GT GreenbergTraurig

Alert | Health Care & FDA Practice/ Data Privacy & Cybersecurity

October 2023

Telehealth Privacy and Security Risk Mitigation: Office for Civil Rights Provides Guidance to Providers, Patients

On Oct. 18, 2023, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued two resources for health care providers and patients regarding the potential risks of using telehealth services. Although HIPAA does not require regulated entities to educate patients about these risks, OCR published these guidance documents to assist providers that wish to voluntarily inform patients of potential privacy and security exposures stemming from the use of telehealth tools.

The first resource, *Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth*, is intended to assist providers in educating patients on how to use telehealth technologies safely. This guidance includes suggestions for how to explain the applicability of HIPAA to remote communication vendors, how telehealth may be used in practice, and how to prepare patients for the use of such technologies. The guidance also includes a non-exhaustive list of risks associated with remote communications (e.g., the chance that health information could inadvertently be disclosed if the patient participates in a telehealth session in a public location) and emphasizes the importance of implementing software updates to avoid potential exploitation of software weaknesses. Finally, the guidance reminds providers that patients have a right to file a privacy complaint if they feel there has been a violation of their privacy rights. Patients can make such complaints via the OCR complaint portal.

The second guidance document, *Telehealth Privacy and Security Tips for Patients*, provides suggestions for patients to better control and improve the security of their devices when accessing telehealth services and transmitting their protected health information. These recommendations include traditional electronic security approaches, such as using strong unique passwords, using encryption tools when possible, and avoiding public wi-fi connections. The guidance also encourages patients to delete health information from personal devices once the patient no longer needs to retain such information, and to turn off devices that may be listening to telehealth meetings, such as smart devices. Further, the guidance encourages patients to note agency guidance related to protecting cell phone privacy and security, improving security when using telehealth services, and ensuring cybersecurity in patients' personal devices.

Authors

This GT Alert was prepared by:

- Catherine E. Galea | +1 215.972.5981 | Cate.Galea@gtlaw.com
- Brad M. Rostolsky | +1 215.972.5936 | Brad.Rostolsky@gtlaw.com
- Tyler Strobel | +1 303.685.7453 | Tyler.Strobel@gtlaw.com