Privacy, Security, and Telehealth

How do ophthalmologists ensure that their practices are adhering to the HIPAA Privacy, Security, and Breach Notification Rules during the COVID-19 pandemic?

BY NANCY L. PERKINS

The COVID-19 pandemic has created a surge in the use of online communication for health care purposes. The risk of exposure to the virus associated with in-person visits to treating physicians has escalated the demand for telehealth, regardless of specialty. Telehealth creates opportunities for eye surgeons and others, but it also comes with risks, including risks to patient privacy and to the security of their personal information.

Under privacy and security regulations implementing HIPAA, physicians who are HIPAA-covered entities are responsible for ensuring that their communications involving the transmission of personal (protected) health information (PHI) are secure. The use of a third-party communications service involving PHI generally triggers a requirement for a HIPAA business associate agreement (BAA) with the provider of the service, which binds the service provider (ie, business associate) to privacy, security, and security breach notification requirements under the HIPAA Privacy, Security, and Breach Notification Rules.

Physicians have become sophisticated about these requirements with respect to provider-to-provider communication. In these situations, security controls such as end-to-end encryption and user authentication measures are typically used to protect PHI included in their communications. But telehealth with patients rarely works as smoothly: Patients may not have access to or be able to afford the types of technology that best serve to secure their PHI. Moreover, during the current pandemic, finding service providers with sufficiently secure technologies that are willing to sign HIPAA BAAs has been challenging.

FREQUENTLY ASKED QUESTIONS

This article examines six major questions on HIPAA privacy and security as they relate to telehealth in the current pandemic climate and beyond.

▸ **No. 1: What solutions are available during the COVID-19 pandemic period?** The Office of Civil Rights (OCR) at the Department of Health and Human Services administers the HIPAA Privacy, Security, and Breach Notification Rules. The OCR has issued a series of notices this year in response to the COVID-19 emergency, including a notice of enforcement discretion related to telehealth.

On March 17, the OCR announced that, effective immediately, it would waive potential penalties for violations of the HIPAA Rules for health care providers and their business associates who conduct telehealth through "everyday communications technologies" during the COVID-19 nationwide public health emergency.[1] A few days later, the OCR released guidance regarding the purpose and scope of the waiver.

As OCR Director Roger Severino explained, the waiver is intended to empower "medical providers to serve patients wherever they are during this national public health emergency," whether for purposes related to COVID-19 or for other treatment needs. The waiver does not extend to HIPAA-covered entities that are health plans or their business associates but specifically focuses on provider communications with patients, including through third-party technology.

▶ **No. 2: What does the OCR'S waiver permit?** Under the OCR telehealth-related waiver, HIPAA-covered health care providers "will not be subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules that occur in the good faith provision of telehealth during the COVID-19 nationwide public health emergency."[2]

What does that mean in practice? What risks of HIPAA violations are most likely in the context of telehealth? HIPAA-related risks from using remote technologies to deliver health care include:

- Violating the HIPAA Privacy Rule by disclosing PHI to a person other than the patient;
- Violating the HIPAA Security Rule by using communications technologies that fail to safeguard the security of electronic PHI;
- Violating both the Privacy and Security Rules by electronically transmitting PHI through a communications vendor without entering into a HIPAA BAA with the vendor; and
- Violating the HIPAA Breach Notification Rule if there is a data security breach involving the vendor's technology and the vendor fails to report the breach (resulting in breach notifications not being made to individuals or to the Department of Health and Human Services).

The OCR waiver might protect against enforcement for these violations, but it is not clear that the waiver would protect against them. That will depend on whether the delivery of telehealth in the particular instance was in good faith.

▶ **No. 3: What is a good faith provision of telehealth services?** The OCR provided guidance on what would *not* constitute a good faith provision of telehealth services:

- Engaging in identity theft or any intentional invasion of privacy;
- Using or disclosing patient data transmitted during a telehealth communication for purposes not authorized under the HIPAA Privacy Rule;
- Violating state licensing laws or professional ethical standards; and
- Using public-facing remote communications products deemed unacceptable by the OCR for telehealth because they are designed to be open to the public or allow wide or indiscriminate access to the communications they host.[3]

The first three types of bad faith conduct are clearly recognizable as inconsistent with legal and ethical principles. The last may require at least some health care providers to do some diligence.

▶ **No. 4: Which remote communications products are public-facing, and which are not?** Public-facing communications products such as a public chat room on the internet (eg, Slack) are designed to be open to the public. Other examples of public-facing products are communications channels such as TikTok, Facebook Live, and Twitch. None of these products strictly controls access by uninvited participants.

In contrast, a nonpublic-facing remote communications product blocks anyone other than the parties intended to be included in the communication from entering the

ACCEPTABLE PRODUCTS FOR TELEHEALTH COMMUNICATIONS

Video Telecommunication Platforms

- Apple FaceTime
- Facebook Messenger video chat
- Google Meet (formerly Hangouts Meet) video
- WhatsApp video chat
- Skype

Texting Platforms

- Signal
- Jabber
- Facebook Messenger
- Google Meet (formerly Hangouts Meet)
- WhatsApp
- iMessage

These lists are not exclusive, and the Office of Civil Rights may update them in the future to include other products that meet the criteria for nonpublic-facing platforms.

communication. In announcing its waiver, the OCR identified examples of nonpublic-facing products that would be acceptable (see *Acceptable Products for Telehealth Communications,* pg 65).

