HIPAA Guidance During COVID-19

March 23, 2020 Kayla Cristales, Jennifer Kreick

PRACTICES Healthcare Transactions and Regulatory, Health Privacy (HIPAA) and Healthcare IT, Healthcare and Life Sciences

UPDATED: 04/09/2020
Amidst continuing COVID-19 concerns, regulators have issued certain guidance and waivers of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requirements and penalties applicable during this public health emergency. A summary of the relevant HIPAA-related guidance is included below.

HIPAA Privacy Guidance During COVID-19

On March 27, 2020, Congress passed the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act"), which contains a requirement for the Department of Health and Human Services ("HHS") to issue guidance no later than 180 days after the enactment of the CARES Act (i.e., by September 23, 2020) on the sharing of individuals' protected health information during the COVID-19 public health emergency. This guidance is to include information on compliance with HIPAA regulations and applicable policies, including such policies that may come into effect during this public health emergency.[1]

On March 24, 2020, the Office for Civil Rights ("OCR") at HHS released guidance on when covered entities may share the name or other identifying information of an individual who has been infected with, or exposed to, the virus SARS-CoV-2, or the disease caused by the virus (COVID-19), with law enforcement, paramedics, other first responders, and public health authorities without an individual's authorization. The guidance reiterated that when HIPAA permits disclosure, except when required by law, or for treatment disclosures, a covered entity must make reasonable efforts to limit the information used or disclosed to that which is the "minimum necessary" to accomplish the purpose for the disclosure.

In addition to outlining the HIPAA rules that permit disclosure (some of which were covered in the February 2020 bulletin discussed below), the guidance includes specific examples of disclosures that covered entities may make under HIPAA to first responders and others. OCR noted that disclosure may be permitted under more than one provision of HIPAA. For example, the following scenarios are permitted under 45 CFR 164.512(a), 164.512(b)(1), and/or 164.512(j)(1), depending on the circumstances:

- A covered entity, such as a hospital, may provide a list of the names and addresses of all individuals it knows to have tested positive, or received treatment, for COVID-19 to an EMS dispatch for use on a per-call basis. The EMS dispatch (even if it is a covered entity) would be allowed to use information on the list to inform EMS personnel who are responding to any particular emergency call so that they can take extra precautions or use personal protective equipment (PPE).

  Discussion: Under this example, a covered entity should not post the contents of such a list publicly, such as on a website or through distribution to the media. A covered entity under this

example also should not distribute compiled lists of individuals to EMS personnel, and instead should disclose only an individual's information on a per-call basis. Sharing the lists or disclosing the contents publicly would not ordinarily constitute the minimum necessary to accomplish the purpose of the disclosure (i.e., protecting the health and safety of the first responders from infectious disease for each particular call).

- A 911 call center may ask screening questions of all callers, for example, their temperature, or whether they have a cough or difficulty breathing, to identify potential cases of COVID-19. To the extent that the call center may be a HIPAA covered entity, the call center is permitted to inform a police officer being dispatched to the scene of the name, address, and screening results of the persons who may be encountered so that the officer can take extra precautions or use PPE to lessen the officer's risk of exposure to COVID-19, even if the subject of the dispatch is for a non-medical situation.

  Discussion: Under this example, a 911 call center that is a covered entity should only disclose the minimum amount of information that the officer needs to take appropriate precautions to minimize the risk of exposure. Depending on the circumstances, the minimum necessary protected health information may include, for example, an individual's name and the result of the screening.

However, OCR reminded covered entities to consult other applicable laws (e.g., state and local statutes and regulations) in their jurisdictions prior to using or making disclosures of individuals' protected health information, as such laws may place further restrictions on disclosures that are permitted by HIPAA. See March Guidance for more information.

OCR had previously released a bulletin in February 2020 to remind covered entities and business associates of the ways patient information may be shared under HIPAA in an outbreak of infectious disease or emergency situation. For example, permitted disclosures include:

- disclosures about the patient as necessary to treat that patient or another patient. See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of "treatment" at 164.501.

