient's or provider's home, navigating disruptions in their living space, lack of proper equipment such as headphones, unwarranted visualization of patient's living conditions, large households not having adequate space for confidential conversations, and lack of a private room for the vulnerable population such as the homeless. In two studies,[20,22] providers cited the lack of private workspace for personnel and difficulty in maintaining awareness of the surroundings to protect patient privacy as challenges.

Three studies identified patient's trust as a challenge to the use of telehealth.[11,13,14] Participants noted that to be successful, providers or other trusted individuals should describe and show

patients how to use the technology; identifying a suitable space may be another reflection of trust, acceptance of remote video consultation to improve measures and gain trust, and perceived trust in the competency of telehealth platforms. Three studies identified professional development and training for telehealth as a challenge.[19,20,22] However, providers' studies did not list trust as a challenge or risk.

Three studies identified limitations of quality assessment and diagnosis as a provider challenge and a risk only.[4,18,23] Individuals with HIV, pregnancy, or mental health diagnoses have special privacy concerns and two studies[15,17] identifying special privacy issues for these patients. Liability, legal, and regulatory challenges were found in two studies,[21,23] and reimbursement challenges[19] and burnout from telehealth use[21] were noted in one study for the providers only, respectively.

Discussion

Key Findings and Best Practices

This study identified the challenges and three key factors associated with telehealth privacy and security: environmental, technology, and operational factors. The authors developed and categorized these factors based on the identified issues and risks, and **Table 4** illustrates the summary of each three factors and examples. To address these risk factors, best practices and recommendations are discussed below.

Environmental Factor Implications

Environmental conditions play an essential role in telehealth privacy and security, which refer to an individual's surroundings, living conditions, and social connections that directly or indirectly impact privacy and security protections. Vulnerable populations such as the homeless, elderly, adolescents, and those who struggle with mental health are often concerned about the lack of private space for telehealth visits. Telehealth patient visits also create difficulty sharing sensitive health information remotely for people with certain conditions or diseases, such as HIV/AIDS, behavior health, and contraception requirements. The space, location, and accessibility to the use of telehealth are also a concern for healthcare providers.

For best practice, providing a safe, accessible environment should be a major concern when performing telehealth practice. Providers should check the availability and suitability of the patient location before and during the telehealth services. Provide guidance and resources to patients for finding a private place for the appointment when necessary. Use email, chat, or messages through the patient portal if a private location is unavailable or reschedule and suggest a better place for the telehealth visit. Explain to a minor patient whether parents or guardians should or should not be present at the appointment. Obtain informed consent or fill out a release of information before the visit begins.

Technological Factor Implications

Technology and digital literacies are other factors in telehealth privacy and security concerns. Technology factors include data security issues such as hacking of video visits, limited access to the internet and technology, lack of digital devices, cellular data use, or Wi-Fi, digital literacy such as limited knowledge and understanding of the technology use, and poor quality of audio or video output. Knowledge of technology use and digital literacy limiting the quality of assessments and diagnosis is another issue in telehealth use.

For best practice, when sharing information online, identify steps to protect patient information, and only enter personal information on secure websites with a lock icon in the URL bar. Require passwords for all online meetings and verify information while the patient remains in the "waiting room." For patients with telehealth visits, do not set up a telehealth appointment or share personal information with an unknown provider; use the provider's main phone number to confirm their identity. Keep devices protected with updated antivirus software. Avoid using public Wi-Fi to access telehealth services, and avoid accessing telehealth on devices shared with people outside of the home or family. Improve the quality of audio and videos by working with IT staff to ensure adequate bandwidth. Utilize the network, quality of service, and other measures to enhance the speed of the internet. Provide resources and training to patients with low health digital literacy. Consider the needs of vulnerable populations, such as English as a second language, disabilities, minors, and the elderly population.

Operational Factor Implications

The operational factor is also important in telehealth privacy and security practice. Reimbursement, payer denials for telehealth services, technology accessibility for all patients, training, and education for both staff and providers, maintenance and updating of devices and software are all related to the operational factors.

For best practice, the healthcare provider should incorporate telehealth services into privacy and security policies, procedures, and workflows, as well as integrate telemedicine into the Notice of Privacy Practices. Conduct thorough training modules with multiple sessions, manually rehearse steps, and ensure workflow integration is in place prior to beginning sessions. Ensure all staff and providers have received telehealth-specific privacy and security training. Include telehealth equipment, software, and devices in the organization's security management plan and annual security risk assessment. Determine the need for business associate agreements.

Healthcare professionals should review insurers' coverage determinations for telehealth services. Perform coding updates in the chargemaster to ensure billing codes meet payer requirements. Provide coding education for providers and office coding and billing staff. Ensure documentation for telehealth services is standardized and meets billing requirements. Use documentation templates or checklists for payer-specific requirements and use automatic time tracking within the organization's electronic health record for CPT code selection if available. Smart and dot phrases with predefined, modifiable snippets, which allow for standardization and timesaving documentation. Be aware of potential fraud or identity theft. At the start of each visit, verify a patient's identity using a government-issued ID and confirm their name, address, and device location.

