

PUBLICATION

Coronavirus: Significant HIPAA Relief in Telehealth Context Due to COVID-19 Response

Authors: Alisa L. Chestler, Andrew Jacob Droke

March 23, 2020

There is no question that COVID-19 has brought unprecedented change to our world. The temporary relaxation of HIPAA's requirements is one of many examples of the government's efforts to address the public's health care needs during this crisis. Over the last month, the Office for Civil Rights (OCR) has issued temporary waivers and associated guidance regarding HIPAA and telehealth services rendered during the public health emergency. The most recent guidance was released on Friday, March 20, 2020 (the Enforcement FAQs and OCR Press Release), and it confirms the loosening of the HIPAA requirements first described in the Notification of Enforcement Discretion issued on March 17, 2020 (the Notification). These temporary measures are intended to encourage the use of telehealth services and enable social distancing.

Most significantly, the Enforcement FAQs confirm that "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." OCR also confirmed that its exercise of discretion "does not affect the application of the HIPAA Rules to other areas of health care outside of telehealth during the emergency."

A few additional highlights from the Enforcement FAQs include:

- OCR will consider all facts and circumstances when determining what constitutes the "good faith" provision of telehealth services in this context. OCR also confirmed that providers who follow the terms of the Notification and any applicable OCR guidance, including the Enforcement FAQs, will not face HIPAA penalties if they experience a data breach that exposes protected health information from a telehealth session.
- OCR stated that the following activities may constitute "bad faith" and, in turn, be subject to enforcement and penalties: criminal acts, fraud, identity theft, intentional invasions of privacy, sales of protected health information or marketing without an authorization, and, importantly, "violations of state licensing laws or professional ethical standards that result in disciplinary actions related to the treatment offered or provided via telehealth." As a result, state laws and requirements cannot be ignored or overlooked when deploying a new technology under these relaxed standards.
- OCR confirmed that the Notification and Enforcement FAQs should not be construed as approval of all remote communication methods, as providers may only use private communication platforms. "Public-facing products such as TikTok, Facebook Live, Twitch, or a chat room like Slack are not acceptable forms of remote communication for telehealth because they are designed to be open to the public or allow wide or indiscriminate access to the communication." The use of a public-facing product may constitute "bad faith" and result in enforcement activity.
- Finally, OCR stated that it "expects health care 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." OCR also noted that "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 this cannot occur, OCR explained that providers must continue to use safeguards designed to limit incidental uses and disclosures of protected health information.

- The Notification does not have an expiration date, and OCR will issue a separate notice when its exercise of enforcement discretion is to end.

The Notification and Enforcement FAQs offer increased flexibility with respect to telehealth services provided during the public health emergency, and they should help enable the delivery of patient care. However, providers who are using or planning to offer telehealth services via platforms that are not HIPAA compliant during this time should review all guidance in tandem, consider applicable state requirements, and ensure that there is an understanding of the permissions and limitations offered via this latest guidance.

For assistance reviewing or deploying telehealth solutions under this guidance, please contact [Alisa Chestler](#), [Andrew Droke](#), or a member of [Baker Donelson's HIPAA Compliance Team](#). Also, please visit our [Coronavirus \(COVID-19\): What You Need to Know](#) information page on our website.