- disclosures for public health activities, including:
  - To a public health authority, such as the CDC or a state or local health department authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability. See 45 CFR §§ 164.501 and 164.512(b)(1)(i).
  - At the direction of a public health authority, to a foreign government agency that is acting in collaboration with the public health authority. See 45 CFR 164.512(b)(1)(i).
  - To persons at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations. See 45 CFR 164.512(b)(1)(iv).

- disclosures to a patient's family members, relatives, friends, or other persons identified by the patient as involved in the patient's care. A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death. These disclosures, when necessary, could involve notification to the police, press or the public at large. See 45 CFR 164.510(b).

- disclosures to anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct. See 45 CFR 164.512(j).

The bulletin also reminded covered entities that except in limited circumstances, disclosures to the media or public at large about an identifiable patient are generally prohibited without the patient's written authorization, and providers are still expected to comply with the minimum necessary standard and implement reasonable safeguards to protect patient information during this time.

Finally, the bulletin reiterated that HIPAA applies only to covered entities (health plans, healthcare clearinghouses, and healthcare providers that conduct one or more covered healthcare transactions electronically) and business associates (persons or entities that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting protected health information). While HIPAA often does not apply to employers who receive health information directly from their employees (unless, for example, the employer is a healthcare provider providing healthcare services to its own employees or the employer learned of the healthcare item or service through a health insurance claim filed by the employee), other state and federal privacy laws may apply. Accordingly, employers should exercise caution when sharing individually identifiable health information of their employees. See February Guidance for more information.

HIPAA Enforcement Discretion for COVID-19 Community-Based Testing Sites

Effective March 13, 2020, OCR issued a Notification of Enforcement Discretion (the "CBTS Notice") stating that it will not impose penalties for noncompliance with regulatory requirements under the HIPAA Rules against covered health care providers and their business associates in connection with the good faith participation in the operation of a COVID-19 specimen collection and testing site (Community-Based Testing Site or CBTS) during the COVID-19 nationwide public health emergency. The operation of a CBTS includes all activities that support the collection of specimens from individuals for COVID-19 testing.

Although not required, OCR encouraged providers to implement reasonable safeguards to protect the privacy and security of protected health information ("PHI"), such as:

- Setting up canopies or similar opaque barriers at a CBTS to provide some privacy to individuals during the collection of samples.
- Controlling foot and car traffic to create adequate distancing at the point of service to minimize the ability of persons to see or overhear screening interactions at a CBTS. (According to HHS, a six foot distance would serve this purpose as well as supporting recommended social distancing measures to minimize the risk of spreading COVID-19.)
- Establishing a "buffer zone" to prevent members of the media or public from observing or filming individuals who approach a CBTS, and posting signs prohibiting filming.
- Posting a Notice of Privacy Practices (NPP), or information about how to find the NPP online, if applicable, in a place that is readily viewable by individuals who approach a CBTS.

HHS notes that the CBTS Notice does not apply to health plans or health care clearinghouses when they are performing health plan and clearinghouse functions, or to covered health care

providers or their business associates when they are performing non-CBTS related activities. For example:

- A pharmacy that participates in the operation of a CBTS in the parking lot of its retail facility could be subject to a civil money penalty for HIPAA violations that occur inside its retail facility at that location that are unrelated to the CBTS.
- A covered clinical laboratory that has workforce members working on site at a CBTS could be subject to a civil money penalty for HIPAA violations that occur at the laboratory itself.
- A covered health care provider that experiences a breach of PHI in its existing electronic health record system, which includes PHI gathered from the operation of a CBTS, could be subject to a civil money penalty for violations of the HIPAA Breach Notification Rule if it fails to notify all individuals affected by the breach (including individuals whose PHI was created or received from the operation of a CBTS).

See CBTS Notice for more information.

HIPAA Enforcement Discretion for Business Associates for Public Health/Health Oversight Activities

Effective April 2, 2020, OCR issued a Notification of Enforcement Discretion (the "BAA Notice") stating that it will not impose penalties for violations of certain HIPAA Privacy Rule provisions against health care providers or their business associates during the COVID-19 nationwide public health emergency 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 10 calendar days after the use or disclosure occurs (or commences, with respect to uses or disclosures that will repeat over time).

