NELSON HARDIMAN
HEALTHCARE LAWYERS

COVID-19 Public Health Emergency Prompts Relaxed Enforcement of HIPAA Requirements Relating to Telehealth

The novel coronavirus (*coronavirus* 2 or "SARS-CoV-2," which causes COVID-19) has placed healthcare professionals in a challenging situation in terms of needing to respond to the crisis, while at the same time minimizing contact with all patients in order to curb the spread of the disease. In record numbers, health care professionals who have historically provided in-person services are having to pivot to telehealth for safety purposes within a matter of days.

On March 17, 2020, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) announced that it would use its enforcement discretion and not impose penalties for noncompliance with certain HIPAA requirements in connection with the good-faith provision of telehealth. According to OCR's Director, the agency is "empowering medical providers to serve patients wherever they are during this national public health emergency," and is "especially concerned about reaching those most at risk, including older persons and persons with disabilities." OCR's enforcement relaxation is effective as of March 17, 2020, and will last until OCR issues another notice, presumably through the duration of the COVID-19 public health emergency. OCR's COVID-19 and HIPAA notices and guidance are available here.

What do the HIPAA Rules require under normal circumstances?

OCR enforces certain regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, to protect the privacy and security of protected health information, namely the HIPAA Privacy, Security and Breach Notification Rules (the HIPAA Rules).

Under normal circumstances, individuals and entities subject to the HIPAA Rules as covered entities or business associates are expected to protect the security of health information protected by implementing administrative, physical, and technical safeguards to protect identifiable health information covered by the HIPAA Rules ("protected health information" or "PHI"). Among other things, the Security Rule requires that appropriate measures are taken to secure electronic PHI at rest and in transit. Encryption of PHI at rest and in transit is a best practice. However, under the HIPAA Rules, encryption is an "addressable" safeguard (but not a standard that may be ignored), leaving some flexibility in terms of implementation, based on a security risk assessment.

Compliance with the HIPAA Rules generally would require a thorough evaluation of the technology used to provide telehealth services, and under normal circumstances would preclude the use of various solutions that are out there for remote communication due to lack of security.

Additionally, under normal circumstances a business associate agreement (BAA) would need to be put into place with the vendor who provides remote communication solutions before the vendor is allowed access to the PHI.

What is the OCR allowing in response to COVID-19?

In the midst of the current COVID-19 public health emergency, providers may make "good faith" use of audio or video communication technology to provide telehealth to patients via any "**non-public facing remote communication**" product available to communicate with patients, and these technologies may be used without

entering into a BAA with the vendor. While OCR's notice seems to suggest that any use of these products would be appropriate, we note that OCR has also encouraged notification of patients that these third-party applications potentially introduce privacy risks and has stated that providers **should enable all available encryption and privacy modes when using such applications**. We also note that in our view "good faith use" does not involve using products that are more convenient when a secure solution with a BAA in place is available. So before using a product, we recommend reviewing what relationships already exist with vendors supplying secure products under a BAA agreement. In addition, health plans are introducing lists of acceptable platforms that should be reviewed, if possible, to ensure reimbursement. As one example, at least one health plan has suggested that **Skype for Business** is acceptable, but not the more basic **Skype.**

What would OCR consider to be "bad faith" use of telehealth?

OCR will evaluate all facts and circumstances when evaluating whether use of telehealth was in bad faith, but has provided the following examples:

- Conduct or furtherance of a criminal act, such as fraud, identity theft, and intentional invasion of privacy;
- Further uses or disclosures of patient data transmitted during a telehealth communication that are prohibited by the HIPAA Privacy Rule (e.g., sale of the data, or use of the data for marketing without authorization);
- Violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth (i.e., based on documented findings of a health care licensing or professional ethics board); and
- Use of public-facing remote communication products (see below for further explanation).

What is a "non-public facing remote communication"?

Per the OCR's guidance, a "non-public facing" remote communication product is one that, as a default, allows only the intended parties to participate in the communication. Health care providers may in good faith provide telehealth via popular applications that allow for video chats, including **Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Whatsapp video chat, or Skype**, without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules.

Which platforms are still prohibited during this emergency?

Per the OCR's notice, Facebook Live, Twitch, TikTok, and similar video communication applications are considered "public facing" (e.g. they are designed to be open to the public/allow indiscriminate access) and should not be used to provide telehealth by covered health care providers.

Does this only affect patients and providers affected by COVID-19?

No. This exercise of discretion applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19. It also applies to all patients regardless of payor status, including those patients that receive Medicare or Medicaid benefits and those that do not.

Who qualifies as a "health care provider"?

Under HIPAA, any person or organization who furnishes, bills, or is paid for health care in the normal course of business is considered a health care provider. By contrast, a health insurance company that merely pays for telehealth services would not be covered by this enforcement discretion.

Does this enforcement discretion also apply to violations of 42 CFR Part 2 (which protects the confidentiality of substance use disorder patient records)?

No. See SAMHSA's separate COVID-19 guidance here.

Do health care providers and/or patients have to be in professional office or health care facility when telehealth services are being provided for the enforcement discretion to apply?

Not necessarily. However, OCR has stated that it expects providers will ordinarily conduct telehealth in private settings, such as a doctor in a clinic or office connecting to a patient who is at home or at another clinic. Providers should always use private locations, and patients should not receive telehealth services in public or semi-public settings, absent patient consent or exigent circumstances.

If telehealth cannot be provided in a private setting, covered health care providers should continue to implement reasonable HIPAA safeguards to limit incidental uses or disclosures of protected health information (PHI).

Does OCR's lack of enforcement eliminate the risks presented by my using a product that does not comply with HIPAA?

No. Among other things, state law requirements still apply and may require you to implement HIPAA-level safeguards, and the HIPAA breach reporting requirement has not been suspended. The cost of a health information breach goes beyond enforcement penalties and is estimated at $429 per record according to the IBM Security and Ponemon Institute's 2019 Cost of Data Breach Study. As a result, securing health information is still necessary for risk management purposes and use of secure methods is still recommended. The list below includes some vendors that represent that they provide HIPAA-compliant video communication products and that they will enter into a HIPAA BAA.

- Skype for Business
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet

What other considerations should providers keep in mind when using telehealth?

Despite this relaxed HIPAA enforcement, providers are reminded not to forego other telehealth-related requirements and best practices at this time. These include but are not limited to meeting the applicable standard of care when treating patients, meeting legal requirements for prescribing, if applicable, obtaining informed patient consent for the use of telehealth, ensuring that providing the care using the communication product is legally permitted as "telehealth" under state law(s), and meeting all other applicable licensure and reimbursement requirements.

Nelson Hardiman lawyers are closely monitoring the response to the novel coronavirus and are experts in health care privacy and telehealth.

Written by Lara Compton and Kristina Sherry.

For more information, please contact:

Lara Compton, Partner
lcompton@nelsonhardiman.com

Kristina Sherry, Attorney at Law
ksherry@nelsonhardiman.com

Harry Nelson, Founding Partner
hnelson@nelsonhardiman.com