Limitations and Future Studies

There are several limitations to this study. First, the search and review only included English-speaking languages, and studies conducted inside of the US; this limited comparison of any studies published in non-English and conducted in other countries. Second, the search only included peer-reviewed empirical studies; therefore, those non-peer-reviewed non-empirical studies, such as reports, case studies, and commentary published non-peer-reviewed, may be missed. Third, this review study included only publications from January 2020 to February 2022 intended to capture information beginning and during the COVID-19 pandemic. Therefore, the studies published before and after this period are excluded.

There are several opportunities for further research and investigation. First, although there have been significant temporary changes in telehealth policies at both the federal and state levels, permanent changes to support telehealth services have been slower to manifest despite the continued demand. Further research in developing and strengthening telehealth policies and regulations to better guide practice. There is also a lack of in-depth studies that address privacy and security concerns with the use of telehealth services and shows a need for continued research. In addition, the growth of telehealth and the use of technology has exposed digital health inequity and identified the need for digital health literacy education to the vulnerable populations. Finally, challenges such as provider telehealth burnout opens an avenue for further investigation.

Conclusion

The growth of telehealth use has inadvertently created challenges and issues for privacy and security. A multidimensional approach is needed when developing the best practices to incorporate and resolve the issues and tailor the needs of patients, providers, and operational managers. Building best practice guidelines and policies to address technology, digital literacy, accessibility and minimize privacy and security risks are necessary.

Author Biographies

Shannon H. Houser (shouser@uab.edu) is a professor in the Department of Health Services Administration at the University of Alabama at Birmingham in Birmingham, Alabama.

Cathy A. Flite (cflite@temple.edu) is an associate professor in the Department of Health Services Administration & Policy at Temple University in Philadelphia, Pennsylvania.

Susan L. Foster (fsusan@wustl.edu) is privacy compliance educator in the HIPAA Privacy Office at the Washington University School of Medicine in St. Louis, Missouri.

Notes

1. Houser, S.H., Flite, C.A., Foster, S.L., et. al. "Patient clinical documentation in telehealth environment: Are we collecting appropriate and sufficient information for best practice?"

mHealth (2022);8:6.

2. Pool, J., Akhlaghpour, S., Fatehi, F., and Gray, L. C. "Data privacy concerns and use of telehealth in the aged care context: An integrative review and research agenda." *International Journal of Medical Informatics* (2022): 104707. doi.org/10.1016/j.ijmedinf.2022.104707.

3. American Medical Association. "2021 telehealth survey report." (2022). https://www.ama-assn.org/system/files/telehealth-survey-report.pdf.

4. Wood, S. M., White, K., Peebles, R., Pickel, J., Alausa, M., Mehringer, J., and Dowshen, N. "Outcomes of a Rapid Adolescent Telehealth Scale-Up During the COVID-19 Pandemic." *Journal of Adolescent Health* 67, no 2 (2020): 172-78.

5. Britton, K. E. and Britton-Colonnese, J. D. "Privacy and security issues surrounding the protection of data generated by continuous glucose monitors." *Journal of Diabetes Science and Technology* 2, (2017): 216-19. doi.org/10.1177/1932296826681585.

6. American Telemedicine Association. "ATA Policy Principles." (July 22, 2020). Retrieved from https://www.americantelemed.org/policies/ata-policy-principles/

7. Schoenthal, J. and Pouncey, D. "Telehealth: a growing field and an evolving risk landscape." *Beazley Blog,* (2022). https://www.beazley.com/

8. Gajarawala, S. N. and Pelkowski, J. N. "Telehealth benefits and barriers." *The Journal for Nurse Practitioners* 17 (2021) 218-221. doi.org/10.1016/j.nurpra.2020.09.013.

9. Puzzitiello, R. N., Moverman, M. A., Pagani, N. R., Ryan, S. P., Salzler, M. J., Jawa, A., and Menendez, M. E. "Public perceptions and disparities in access to telehealth orthopaedic services in the COVID-19 era." *Journal of the National Medical Association* 113, no. 4 (2021): 405-13.

10. Center for Connected Health Policy/Public Health Institute. "A decade of telehealth policy." (2022). https://www.cchpca.org/2022/08/10YearReportfinal.pdf

11. Alexander, D. S., Kiser, S., North, S., Roberts, C. A., and Carpenter, D. M. "Exploring community members' perceptions to adopt a Tele-COPD program in rural counties." *Exploratory Research in Clinical and Social Pharmacy* 2, no. 1 (2021): 100023. doi.org/10.1016/j.rcsop.2021.100023.

