WORLD **PRIVACY** FORUM

WPF Statement on COVID-19 and Changes in HIPAA Practices

March 18, 2020

In This Statement:

- What are the changes to HIPAA that have been enacted during the COVID-19 national emergency?
- What are the privacy concerns?
- WPF recommendations to ensure patient privacy is protected during and after the emergency

In response to the COVID-19 (coronavirus) pandemic, the U.S. Department of Health and Human Services announced some changes in HIPAA practices. In general, the HIPAA privacy rule already provides plenty of flexibility for operation of the health care system under emergency circumstances. See, for example, a discussion of the rule's provisions and their application in emergency circumstances at: https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf.

During emergencies – like hurricanes and other natural disasters – HHS routinely announces that it will waive sanctions and penalties from noncompliance with selected provisions of the HIPAA privacy rule. These waivers are expressly limited in scope and application and include**:**

> (a) the requirements to obtain a patient's agreement to speak with family members or friends or to honor a patient's request to opt out of the facility directory (45 C.F.R. § 164.510);
> (b) the requirement to distribute a notice of privacy practices (45 C.F.R. § 164.520); and
> (c) the patient's right to request privacy restrictions or confidential communications (45 C.F.R. § 164.522).

These “traditional” waivers are also in place for the coronavirus pandemic. See https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx

All of these actions are familiar and, from the perspective of the World Privacy Forum, unobjectionable. We recognize that privacy rules must make accommodations under emergency circumstances, although there is no reason to abandon privacy rules entirely. Privacy remains an essential element of health care at all times. So does public health.

Additional steps from HHS regarding COVID - 19

For the coronavirus pandemic, HHS took additional steps. HHS announced that it will exercise enforcement discretion and not impose penalties for noncompliance with the HIPAA requirements against covered health care providers who provide in good faith telehealth services during the COVID-19 nationwide public health emergency. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

Normally, the HIPAA security rule requires that a covered entity, including health care providers, must review the risks of using new technologies and must consider whether encryption should be used for communications. The rule requires both a process and documentation of the decisions made. See, for example, 45 C.F.R. §§ 164.306 and 164.308.

The waiver by HHS means that during the emergency, health care providers can use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, or Skype, to provide telehealth services without going through the otherwise required risk evaluation and documentation. HHS will not seek to penalize HIPAA covered entities for noncompliance.

Further, the use of some services provided by a business associate normally requires a business associate agreement between the covered entity and the business associate. HHS will not impose penalties for the absence of an agreement for telehealth functions during the emergency.

The World Privacy Forum understands the need for these waivers in the current circumstances. We note that HHS encourages providers to notify patients of the risks and to use available encryption when using popular applications for telehealth. This is entirely appropriate.

We were pleased to see that HHS carefully distinguished between video communication applications that are public facing – Facebook Live, Twitch, TikTok, and others – and those that are not. Public facing applications pose grave threats to patient privacy, and HHS properly stated that they should not be used by covered entities for telehealth.

Concerns and Recommendations

While the World Privacy Forum supports the announced waivers, we remain concerned that some providers of video communications services may somehow see the use of their services for telehealth as a business opportunity that will allow them to collect, maintain, and exploit information that travels through those communications. **Under present circumstances, no existing law may prevent commercial use of health information communicated in this way.**

WPF has three key recommendations to ensure patient privacy during and after the emergency:

1. We urge that any company involved will exercise restraint and appropriate behavior and expressly avoid collecting or using any health care information (including the mere fact of a communication between provider and patient) that is not essential to the communication service provided.

2. Further, any necessarily retained data should be deleted when the emergency is over.

3. Both providers and patients may need to take steps after the emergency to remove any protected health information from communications applications used for telehealth.

WPF will update this statement about COVID-19 as new information is announced. For more information about health privacy, see our Patient's Guide to HIPAA, available online, in eBook form, and in downloadable PDF.

Health Privacy Resources

A Patient's Guide to HIPAA: https://www.worldprivacyforum.org/2019/03/hipaa/

HIPAA waivers in place for the coronavirus pandemic: https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx

HHS notification of HIPAA enforcement during COVID-19 pandemic: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

HIPAA provisions in emergency circumstances: https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf.