March 24, 2020

OCR Releases FAQs Clarifying Telehealth Enforcement Discretion During COVID-19

On March 20, 2020, the Office for Civil Rights at the U.S. Department of Health and Human Services ("OCR") released guidance in the form of FAQs[1] clarifying its notification earlier in the week that it would not penalize health care providers for noncompliance with HIPAA rules in the good faith provision of telehealth during the nationwide COVID-19 public health emergency (the "Notification of Enforcement Discretion" or "Notification").[2]

The FAQs clarify that the scope of OCR's enforcement discretion is "all health care providers that are covered by HIPAA and provide telehealth services during the emergency",[3] and clarifies a number of additional topics, most notably: where telehealth can be conducted; what services can be provided; what constitutes bad faith; and permissible communication products. Importantly, OCR also specifically notes that the Notification applies to "all HIPAA-covered health care providers, with no limitation on the patients they serve with telehealth, including those patients that receive Medicare or Medicaid benefits, and those that do not."

Where Telehealth Can Be Conducted

OCR notes that health care providers "ordinarily" conduct telehealth in private settings, and patients should not receive telehealth services in public or semi-public settings, "absent patient consent or exigent circumstances." However, if services cannot be provided in a private setting, health care providers should continue to implement reasonable HIPAA safeguards to limit incidental uses or disclosures of protected health information (*e.g.*, lowered voices, not using speakerphone, and recommending that patients move to a reasonable distance from others).

---

[1] OCR, FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency, dated March 20, 2020, available at https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf.

[2] OCR, Notification of Enforcement Discretion for telehealth remote communications during the COVID-19 nationwide public health emergency, dated March 17, 2020, available at https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

[3] As noted by the FAQs, under the Health Insurance Portability and Accountability Act (HIPAA), a "health care provider" is a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Health care providers include, for example, physicians, nurses, clinics, hospitals, home health aides, therapists, other mental health professionals, dentists, pharmacists, laboratories, and any other person or entity that provides health care. A "health care provider" is a covered entity under HIPAA if it transmits any health information in electronic form in connection with a transaction for which the Secretary has adopted a standard (*e.g.*, billing insurance electronically). *See* 45 C.F.R. 160.103 (definitions of health care provider, health care, and covered entity).

Notably, the FAQs clarify that the enforcement discretion does not apply to health insurance companies that "merely pay[] for telehealth services," because they are "not engaged in the provision of health care."

What Services Can Be Provided

The FAQs, like the Notification, defers to a physician's professional judgment in determining what services can be provided, stating that enforcement discretion applies to all telehealth services that a health care provider, in their professional judgement, believes can be provided through telehealth "in the given circumstances of the current emergency," whether or not related to COVID-19. (Relatedly, a separate guidance seems to suggest that substance use disorder information can be disclosed for telehealth treatment.)[4]

What Constitutes Bad Faith

OCR's enforcement discretion is limited to "good faith" provision of telehealth. In the FAQs, OCR states that it would consider "all facts and circumstances" to determine good faith, but gave some examples of what it might consider bad faith:

- 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 telehealth that are prohibited (*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; or
- Use of public-facing remote communication products that OCR has identified as unacceptable.

The limitation related to state licensing laws may continue to create barriers for telehealth. States frequently limit telehealth to providers with in-state licenses (though many states are acting to permit telehealth within the state by out-of-state providers during the COVID-19 public health emergency).[5] The Centers for Medicare & Medicaid Services ("CMS") has waived locational licensing requirements for Medicare and Medicaid reimbursement purposes (permitting providers licensed in one state to receive reimbursement for services provided in another),[6] but state licensing restrictions

---

[4] The Substance Abuse and Mental Health Services Administration ("SAMHSA"), which enforces confidentiality requirements related to substance use disorder records (42 C.F.R. Part 2), acknowledged in a guidance document the "increased need for telehealth," noting that this may mean providers cannot obtain written patient consent. The guidance then cites an existing exception permitting disclosure without prior informed consent in medical emergencies, stating in bold text that "[w]e emphasize that, under the medical emergency exception, providers make their own determinations whether a bona fide medical emergency exists for purposes of providing needed treatment to patients." The suggestion appears to be that providers can rely on the medical emergency exception to disclose substance use disorder information for the purposes of telehealth treatment. The guidance is available at https://www.samhsa.gov/sites/default/files/covid-19-42-cfr-part-2-guidance-03192020.pdf.

[5] *See, e.g.*, New York Executive Order No. 202.5: Continuing Temporary Suspension and Modification of Laws Relating to the Disaster Emergency issued March 18, 2020, available at https://www.governor.ny.gov/news/no-2025-continuing-temporary-suspension-and-modification-laws-relating-disaster-emergency.

[6] CMS, COVID-19 Emergency Declaration Health Care Providers Fact Sheet issued March 13, 2020, available at https://www.cms.gov/files/document/covid19-emergency-declaration-health-care-providers-fact-sheet.pdf; pursuant to authority delegated by the Department of Health and Human Services, Waiver or Modification of Requirements Under Section 1135 of the

continue to apply. In listing "violations of state licensing laws" as an example of bad faith, OCR may be suggesting that if a state took disciplinary action against an out-of-state provider for not having in-state licensing, that action could then also subject the out-of-state provider to OCR penalties.

Permissible Communication Products

OCR enforcement discretion applies to "non-public-facing" remote communication products, which the FAQs define as products that, "as a default, allow[] only the intended parties to participate in the communication." The FAQs include as examples platforms such as Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Whatsapp video chat, or Skype, as well as texting applications such as Signal, Jabber, Facebook Messenger, Google Hangouts, Whatsapp, or iMessage.

OCR noted that these products often employ end-to-end encryption, which allows only the two participating individuals to see what is transmitted. The platforms also support individual user accounts, logins, and passcodes to verify participants and limit access. In addition, participants have some control over capabilities such as recording, muting, or turning off an audio or video signal.

The FAQs reiterate that public-facing products (such as Facebook Live, Twitch, TikTok, and "a chat room like Slack") are not permissible, and that a provider using these products would not be covered by the Notification. For example, a provider hosting a public presentation should not identify patients or provide individual patient advice in such a livestream.

Other Clarifications

Other FAQs in the guidance clarify that the enforcement discretion applies to:

- all patients, whether or not they are covered by Medicare or Medicaid;[7]
- all health care providers covered by HIPAA that provide telehealth, but not health insurance companies that pay for telehealth services;
- all types of telehealth, whether or not payors impose reimbursement restrictions;
- noncompliance with the HIPAA privacy, security, and breach notification rules, but no impact on HHS regulations related to confidentiality of substance abuse disorders;[8] and

---

Social Security Act issued March 13, 2020, available at https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx.

[7] However, information about Medicare and Medicaid coverage of telehealth is linked in the FAQ: https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet and https://edit.cms.gov/files/document/medicare-telehealth-frequently-asked-questions-faqs-31720.pdf.

[8] However, as discussed above, SAMHSA has likewise issued guidance on providing substance use disorder treatment via telehealth during under COVID-19. SAMHSA, COVID-19 Public Health Emergency Response and 42 CFR Part 2 Guidance, available at https://www.samhsa.gov/sites/default/files/covid-19-42-cfr-part-2-guidance-03192020.pdf.

- even when the telehealth session is breached (hacked).

OCR emphasized, as in the Notification, that providers should notify patients that third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications. Finally, the FAQs note that there is no expiration date to the enforcement discretion; OCR will issue a notice when it is no longer exercising enforcement discretion "based upon the latest facts and circumstances."

A full list of the FAQs is available here.