12. Allison, B. A., Rea, S., Mikesell, L., and Perry, M. F. "Adolescent and Parent Perceptions of Telehealth Visits: A Mixed-Methods Study." *Journal of Adolescent Health* 70, no. 3 (2022): 403-13.

13. Dekker, A. B., Bandell, D. L. J. I., Kortlever, J. T. P., Schipper, I. B., and Ring, D. "Factors associated with patient willingness to conduct a remote video musculoskeletal consultation." *Archives of Bone and Joint Surgery* 8, no. 6 (2020): 656-60.

14. Esmaeilzadeh, P., and Mirzaei, T. "Do Hospitals Need to Extend Telehealth Services? An Experimental Study of Different Telehealth Modalities during the COVID-19 Pandemic." *Methods of information in medicine* 60, no. 3 (2021): 71-83.

15. Harsono, D., Deng, Y., Chung, S., Barakat, L. A., Friedl, G., Meyer, J. P., Porter, E., Villanueva, M., Wolf, M. S., Yager, J. E., and Edelman, E. J. "Experiences with Telemedicine for HIV Care During the COVID-19 Pandemic: A Mixed-Methods Study." *AIDS and Behavior* (2022): 1-13.

16. Majmundar, N., Ducruet, A. F., Wilkinson, D. A., Catapano, J. S., Patel, J., Baranoski, J. F., Cole, T. S., and Albuquerque, F. C. "Telemedicine for Endovascular Neurosurgery Consultation During the COVID-19 Era: Patient Satisfaction Survey." *World Neurosurgery* 158, no.1 (2022): e577-e582.

17. Manze, M., Romero, D., Johnson, G., and Pickering, S. "Factors related to delays in obtaining contraception among pregnancy-capable adults in New York state during the COVID-19 pandemic: The CAP study." *Sexual & Reproductive Healthcare* 31, no. 1 (2022): 100697.

18. Monk, A. D., Knight, M. M., Games, K. E., and Winkelmann, Z. K. "Athletic Trainers' Experiences and Perceptions Regarding Telemedicine." *Athletic Training & Sports Health Care: The Journal for the Practicing Clinician* 13, no. 4 (2021): e184-e92.

19. Palinkas, L. A., De Leon, J., Salinas, E., Chu, S., Hunter, K., Marshall, T. M., Tadehara, E., Strnad, C. M., Purtle, J., Horwitz, S. M., et al. "Impact of the COVID-19 pandemic on child and adolescent mental health policy and practice implementation." *International Journal of Environmental Research and Public Health* 18, no. 18 (2021): 9622. doi: 10.3390/ijerph18189622.

20. Payán, D. D., Frehn, J. L., Garcia, L., Tierney, A. A., and Rodriguez, H. P. "Telemedicine implementation and use in community health centers during COVID-19: Clinic personnel and patient perspectives." *SSM Qualitative Research in Health* – (2022): 100054. doi: 10.1016/j.ssmqr.2022.100054.

21. Pooni, R., Ronis, T., Lee, T., and CARRA Investigators. "Telemedicine use by pediatric rheumatologists during the COVID-19 pandemic." *Pediatric Rheumatology* 19, no. 1 (2021): 1-7. doi: 10.1186/s12969-021-00565-7.

22. Rogers, H., Madathil, K. C., Joseph, A., Holmstedt, C., Qanungo, S., McNeese, N., Morris, T., Holden, R. J., and McElligott, J. T. "An exploratory study investigating the barriers, facilitators, and demands affecting caregivers in a telemedicine integrated ambulance-based setting for stroke care." *Applied Ergonomics* 97, no 1. (2021): 103537.

23. Schinasi, D. A., Foster, C. C., Bohling, M. K., Barrera, L., and Macy, M. L. "Attitudes and Perceptions of Telemedicine in Response to the COVID-19 Pandemic: A Survey of Naïve Healthcare Providers." *Frontiers in Pediatrics* no. 9 (2021): 647937.

24. Schoebel, V., Wayment, C., Gaiser, M., Page, C., Buche, J., and Beck, A. J. "Telebehavioral Health During the COVID-19 Pandemic: A Qualitative Analysis of Provider Experiences and Perspectives." *Telemedicine Journal and e-Health* 27, no. 8 (2021): 947-54.

25. Thomas, N. A., Drewry, A., Racine Passmore, S., Assad, N., and Hoppe, K. K. "Patient perceptions, opinions and satisfaction of telehealth with remote blood pressure monitoring postpartum." *BMC Pregnancy and Childbirth* 21, no. 1 (2021): 153.

26. Zayde, A., Kilbride, A., Kucer, A., Willis, H. A., Nikitiades, A., Alpert, J., and Gabbay, V. "Connection During COVID-19: Pilot Study of a Telehealth Group Parenting Intervention." *American Journal of Psychotherapy* (2021). doi: 10.1176/appi.psychotherapy.20210005.