World Privacy Statement on HIPAA Waiver of April 2, 2020 and its Consequential Impacts on Privacy

April 6, 2020

In This Statement:

- **What is a HIPAA waiver? Which waivers are in place during the COVID-19 national emergency?**
- **What changes does the April 2, 2020 HIPAA waiver create?**
- **What are the privacy concerns?**
- **WPF recommendations to correct the problems with the April 2, 2020 HIPAA waiver 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 has announced two changes in HIPAA privacy practices. The newest changes were announced April 2, 2020. This document discusses the April 2 changes to HIPAA, which are substantive and have the potential for far-reaching consequences for patient privacy.

What is a HIPAA Waiver, and which waivers are in place during the COVID-19 national emergency?

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);
> (d) As of March 13, 2020, HHS announced a new HIPAA waiver regarding telehealth. HHS 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. See: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

These "traditional" waivers, plus the two new COVID-19 waivers are in place for the coronavirus pandemic. The traditional waivers were activated March 13, 2020. See https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx.

The World Privacy Forum issued a statement March 18, 2020 about the first COVID-19 HIPAA waiver, which we found appropriate and sufficiently narrow. That statement is here: https://www.worldprivacyforum.org/2020/03/wpf-statement-on-covid-19-and-changes-in-hipaa-practices/.

This statement is regarding the April 2, 2020 COVID-19 HIPAA waiver. The April 2, 2020 waiver announcement is here: https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf

What privacy changes does the April 2, 2020 HIPAA waiver create?

The April 2 HIPAA waiver provides:

> To facilitate uses and disclosures for public health and health oversight activities during this nationwide public health emergency, effective immediately, OCR will exercise its enforcement discretion and will not impose penalties against a business associate or covered entity under the Privacy Rule provisions 45 CFR 164.502(a)(3), 45 CFR 164.502(e)(2), 45 CFR 164.504(e)(1) and (5) if, and only if:
>
> - The business associate makes a good faith use or disclosure of the covered Entity's PHI for public health activities consistent with 45 CFR 164.512(b), or health oversight activities consistent with 45 CFR 164.512(d); and,
> - the business associate informs the covered entity within ten (10) calendar days after the use or disclosure occurs (or commences, with respect to uses or disclosures that will repeat over time).

While the goal of facilitating a quick response to the virus is admirable, the April 2, 2020 HIPAA waiver is substantively different than previous HIPAA waivers due to its extraordinarily broad scope, among other significant problems and concerns.

The April 2 HIPAA waiver seeks to "facilitate uses and disclosures for **public health** and **health oversight activities** during this nationwide public health emergency." It allows a business associate to make a good faith **use or disclosure** of a **covered entity's health records** for **public health activities** or for **health oversight activities**. The business associate must inform the covered entity within **ten calendar days after** the use or disclosure occurs.

In short, this is an unprecedented HIPAA waiver that allows business associates, without the permission of the hospital, clinic, or health care provider, to use or release the protected health information of patients.

HIPAA already allows covered entities like hospitals to use or disclose health records without patient consent for public health activities and for health oversight activities. Public health authorities and public health activities are expansively defined in the HIPAA privacy rule.

In general, disclosures of PHI for public health purposes are reasonable and beneficial. Allowable disclosures include not only traditional public health agencies, but also to persons subject to the Food and Drug Administration for regulated products and activities (e.g., to pharmaceutical manufacturers), to employers under limited conditions, and to schools under narrower circumstances.

HIPAA also already allows covered entities to use or disclose health records without patient consent for health oversight activities. Activities that qualify to receive patient records under this provision include audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of the health care system; government benefits programs for which health is relevant to eligibility; and regulated entities for which health information is necessary for determining compliance with program standards. There are some protections so that information disclosed for health oversight should not be used to investigate individuals for non-health care related activities.

Many of the activities that qualify as health oversight are essential parts of the health care system. However, as with the HIPAA public health provisions, the authority is broad and unbounded in many ways. Many different types of activities qualify as health oversight.

Normally, a covered entity that discloses patient information for health oversight purposes (whether on its own motion or, more likely, in response to a request from an oversight agency) has an incentive to limit disclosures. The tension between covered entities and oversight agencies will normally help to limit overbroad or unreasonable demands for health records.

What are the privacy concerns regarding the April 2, 2020 HIPAA waiver?

We have identified meaningful and far-reaching problems with the April 2, 2020 waiver.

