



HIPAA and Telehealth

Protecting Health Information in a Digital World

Author _ **Melissa Kovac** (melissa.kovac@terumobct.com), **Terumo Blood and Cell Technologies**

In 1996, the Healthcare Information Portability and Accountability Act (HIPAA) was enacted to protect the privacy and security of patients' protected health information. Since then, technology has taken health information far beyond paper medical records and grainy faxes. As telehealth, in the forms of electronic health records, virtual visits, apps, and wearable devices, has increased in popularity, HIPAA clearly is no longer sufficient to guarantee the privacy of the health information it was enacted to protect. Updates to HIPAA are necessary, and those updates should be made with future technological advancements in mind.

Telehealth, broadly defined as healthcare provided via telecommunication and digital technologies, has in recent years been promoted as a way to increase access to healthcare services for rural, under-resourced, and underserved populations (Enlund 2020, 1–2). Telehealth services range from simple administrative patient portals and convenient apps to telephone and video visits with otherwise inaccessible specialists (US Department of Health and Human Services [HHS], n.d.). When available, it offers patients greater control and can be a convenient, time-saving, and cost-effective way to obtain medical care. Unfortunately, it also puts protected health information (PHI) at risk and is vulnerable to privacy and security breaches (Gajarawala 2021, 218–19).

In the United States, the vanguard of electronic healthcare information privacy regulation is the Healthcare Information Portability and Accountability Act of 1996 (HIPAA). HIPAA guarantees that individuals' PHI is kept private and secure as it travels to and from patients, healthcare providers, insurance companies, and approved business associates (HHS 2013). Patients have a right to access

their PHI, and it may not be shared with others without the patient's explicit permission, with few exceptions. Protected health information includes medical records, reports of conversations about patient care, and insurance and billing information (HHS 2020a).

There have, not surprisingly, been violations of the patient confidentiality and information security



guaranteed by HIPAA—messages left with the wrong person, PHI shared by healthcare providers outside of work, lax risk analysis and management, outright theft—and penalties have included job loss, fines, and criminal prosecution (Tariq 2020). A 2019 review of breaches affecting more than five hundred patients in the United States found that 53 percent of breaches were “attributable to internal mistakes or neglect” while 47 percent of breaches were from external sources and primarily the result of hacking or other IT incidents (Jiang 2019, 266).

HIPAA, however, was only the first step on the road to protecting electronic PHI, and that first step was taken twenty-five years ago. Banerjee explains:

When HIPAA was enacted, healthcare service provider’s medical record documents were the primary, if not the only, sources of health information. This is the reason why non-healthcare entities were not included in the purview of the law. However, increased penetration of technologies capable of generating PHI, the lack of laws to protect user data from [non-covered entities], and the increasing diversity of non-healthcare providers with access to such information, have together increased the risks of consumer data breaches and misuse. (Banerjee 2018, 7)

Subsequent federal legislation has “failed to address the new privacy and security challenges presented by the digitization of health information” (Theodos 2021, para. 7). Notably, these new technologies function outside the purview of HHS and are not required to protect health information (Theodos 2021). According to Rosenbloom (2019), “advances in technology, diffusion of health IT across diverse sectors of health care, [and] patients’ expectations,” such as immediate availability of information and apps on mobile devices, contribute to compromises in privacy (1118, 1115). Many apps neither transmit data over a secure connection nor encrypt it, and they may legally sell to data brokers what would in other contexts be PHI (Galvin 2020, 36).

Wearable devices are also of concern. Wearables measure and report physiological and behavioral information as varied as heart rate, amount of sweat, and seizure activity, but that data does not belong to the user; rather, it belongs to the companies that manufacture the devices and store the data (Theodos 2021). Unfortunately, most people who use the devices are unaware of that. In one study, while 70 percent of respondents said confidentiality was important, only 28 percent reported that they were familiar with how their devices protected their privacy,

and only 24 percent were familiar with how their devices transmitted and stored their data (Cilliers 2020, 4–5).

