Journal of the American Medical Informatics Association, 28(3), 2021, 671–672
doi: 10.1093/jamia/ocaa310
Advance Access Publication Date: 16 December 2020
Correspondence

Correspondence

Telemedicine, privacy, and information security in the age of COVID-19

Mohammad S. Jalali [1,2,3] Adam Landman,[1,4,5] and William J. Gordon[1,4,6]

[1]Harvard Medical School, Boston, Massachusetts, USA, [2]Institute for Technology Assessment, Massachusetts General Hospital, Boston, Massachusetts, USA, [3]MIT Sloan School of Management, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA, [4]Mass General Brigham, Somerville, Massachusetts, USA[5]Department of Emergency Medicine, Brigham and Women's Hospital, Boston, Massachusetts, USA, and [6]Division of General Internal Medicine and Primary Care, Brigham and Women's Hospital, Boston, Massachusetts, USA

Corresponding Author: William J. Gordon, MD, MBI, BWH Hospitalist Service, PBB-B4-428, 75 Francis Street, Boston, MA 02115, USA (wjgordon@partners.org)

Received 18 November 2020; Editorial Decision 20 November 2020; Accepted 30 November 2020

The spread of COVID-19 has resulted in unprecedented circumstances that have necessitated a shift toward adopting infrastructure for telemedicine, due in large part to the inaccessibility of traditional care services and high exposure risks of in-person healthcare visits. With the increased strain and demand on traditional medical resources, telemedicine has emerged as an essential component of clinical care delivery and many healthcare organizations are reporting substantial increases in telemedicine use. For example, 1 medical center in New York City saw an increase in urgent care virtual visits from a pre-COVID-19 average of 102 daily to 802 post-COVID-19 expansion (March 2, 2020–April 14, 2020).[1]

Despite the numerous barriers to telemedicine, such as educating staff, cost, reimbursement, access to broadband, and patient digital literacy, telemedicine has flourished during the pandemic, forcing implementations that may have taken years without such a catalyst. As we continue this shift to telemedicine, new issues and risks unravel that need to be addressed, particularly in regard to information security and privacy, and ongoing work is needed to ensure that our technology infrastructure provides an environment for safe and effective care delivery.

In the US, the Department of Health and Human Services recently lifted several restrictions on communication apps, (eg, allowing the use of popular video conferencing applications, like Apple FaceTime, Facebook Messenger video chat, Google Hangouts, Zoom, and Skype) and increasing the range of services that are billable using telehealth.[2] These actions reduced barriers that previously prevented the use of telemedicine services for individuals. Despite these advancements, the substantial information security and privacy concerns surrounding telemedicine cannot be overlooked. For example, Zoom, currently 1 of the most popular video conferencing platforms, has had a 10-fold increase in usage over just a few months including increased use in healthcare, leading to several important privacy considerations, such as intruders joining video conferences or inadequate encryption of communications, leading to the possibility of eavesdropping.

Additionally, governmental agencies have warned of increased risk of cyberattacks towards the healthcare sector and organizations doing research on COVID-19.[3] Ransomware attacks—a type of cybersecurity threat that involves encrypting data and demanding payment in return for unencryption—have continued unabated during the pandemic, with many targeting hospitals.[4] A recent ransomware attack in Germany led to a patient's death, perhaps the first death in healthcare directly attributable to a cyberattack. Other recent ransomware attacks have included the Illinois Public Health website and a medical testing facility in the UK.[3] Successful cyberattacks negatively impact hospital operations, delay access to clinical services, and lead to significant economic loss, all of which would be devastating to organizations already under extraordinary economic and clinical strain.

Protection against these threats to secure telemedicine platforms is complex, and requires a multi-disciplinary, multi-stakeholder approach. Awareness is an important first step, and can take the form of education, employee training, and simulated cyberattacks (eg, sending fake phishing emails and providing training for those who click) toward establishing a culture of security. Recent research in hospitals shows that among several personal characteristics and or-

ganizational conditions, employees' workload had the strongest impact on the rate of clicking on phishing links.[5] While extensive emailing of announcements may be needed to keep employees up to date during the pandemic, it could unnecessarily add to workload, putting them at higher risk of clicking on phishing emails. Moreover, best-practice security behaviors must be followed—encrypting data, keeping software updated, running antivirus software, using 2-factor authentication, and following local cybersecurity regulations or recommendations.

While healthcare organizations and ambulatory practices may initially need to use consumer video conferencing tools, they should transition to an enterprise (healthcare specific) video conferencing product. Enterprise grade software versions may include key security features such as encryption and may offer additional configuration settings that can be standardized for the entire organization, such as requiring a waiting room with every teleconference.

Overall, healthcare organizations need to enhance (if not revolutionize) their cybersecurity infrastructure by developing stronger prevention and detection protocols, both administrative and technological. Executives need to be willing to invest fully in cybersecurity throughout the organization. Emerging fields, such as artificial intelligence, the internet of things, and blockchain can also be employed as prevention and detection tools to combat cyber threats more effectively. To leverage these technologies, healthcare organizations need to partner with telemedicine and cybersecurity vendors to understand how to best implement and use their infrastructure and products.

While prevention and detection capabilities are essential, healthcare organizations should be prepared with well-defined response plans. Unfortunately, response plans are often ignored or they are not considered as prevention and detection strategies. Response plans that are tested and practiced are required to minimize the negative consequences of an incident and ensure the provision of safe, secure, and reliable health care operations.

Ultimately, while healthcare systems should allocate significant resources towards improving telemedicine capabilities, it is up to healthcare delivery organizations to ensure that these new capabilities are safe, secure, and protect patient privacy. Balancing the significant privacy and information security concerns with the enormous potential benefits of virtual care during this pandemic will remain a vital component to our continuously evolving response to COVID-19.

FUNDING

None.

REFERENCES

1. Mann DM, Chen J, Chunara R, *et al.* COVID-19 transforms health care through telemedicine: evidence from the field. *J Am Med Inform Assoc* 2020; 27 (7): 1132–5.
2. The US Department of Health and Human Services. *Notification of enforcement discretion for telehealth remote communications during the COVID-19 nationwide public health emergency.* 2020. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html Accessed March, 2020.
3. NJCCIC Advisory. Cyber Threats & Cybersecurity for Healthcare during COVID-19. 2020; Ewing Township, NJ. https://www.cyber.nj.gov/alerts-advisories/cyber-threats-cybersecurity-for-healthcare-during-covid-19 Accessed October 1, 2020.
4. Eddy M, Perlroth N. Cyber Attack Suspected in German Woman's Death. The New York Times 2020. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html Accessed October 1, 2020.
5. Jalali MS, Bruckes M, Westmattelmann D, *et al.* Why employees (still) click on phishing links: investigation in hospitals. *J Med Internet Res* 2020; 22 (1): e16775.