Business Associates are only obliged to act in “good faith"

Under the April 2 waiver, a business associate is only obliged to act in “good faith.” For many business associates who conduct activities that do not involve making health care judgments or applying relevant expertise, the good faith defense might mean no more than “we thought it might help.” The waiver should have been narrowed, and needed to include a requirement for good faith exercise of *professional judgment*. A record storage company should not be making any disclosure decisions about public health matters. It might be appropriate for a medical laboratory that functions as a business associate to make professional judgments about the value of sharing records. The April 2 waiver did not make this distinction.

Business associates can use and/or disclose patient record if it provides notice 10 days *after* the use or disclosure

The April 2 waiver allows a business associate to use or disclose the records it holds for a covered entity **if it provides the entity with notice ten days after the use or disclosure.** If HHS thought there was a need to authorize some activities by business associates, it should have required advance notice to the covered entity with the ability of the covered entity to veto the proposed action by the business associate. If advance notice is impractical, then HHS could have required

notice either concurrently with the business associate's action or at the earlier possible time thereafter.

Ten days is simply too long to allow a business associate to act on its own. A covered entity should have veto authority over actions by its business associate at any time. Further, without notice, a business associate might duplicate efforts already underway by the covered entity. This aspect of the rule is likely to create meaningful privacy problems in the U.S. healthcare system.

No requirement that business associates be public health or health oversight experts

The waiver does not set standards for what types of business associates can use or disclose protected health information of patients without prior notice or consent of the healthcare provider. Under the broad April 2 waiver, any business associate can make uses or disclosures of patient information. There is far too much room for negative outcomes here, because business associates may receive use and disclosure requests from entities which are neither a public health or a health oversight agency. An inexperienced business associate with less knowledge of HIPAA might agree to a disclosure that no covered entity's HIPAA lawyers would allow.

Many non-health companies can be business associates. This waiver opens the door for nearly unconstrained use and disclosure of patient records by any business associate, which could mean thousands of companies.

The waiver allows public health disclosures that are broader than CDC and state public health agencies

The April 2 waiver allows public health disclosures that are broader than what the CDC and similar state public health agencies allow. Currently, the waiver allows additional disclosures as public health disclosures, for example, it allows disclosures to employers under specified circumstances, and it allows disclosures to pharmaceutical manufacturers, again, under specified circumstances.

The waiver allows business associates to use and disclose health records to undertake public health activities on their own, without direction by a public health authority

The April 2 HIPAA waiver allows business associates to *use* and *disclose* health records for public health activities. It is not clear what this authority entails, but it seems to permit a business associate to undertake public health activities on its own, without direction from either the covered entity whose records it holds or without direction from a public health authority. A business associate can convey patient information to a public health authority even if the authority does not want or need the data. If there is a case to be made that some business associates might possibly use records helpfully, it is certain true that *all* business associates cannot do so.

Additionally, business associates can use and disclose health records for health oversight without any requirement for a request from a public health emergency. A business associate may not have an interest in limiting disclosures in the way that a covered entity whose activities are being

overseen would. The business associate is not at risk, and it has no relationship with patients that it has a specific reason to protect.

Business associates do not engage in health oversight activities

The April 2 waiver allows business associates to *use* health records for health oversight purposes. It is not clear what this means, as a business associate does not engage in health oversight. Nor is a business associate likely to pay attention to the already value limit in the HIPAA privacy rule that records disclosed for health oversight should not be used to investigate individuals for non-health care related activities.

Recommendations Regarding the April 2, 2020 HIPAA Waiver

1. **The standard should go beyond good faith. It should require *professional judgement* by a health care professional, health researcher, or public health authority.**

2. **Uses and disclosures under the waiver must be narrowed. The waiver should be more narrowly focused so that it covers only disclosures to traditional government public health agencies. (Federal, state, and local.)**

3. **Veto power by the covered entities is essential: In all circumstances a covered entity should be able to veto unauthorized uses and disclosures by a business associate.**

4. **If no veto power is given, then at a minimum advance notice (even informal notice) to covered entities is necessary.**

5. **If the recommendations regarding veto power and advance notice are not followed, then notice to the covered entity must be concurrent with any uses or disclosures undertaken by the business associate.**

6. **Health oversight activities should be removed from the waiver. It may make sense to authorize disclosures to public health agencies that have the capabilities of responding to the crisis. It doesn't make sense to give the same authority for uses and disclosures to auditors, police, prosecutors and other health oversight entities that do not have expertise in health treatment, research, or public health.**

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/

World Privacy Forum statement March 18, 2020 about the first COVID-19 HIPAA waiver: https://www.worldprivacyforum.org/2020/03/wpf-statement-on-covid-19-and-changes-in-hipaa-practices/.

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

HHS notification of April 2, 2020 HIPAA waiver during COVID-19 pandemic: https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf

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