

Teesta Sisodia-Sullivan, HIPAA Coordinator
Information Technology Division, Privacy and Security Office
North Carolina Department of Health and Human Services <<https://www.ncdhhs.gov/>>

March 17, 2020

Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency

We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities. – Roger Severino, OCR Director.

The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is responsible for enforcing 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).

During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. This notification is effective immediately.

A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients. OCR is exercising its enforcement discretion to not impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency. 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.

For example, a covered health care provider in the exercise of their professional judgement may request to examine a patient exhibiting COVID-19 symptoms, using a video chat application connecting the provider's or patient's phone or desktop computer in order to assess a greater number of patients while limiting the risk of infection of other persons who would be exposed from an in-person consultation. Likewise, a covered health care provider may provide similar telehealth services in the exercise of their professional judgment to assess or treat any other medical condition, even if not related to COVID-19, such as a sprained ankle, dental consultation or psychological evaluation, or other conditions.

Under this Notice, covered health care providers may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide 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.

Under this Notice, however, Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by covered health care providers.

Covered health care providers that seek additional privacy protections for telehealth while using video communication products should provide such services through technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products. 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

Note: OCR has not reviewed the BAAs offered by these vendors, and this list does not constitute an endorsement, certification, or recommendation of specific technology, software, applications, or products. There may be other technology vendors that offer HIPAA-compliant video communication products that will enter into a HIPAA BAA with a covered entity. Further, OCR does not endorse any of the applications that allow for video chats listed above.

Under this Notice, however, OCR will not impose penalties against covered health care providers for the lack of a BAA with video communication vendors or any other noncompliance with the HIPAA Rules that relates to the good faith provision of telehealth services during the COVID-19 nationwide public health emergency.

OCR has published a bulletin advising covered entities of further flexibilities available to them as well as obligations that remain in effect under HIPAA as they respond to crises or emergencies at <https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf> - PDF <<https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf>> .

Guidance on BAAs, including sample BAA provisions, is available at <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html> <<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>> .

Additional information about HIPAA Security Rule safeguards is available at <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> <<https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>> .

HealthIT.gov has technical assistance on telehealth at <https://www.healthit.gov/telehealth> <<https://www.healthit.gov/telehealth>> .

###

This email is being sent to you from the OCR-Security-List listserv, operated by the Office for Civil Rights (OCR) in the US Department of Health and Human Services.

This is an announce-only list, a resource to distribute information about the HIPAA Privacy and Security Rules. For additional information on a wide range of topics about the Privacy and Security Rules, please visit the OCR Privacy website at <http://www.hhs.gov/ocr/privacy/index.html>. You can also call the OCR Privacy toll-free phone line at (866) 627-7748. Information about OCR's civil rights authorities and responsibilities can be found on the OCR home page at <http://www.hhs.gov/ocr/office/index.html>.

If you believe that a person or organization covered by the Privacy and Security Rules (a "covered entity") violated your health information privacy rights or otherwise violated the Privacy or Security Rules, you may file a complaint with OCR. For additional information about how to file a complaint, visit OCR's web page on filing complaints at <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>.

To subscribe to or unsubscribe from the list serv, go to <https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-SECURITY-LIST&a=1> <<https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-SECURITY-LIST&a=1>>

Email correspondence to and from this address is subject to the North Carolina Public Records Law and may be disclosed to third parties by an authorized State official. Unauthorized disclosure of juvenile, health, legally privileged, or otherwise confidential information, including confidential information relating to an ongoing State procurement effort, is prohibited by law. If you have received this email in error, please notify the sender immediately and delete all records of this email.