COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 2. February 08, 2024 'An Unknown Individual Walked In': Protecting Against Telehealth Risks Includes Non-IT Threats

By Theresa Defino

The HHS Office for Civil Rights (OCR) and other government agencies aren't just worried that providers understand—and mitigate—the privacy and security risks of telehealth.

In fact, in 2022, the Government Accountability Office (GAO) issued *Medicare Telehealth Actions Needed to Strengthen Oversight and Help Providers Educate Patients on Privacy and Security Risks.*[1] While three of GAO's four recommendations were directed at the Centers for Medicare & Medicaid Services, it had one for OCR, which prompted the agency's two-part guidance for providers on helping patients protected health information (PHI) stay safe during a telehealth visit.

GAO offered eye-opening information from OCR about some complaints received during the pandemic about telehealth—data agency officials don't appear to have shared publicly outside of the report. The nature of some of the complaints harkens back to age-old privacy issues, such as conversations not really being private, which have little to do with the technology of telehealth. These can serve as reminders to providers that a focus on foundational issues still will serve them well, particularly as certain telehealth flexibilities adopted during the pandemic become permanent, ensuring that not only is telehealth here to stay, it is growing.

An article in a recent *RPP* offered experts' suggestions for providers and other covered entities (CEs) to ensure their telehealth programs are HIPAA-compliant, particularly now that OCR's noncompliance waivers have expired.[2] Revising, if necessary, contracts with vendors and other business associates to employ only products that meet privacy and security requirements is among the tasks that—if not already completed—are overdue.

According to GAO, "from March 2020 through December 2021, OCR received 43 complaints regarding privacy and security concerns with telehealth visits."

Among them:

- Seventeen people said that "third parties were present during a telehealth visit," with some complaining that they saw "an unknown individual walk behind the provider."
- Thirteen people "alleged the provider shared patients' PHI without permission during their telehealth visit."
- Seven others "alleged patients overheard or saw the PHI of another patient."

Small Providers May Lack Funds for Secure Solutions

Just six complaints dealt directly with a telehealth platform itself, OCR told GAO. "Specifically, five patients and one employee of a covered provider alleged that providers were using telehealth platforms that did not meet the HIPAA requirements." (This, of course, might have been okay during the enforcement discretion period).

GAO wasn't able to assess how widespread the use of noncompliant telehealth platforms was at the time it

completed its report. Twenty of 26 "provider groups with whom we spoke said providers' use of telehealth platforms that may not meet HIPAA Rule requirements varied," the report states. Five "said investing in HIPAA-compliant telehealth platforms may be difficult for small practices." This could spell trouble because such groups make up the majority of medical providers in the United States.

GAO also reported that "when telehealth platforms are used for a health care visit, the communication between the provider and patient is subject to the HIPAA Privacy Rule. If the communication also involves the electronic transmission of PHI over the telehealth platform, it is subject to the HIPAA Security Rule."

OCR communicated to GAO that "the primary privacy risks are that the oral conversation will be overheard, or the telehealth platform vendor will inappropriately use or disclose information—such as a transcript or image (e.g., a digital x-ray that includes PHI, such as the patient's name)—relating to the communication; and security risks for the protection of electronic PHI are that the telehealth platform will not have adequate security features to protect the electronic PHI, or a covered provider or patient will not activate those features if they are available."