The incremental growth in the use of telehealth, particularly virtual visits, was upended in 2020. To limit the transmission of COVID-19, healthcare providers instituted virtual visits, either by phone or by video. Concerns about privacy were quickly acknowledged by HHS. In February 2020, the department announced that despite the pandemic, HIPAA privacy and security rules would for the most part remain in effect (Bassan 2020, 2). However, only a month later and with the goal of encouraging the use of telehealth, HHS changed course and issued a Notification of Enforcement Discretion that relaxed HIPAA rules (Bassan 2020, 5; Mortell 2020, 390). The relaxed standards apply to technologies that “include video-conferencing, the internet, asynchronous imaging, streaming media, landline, and wireless communications” (Bassan 2020, 5). HHS specifically stated that a healthcare provider may use technologies that “may not fully comply with the requirements of the HIPAA rules,” if the provider makes a good faith effort to keep patient data private. Included among these technologies are FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, and Skype (HHS 2021). As of June 2021, the Notification of Enforcement Discretion has no expiration date (HHS 2020b).

The use of telehealth has increased exponentially during the COVID-19 pandemic; in some hospital systems, the use increased by thousands of percent (Ramaswamy 2020, 1). As Bassan writes, “Given the implementation of the technology during the pandemic, it is unlikely that the use of telehealth would disappear after the pandemic” (Bassan 2020, 11). Perhaps most importantly for the future of telemedicine, outpatients were significantly more satisfied with virtual visits during the pandemic than they were with in-person visits prior to it (Ramaswamy 2020, 5); even before COVID-19, one study showed that while fewer than 4 percent of people had had a video visit with a healthcare provider, almost 50 percent were willing to do so (Fischer 2020, 5).

The use of wearable devices is also increasing: in 2020, 29.8 percent of Americans reported using an electronic wearable device to track health or activity, compared with 26.7 percent in 2019 (US National Cancer Institute 2020). According to a recent Gallup poll, 32 percent of Americans have at some point tracked health data using an app (McCarthy 2019). HIPAA, even with its privacy and security rules in place, is not a sufficient guarantor of healthcare information privacy and should be updated to better align “individual access to health data with the current



realities of electronic medical records and the expectations of modern, engaged patients” (Rosenbloom 2019, 1118).

It is unreasonable to expect that patients will understand—or even read—complicated privacy statements. Bassan suggests that HHS institute regulations like those in the California Consumer Privacy Act: companies must disclose what information they’re collecting, what they’re doing with it, and whether they’re selling it to third parties, and patients should have access to all collected information and the opportunity to opt out of sharing (Bassan 2020, 9). All healthcare providers should invest in cybersecurity and build videoconferencing products that include “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” (Jalali 2021, 672). HHS should also extend HIPAA’s existing rules to

noncovered entities, wearable devices, and apps (Rosenbloom 2019, 1116). Banerjee recommends that HHS create “a ‘watchdog’ unit that is charged with identifying and monitoring types of new behavioral data that can be captured by wearable technology,” determining whether that data is identifiable, and, if necessary, adding it to HIPAA’s catalog of technologies that can be used to identify a specific patient (Banerjee 2018, 7).

Telehealth products and services will undoubtedly proliferate and mature over the next twenty-five years, much as they have in the twenty-five years since HIPAA was first enacted. Any new laws, regulations, and government and industry cooperative agreements must be developed with that growth in mind. Health information is some of the most intimate information there is, and patients’ right to privacy and the security of their data must be preserved, no matter what the technology.