HIPAA permits a business associate to use and disclose PHI to conduct certain functions or activities on behalf of the covered entity, or provide certain services to the covered entity, but only pursuant to the explicit terms of a business associate agreement ("BAA"), or as required by law. According to the OCR, some business associates were not able to provide federal public health authorities and health oversight agencies, state and local health departments, and state emergency operations centers with PHI or perform public health data analytics on such PHI because their BAAs did not expressly permit these uses and disclosures.

The business associate remains liable for complying with the Security Rule requirements (i.e., ensuring the secure transmission of PHI to the public health authority or health oversight agency), and complying with any other federal or state laws (including breach of contract claims or state privacy laws) that might apply to the uses and disclosures of such information. See BAA Notice for more information.

HIPAA Enforcement Discretion for Telehealth

Effective March 17, 2020, OCR issued a Notification of Enforcement Discretion ("Notice") stating that it will not impose penalties for noncompliance with HIPAA against health care providers in

connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. This Notice applies to telehealth provided for any reason, regardless of whether the services relate to the diagnosis and treatment of COVID-19.

The OCR specified that a covered health care provider may provide telehealth services through any non-public facing remote communication product, including popular applications that allow for chats (e.g., Facebook Messenger video chat or Skype). However, health care providers should not use certain video communication that are public facing (e.g., Facebook Live, Twitch, and TikTok). OCR also will not impose penalties against healthcare providers for the lack of a BAA with a video communication vendor or any other noncompliance with the HIPAA regulations that relates to the good faith provision of telehealth services during the COVID-19 nationwide public health emergency. For healthcare provider seeking additional privacy protections, the Notice provided a list of vendors that represent that they provide HIPAA-compliant video communication products and will enter into HIPAA-compliant BAAs. These vendors include, among others, Skype for Business, Zoom for Healthcare, and Doxy.me. See the Notice, FAQ, and our Client Alert for more information.

Limited Waiver of HIPAA Sanctions and Penalties

Effective March 15, 2020, in response to the President's declaration of a nationwide emergency and the Secretary of HHS' earlier declaration of a public health emergency on January 31, 2020, the Secretary exercised its authority to waive sanctions and penalties against a covered hospital that does not comply with the following provisions of the HIPAA Privacy Rule:

- the requirement to obtain a patient's agreement to speak with family members or friends involved in the patient's care. See 45 CFR 164.510(b).
- the requirement to honor a request to opt out of the facility directory. See 45 CFR 164.510(a).
- the requirement to distribute a notice of privacy practices. See 45 CFR 164.520.
- the patient's right to request privacy restrictions. See 45 CFR 164.522(a).
- the patient's right to request confidential communications. See 45 CFR 164.522(b).

The waiver only applies (1) in the emergency area identified in the public health emergency declaration; (2) to hospitals that have instituted a disaster protocol; and (3) for up to 72 hours from the time the hospital implements its disaster protocol. See the Waiver for more information.

If you have questions regarding COVID-19 and HIPAA compliance and enforcement, please contact a member of our Healthcare and Life Sciences Practice Group below. You can also check out our COVID-19 Resources page for more information.

---

[1] The CARES Act also included provisions that significantly change the federal law (42 U.S.C. § 290dd-2) and its implementing regulations (42 C.F.R. Part 2) (collectively, "Part 2") that govern the confidentiality of substance use disorder records. Although not part of HIPAA, the CARES Act modified Part 2 to align it more closely with certain HIPAA requirements and permit certain additional disclosures. For example, the changes to Part 2 include, among others, (i) incorporating HIPAA's breach notification requirements, (ii) requiring Part 2 programs to provide notices of privacy

practices, and (iii) providing that once a Part 2 program provider obtains the prior written consent of the patient, the substance use disorder record may be used or disclosed by a covered entity, business associate, or Part 2 program for purposes of treatment, payment, and healthcare operations, as permitted by HIPAA, and information so disclosed may then be redisclosed as permitted by HIPAA, until the patient revokes his or her consent. The amendments to Part 2 become effective 12 months after the date of enactment of the CARES Act (i.e., March 27, 2021).