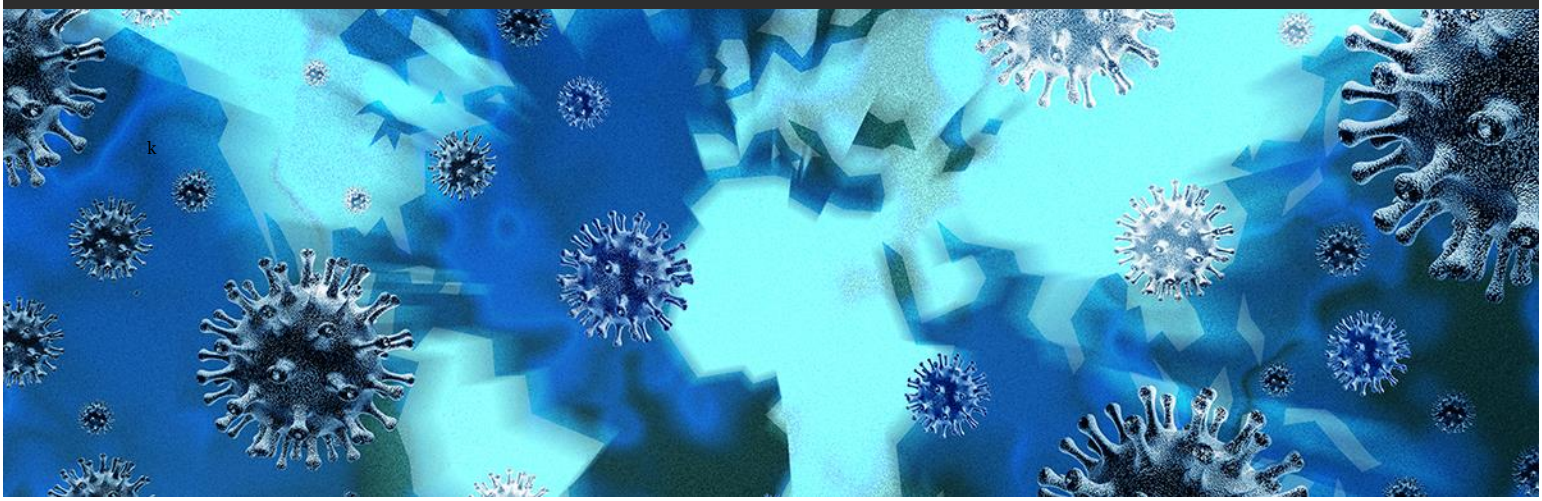
GT GreenbergTraurig

Alert | Health Emergency Preparedness Task Force: Coronavirus Disease 2019



k

March 2020

Sharing Protected Health Information During the COVID-19 Public Health Crisis

In light of the Coronavirus Disease 2019 (COVID-19) outbreak and public health emergency, health care providers and other parties subject to the Health Insurance Portability and Accountability Act of 1996 and its implementing statutes and regulations (collectively, HIPAA) are asking how health privacy restrictions apply during this unprecedented pandemic. To address these questions, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued multiple bulletins (OCR Bulletin) to ensure that HIPAA-covered entities and their business associates are aware of the ways that patient information may be shared under the HIPAA Privacy Rule in an outbreak of infectious disease or other emergency situation, and to serve as a reminder that the protections of the Privacy Rule are not set aside during an emergency. Please note, governmental responses to COVID-19 continue to develop so the information outlined below is subject to change.

HIPAA Applies Only to Covered Entities and Business Associates

It is important to note that the HIPAA Privacy Rule only applies to disclosures made by employees, volunteers, and other members of a covered entity's or business associate's workforce. Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more covered health care transactions electronically, such as transmitting health care claims to a health plan. Business associates generally are persons or entities (other than members of the workforce of a covered entity) 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. Business associates also include subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate. The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired). There may be other state or federal rules that apply.

Current HIPAA Waivers

In response to President Donald J. Trump's declaration of a nationwide emergency concerning COVID-19, and Secretary of HHS Alex M. Azar's earlier declaration of a public health emergency on Jan. 31, 2020, effective March 15, 2020, Secretary Azar has exercised the authority to waive sanctions and penalties against a covered *hospital* that does not comply with the following limited provisions of the HIPAA Privacy Rule:

- The requirements 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).

This waiver only applies: (1) in the emergency area; (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. When the Presidential or Secretarial public health emergency declaration terminates, a hospital must then comply with all requirements of the Privacy Rule for any patient still under its care, even if 72 hours have not elapsed since implementation of its disaster protocol. The full bulletin announcing the waiver can be found here.

Enforcement Discretion Notice

OCR also issued an Enforcement Discretion Notice on March 17, 2020, which stated that OCR 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. The OCR indicated its desire to promote the use of audio or video telecommunications to provide telehealth services to patients, even if not related to COVID-19, and intent to exercise its enforcement discretion and not impose penalties for use of telehealth platforms and non-public communication products that may not fully comply with the requirements under HIPAA privacy and security rules (e.g., no Business Associate Agreement). OCR encourages providers to notify patients that these third-party applications potentially introduce privacy risks and instructs providers to enable all available encryption and privacy modes when using such applications. This Notice, along with a more detailed analysis of the use of telehealth in connection with the COVID-19 pandemic, is discussed in another GT Alert.