References

- Banerjee, Syagnik, Thomas Hemphill, and Phil Longstreet. 2018. “Wearable Devices and Healthcare: Data Sharing and Privacy.” *The Information Society* 34, no. 1: 49–57.
- Bassan, Sharon. 2020. “Data Privacy Considerations for Telehealth Consumers Amid COVID-19.” *Journal of Law and the Biosciences* 7, no. 1: 1–12.
- Cilliers, Liezel. 2020. “Wearable Devices in Healthcare: Privacy and Information Security Issues.” *Health Information Management Journal* 49, no. 2-3: 150–56.
- Enlund, Sydne. 2020. “Tapping Into Telehealth to Expand Care.” *LegisBrief* 28, no. 5: 1–2.
- Fischer, Shira H., Kristin N. Ray, Ateev Mehrotra, Erika Litvin Bloom, and Lori Uscher-Pines. 2020. “Prevalence and Characteristics of Telehealth Utilization in the United States.” *JAMA Network Open* 3, no. 10: e2022302–e2022302.
- Gajjarwala, Shilpa N., and Jessica N. Pelkowski. 2021. “Telehealth Benefits and Barriers.” *The Journal for Nurse Practitioners* 17, no. 2: 218–21.
- Galvin, Hannah K., and Paul R. DeMuro. 2020. “Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016–2019.” *Yearbook of Medical Informatics* 29, no. 1: 32–43.
- Jalali, Mohammad S., Adam Landman, and William J. Gordon. 2021. “Telemedicine, Privacy, and Information Security in the Age of COVID-19.” *Journal of the American Medical Informatics Association* 28, no. 3: 671–72.
- Jiang, John Xuefeng, and Ge Bai. 2019. “Evaluation of Causes of Protected Health Information Breaches.” *JAMA Internal Medicine* 179, no. 2: 265–67.
- McCarthy, Justin. 2019. “One in Five U.S. Adults Use Health Apps, Wearable Trackers.” Gallup, December 11. <https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx>.
- Mortell, Thomas J., and Austin T. Strobel. 2020. “Changes in the Office for Civil Rights Enforcement Policy on Telehealth Remote Communications in Response to COVID-19.” *Journal of Pediatric Rehabilitation Medicine* 13, no. 3: 389–92.
- Ramaswamy, Ashwin, Miko Yu, Siri Drangsholt, Eric Ng, Patrick J. Culligan, Peter N. Schlegel, and Jim C. Hu. 2020. “Patient Satisfaction With Telemedicine During the COVID-19 Pandemic: Retrospective Cohort Study.” *Journal of Medical Internet Research* 22, no. 9: e20786.
- Rosenbloom, S. Trent, Jeffery R. L. Smith, Rita Bowen, Janelle Burns, Lauren Riplinger, and Thomas H. Payne. 2019. “Updating HIPAA for the Electronic Medical Record Era.” *Journal of the American Medical Informatics Association* 26, no. 10: 1115–19.
- Tariq Rayhan A., and Pamela B. Hackert. 2018. *Patient Confidentiality*. Treasure Island, FL: StatPearls. <https://www.ncbi.nlm.nih.gov/books/NBK519540/>.
- Theodos, Kim, and Scott Sittig. 2021. “Health Information Privacy Laws in the Digital Age: HIPAA Doesn’t Apply.” *Perspectives in Health Information Management* 18 (Winter).
- US Department of Health and Human Services (HHS). n.d. “Telehealth.” Accessed May 11, 2021. <https://www.hhs.gov/hipaa/for-professionals/faq/telehealth/index.html>.



- . 2013. “Summary of the HIPAA Privacy Rule.” <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>.
- . 2020a. “Your Rights Under HIPAA.” <https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html>.
- . 2020b. “When Does the Notification of Enforcement Discretion Regarding COVID-19 and Remote Telehealth Communications Expire?” <https://www.hhs.gov/hipaa/for-professionals/faq/3020/when-does-the-notification-of-enforcement-discretion-regarding-covid-19-and-remote-telehealth-communications-expire/index.html>.
- . 2021. “Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency.” <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>.
- US National Cancer Institute. 2020. “Health Information National Trends Survey: In the Past 12 Months, Have You Used an Electronic Wearable Device to Monitor or Track Your Health or Activity?” <https://hints.cancer.gov/view-questions-topics/question-details.aspx?qid=1746>.



INTELLECTUAL FREEDOM ROUND TABLE

IFRT offers the opportunity for greater involvement in defending intellectual freedom.

Become a member for only \$15 a year.

Join: ala.org/membership

Engage: ala.org/ifrt

 @IFRT_ALA  IFRTALA

	FREE eLEARNING & EDUCATION
	CONNECTIONS & COMMUNITY TO COMBAT CENSORSHIP
	RECOGNITION OF PROFESSIONAL ACHIEVEMENT THROUGH AWARDS

"LIBRARIES SHOULD CHALLENGE CENSORSHIP IN THE FULFILLMENT OF THEIR RESPONSIBILITY TO PROVIDE INFORMATION AND ENLIGHTENMENT."

Library Bill of Rights