As the OCR notes, the nonpublic-facing platforms it identified typically provide end-to-end encryption, which allows only an individual and the person with whom the individual is communicating to see what is transmitted. These platforms also provide individual user accounts, logins, and passcodes for participants and generally give participants control over privacy-related options such as recording the communication, muting their own lines, or turning off the video or audio signal at any time.

When the OCR issued its notice of enforcement discretion on telehealth, Zoom was receiving considerable criticism over reported security vulnerabilities and apparently would have been a risky choice of communications vendor for telehealth purposes. This provider has since taken steps to address these vulnerabilities, including offering end-to-end encryption to both paying and nonpaying users. Given that this platform also provides muting, recording, and shutting off audio at any time, the OCR would likely consider Zoom an acceptable, nonpublic-facing platform at this time.

▸ **No. 5: Will all nonpublic-facing communications product vendors enter into BAAs?** Some vendors of telehealth technology, including Doxy.me, Google Meet (formerly Hangouts Meet), Skype for Business, Updox, VSee, and Zoom for Healthcare, offer to enter into HIPAA BAAs with their customers. Many other vendors, however, including those that offer nonpublic-facing communications platforms that can be used for telehealth, do not purport to provide the level of data protection mandated under a HIPAA BAA.

For as long as the OCR waiver for good faith telehealth remains in place, HIPAA-covered entities may use nonpublic-facing communications platforms (including Apple FaceTime, Facebook Messenger video chat, Google Meet video, and Skype) to provide telehealth during the COVID-19 emergency period even if the vendors of those platforms do not execute HIPAA BAAs. Health care providers that use such vendors, however, should warn patients of the associated data security risks. Furthermore, all providers offering telehealth should conduct sessions in private settings such as in a clinic or office and should encourage patients to conduct their sessions in a separate room at home or elsewhere. Patients should not receive telehealth services in public or semipublic settings, absent their explicit request after being informed of the risk or in exigent circumstances.

▸ **No. 6: What about telehealth under HIPAA in the long term?** The forced reliance on telehealth during the COVID-19 pandemic to protect patients and physicians almost certainly will result in an expanded use of telehealth in the long term. In a study conducted in April, approximately 90% of the respondents in a survey of more than 1,000 physicians reported using at least some form of telehealth, and 60% said they were planning to continue that practice after the emergency.[4]

The HIPAA waivers currently in place are not intended as long-term provisions of law, however, and are expressly intended to expire once the COVID-19 national public health emergency is over. Providers that seek to take advantage of the benefits of telehealth, including its considerable efficiencies and cost-effectiveness, should be planning for adequate privacy in their telehealth policies, procedures, technology, and contractual provisions for the long term.

Health care providers should actively press telehealth communications vendors for descriptions of their security measures and, once the waiver expires, must require that the vendors enter into BAAs. Comparison shopping with a variety of vendors is recommended, with demands for end-to-end encryption and the other types of security controls mentioned earlier in this article.

Technology can be expected to advance rapidly, and health care providers should not rest easy with a telehealth communications vendor whose security measures do not keep pace. Hackers will constantly be developing and testing new avenues by which to intrude on communications systems where PHI is available because health care information reportedly is of far greater value than credit card information.[5] Providers must be proactive about these risks in order to meet the requirements of the HIPAA Security Rule and state laws for reasonable security.

CONCLUSION

Telehealth is in its infancy and promises to have a long life. Ideally, it should be as private and secure as a physician-patient meeting in a closed-door physician's office. If providers are educated on the risks, they can work to mitigate them. The OCR's current waiver should not be construed to minimize the risks but rather to highlight them. ■

1. US Department of Health & Human Services. OCR announces notification of enforcement discretion for telehealth remote communications during the COVID-19 nationwide public health emergency. March 17, 2020. Accessed August 6, 2020. https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html
2. US Department of Health and Human Services Office for Civil Rights. FAQs on telehealth and HIPAA during the COVID-19 nationwide public health emergency. https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf
3. US Department of Health & Human Services. Notification of enforcement discretion for telehealth remote communications during the COVID-19 nationwide public health emergency. Accessed August 6, 2020. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html
4. Sermo Team. Telemedicine explodes in these uncertain times. Sermo. April 16, 2020. Accessed August 6, 2020. https://www.sermo.com/blog-telemedicine-explodes-in-these-uncertain-times
5. Yao M. Your electronic medical records could be worth $1000 to hackers. Forbes. April 14, 2017. Accessed August 6, 2020. https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#b836c4850cf1

NANCY L. PERKINS
- Counsel, Arnold & Porter, Washington, DC
- nancy.perkins@arnoldporter.com
- Financial disclosure: None