FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency

1. What is telehealth?

The Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) defines telehealth as the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, and public health and health administration. Technologies include videoconferencing, the internet, store-and-forward imaging, streaming media, and landline and wireless communications.

Telehealth services may be provided, for example, through audio, text messaging, or video communication technology, including videoconferencing software. For purposes of reimbursement, certain payors, including Medicare and Medicaid, may impose restrictions on the types of technologies that can be used.[1] Those restrictions do not limit the scope of the HIPAA Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications.

2. What entities are included and excluded under the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications?

The Notification of Enforcement Discretion issued by the HHS Office for Civil Rights (OCR) applies to all health care providers that are covered by HIPAA and provide telehealth services during the emergency. A health insurance

[1] Medicare pays for many different services that involve use of these types of communications technologies. A fact sheet regarding Medicare payment and coverage is available at: https://www.cms.gov/files/document/03052020-medicare-covid-19-fact-sheet.pdf. Telehealth services paid by Medicare are the services defined in section 1834(m) of the Social Security Act that would otherwise be furnished in person but are instead furnished via real-time, interactive communication technology.

company that pays for telehealth services is not covered by the Notification of Enforcement Discretion.

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 CFR 160.103 (definitions of *health care provider*, *health care*, and *covered entity*).

By contrast, a health insurance company that merely pays for telehealth services would not be covered by the Notification of Enforcement Discretion because it is not engaged in the provision of health care.

3. What patients can a covered health care provider treat under the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications and does it include Medicare and Medicaid patients?

This 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.

Information specifically about telehealth and Medicare is available at 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.

4. Which parts of the HIPAA Rules are included in the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications?

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. This Notification does not affect the application of the HIPAA Rules to other areas of health care outside of telehealth during the emergency.

5. Does the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications apply to violations of 42 CFR Part 2, the HHS regulation that protects the confidentiality of substance use disorder patient records?

No, the Notification addresses the enforcement only of the HIPAA Rules. The Substance Abuse and Mental Health Services Administration (SAMHSA) has issued similar guidance on COVID-19 and 42 CFR Part 2, which is available at: https://www.samhsa.gov/sites/default/files/covid-19-42-cfr-part-2-guidance-03192020.pdf.

6. When does the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications expire?

The Notification of Enforcement Discretion does not have an expiration date. OCR will issue a notice to the public when it is no longer exercising its enforcement discretion based upon the latest facts and circumstances.

7. Where can health care providers conduct telehealth?

OCR 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. 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). Such reasonable precautions could include using lowered voices, not using speakerphone, or recommending that the patient move to a reasonable distance from others when discussing PHI.

8. What telehealth services are covered by the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications?

All services that a covered health care provider, in their professional judgement, believes can be provided through telehealth in the given circumstances of the current emergency are covered by this Notification. This includes diagnosis or treatment of COVID-19 related conditions, such as

taking a patient's temperature or other vitals remotely, and diagnosis or treatment of non-COVID-19 related conditions, such as review of physical therapy practices, mental health counseling, or adjustment of prescriptions, among many others.

9. What may constitute bad faith in the provision of telehealth by a covered health care provider, which would not be covered by the Notification of Enforcement Discretion regarding COVID-19 and remote telehealth communications?

OCR would consider all facts and circumstances when determining whether a health care provider's use of telehealth services is provided in good faith and thereby covered by the Notice. Some examples of what OCR may consider a bad faith provision of telehealth services that is not covered by this Notice include:

- 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); or
- Use of public-facing remote communication products, such as TikTok, Facebook Live, Twitch, or a chat room like Slack, which OCR has identified in the Notification as unacceptable 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.

10. What is a "non-public facing" remote communication product?

A "non-public facing" remote communication product is one that, as a default, allows only the intended parties to participate in the communication.

Non-public facing remote communication products would include, for example, platforms such as Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Whatsapp video chat, Zoom, or Skype. Such products also would include commonly used texting applications such as Signal, Jabber, Facebook Messenger, Google Hangouts, Whatsapp, or

iMessage. Typically, these platforms employ end-to-end encryption, which allows only an individual and the person with whom the individual is communicating to see what is transmitted. The platforms also support individual user accounts, logins, and passcodes to help limit access and verify participants. In addition, participants are able to assert some degree of control over particular capabilities, such as choosing to record or not record the communication or to mute or turn off the video or audio signal at any point.

In contrast, 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. For example, a provider that uses Facebook Live to stream a presentation made available to all its patients about the risks of COVID-19 would not be considered reasonably private provision of telehealth services. A provider that chooses to host such a public-facing presentation would not be covered by the Notification and should not identify patients or offer individualized patient advice in such a livestream.

11. If a covered health care provider uses telehealth services during the COVID-19 outbreak and electronic protected health information is intercepted during transmission, will OCR impose a penalty on the provider for violating the HIPAA Security Rule?

No. OCR will exercise its enforcement discretion and will not pursue otherwise applicable penalties for breaches that result from the good faith provision of telehealth services during the COVID-19 nationwide public health emergency. OCR would consider all facts and circumstances when determining what constitutes a good faith provision of telehealth services. For example, if a provider follows the terms of the Notification and any applicable OCR guidance (such as this and other FAQs on COVID-19 and HIPAA), it will not face HIPAA penalties if it experiences a hack that exposes protected health information from a telehealth session.

OCR believes that many current and commonly available remote electronic communication products include security features to protect ePHI transmitted between health care providers and patients. In addition, video communication vendors familiar with the requirements of the Security Rule often include stronger security capabilities to prevent data interception and

provide assurances they will protect ePHI by signing a HIPAA business associate agreement (BAA). Providers seeking to use video communication products are encouraged to use such vendors, but will not be penalized for using less secure products in their effort to provide the most timely and accessible care possible to patients during the Public Health Emergency. Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.

OCR does not endorse the use of or the security capabilities of any particular communications product.