The initial OCR Bulletin regarding data sharing during the COVID-19 outbreak provides, in pertinent part, the following guidance:

Sharing Patient Information

Treatment. Under the Privacy Rule, covered entities may disclose, without a patient's authorization, protected health information about the patient as necessary to treat the patient or to treat a different patient. Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment.

Public Health Activities. The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information that is necessary to carry out their public health mission. Therefore, the Privacy Rule permits covered entities to disclose needed protected health information without individual authorization:

- ***To a public health authority***, such as the [Centers for Disease Control and Prevention (CDC)] or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. A "public health authority" is an agency or authority of the United States government, a state, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. For example, a covered entity may disclose to the CDC protected health information on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have [COVID-19].
- ***At the direction of a public health authority, to a foreign government agency*** that is acting in collaboration with the public health authority.
- 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.

Disclosures to Family, Friends, and Others Involved in an Individual's Care and for Notification A covered entity may share protected health information with 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. This may include, where necessary to notify family members and others, the police, the press, or the public at large.

- The covered entity should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object, when possible; if the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient's best interests. Note that the requirement to obtain permission has been temporarily waived for covered hospitals as described above.
- For patients who are unconscious or incapacitated: a health care provider may share relevant information about the patient with family, friends, or others involved in the patient's care or payment for care, if the health care provider determines, based on professional judgment, that doing so is in the best interests of the patient. For example, a provider may determine that it is in the best interests of an

elderly patient to share relevant information with the patient's adult child, but generally could not share unrelated information about the patient's medical history without permission.

- In addition, a covered entity may share protected health information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, for the purpose of coordinating the notification of family members or other persons involved in the patient's care, of the patient's location, general condition, or death. It is unnecessary to obtain a patient's permission to share the information in this situation if doing so would interfere with the organization's ability to respond to the emergency.

Disclosures to Prevent a Serious and Imminent Threat. Health care providers may share patient information with 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. Thus, providers may disclose a patient's health information to anyone who is in a position to prevent or lessen the serious and imminent threat, including family, friends, caregivers, and law enforcement without a patient's permission. HIPAA expressly defers to the professional judgment of health professionals in making determinations about the nature and severity of the threat to health and safety.

Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification. In general, except in the limited circumstances described elsewhere in th[e] Bulletin, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, may not be done without the patient's written authorization (or the written authorization of a personal representative who is a person legally authorized to make health care decisions for the patient). Where a patient has not objected to or restricted the release of protected health information, a covered hospital or other health care facility may, upon a request to disclose information about a particular patient asked for by name, release limited facility directory information to acknowledge an individual is a patient at the facility, and may provide basic information about the patient's condition in general terms (e.g., critical or stable, deceased, or treated and released). Covered entities may also disclose information when the patient is incapacitated, if the disclosure is believed to be in the best interest of the patient and is consistent with any prior expressed preferences of the patient.

Minimum Necessary. For most disclosures, a covered entity must make reasonable efforts to limit the information disclosed to that which is the "minimum necessary" to accomplish the purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.) Covered entities may rely on representations from a public health authority or other public official that the requested information is the minimum necessary for the purpose, when that reliance is reasonable under the circumstances. For example, a covered entity may rely on representations from the CDC that the protected health information requested by the CDC about all patients exposed to or suspected or confirmed to have [COVID-19] is the minimum necessary for the public health purpose. In addition, internally, covered entities should continue to apply their role-based access policies to limit access to protected health information to only those workforce members who need it to carry out their duties.

Safeguarding Patient Information

In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information.

Uncharted Territory of COVID-19

Since HIPAA was enacted in 1996, the United States has not faced a disease outbreak of COVID-19's caliber. Accordingly, OCR and covered entities have never truly needed broad-sweeping waivers or public health pronouncements regarding health information privacy like those being contemplated during this pandemic. For now, the HIPAA Privacy and Security Rules still apply to most covered entities as usual, with the exception of a limited waiver applicable to covered hospitals and the relaxation of enforcement standards in connection with the good faith use of telehealth.

42 CFR Part 2 Providers

While the HHS Substance Abuse and Mental Health Services Administration (SAMHSA) has recently issued recommendations for Part 2 programs seeking guidance on clinical containment during the COVID-19 emergency, SAMHSA has not waived any requirements related to sharing Part 2 information. Absent certain limited exceptions, 42 CFR Part 2 generally requires written patient consent to disclose Part 2 information for treatment, payment, or health care operations purposes. These regulations set forth the consent requirements under Part 2 regulations, and mandate that the consent be in writing, whether paper or electronic. They also require the consent to be signed by the patient and, when required for a patient who is a minor, the consent must include the signature of an individual authorized to give consent. Electronic signatures are permitted under Part 2 to the extent not prohibited by applicable state law. However, there is an exception to the written patient consent requirement for medical emergencies. That exception provides that Part 2 patient information may be disclosed *to medical personnel* to the extent *necessary to meet a bona fide medical emergency* in which the patient's prior informed consent cannot be obtained. Although these key terms are undefined by the Part 2 regulations, there are specific procedures related to this exception, which require the Part 2 program to immediately document, in writing, the disclosure in the patient's record, including:

1. the name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;
2. the name of the individual making the disclosure;
3. the date and time of the disclosure; and
4. the nature of the emergency (or error, if the report was to FDA pursuant to 2.31(b).

For more information and updates on the developing situation, visit GT's Health Emergency Preparedness Task Force: Coronavirus Disease 2019.

Authors

This GT Alert was prepared by:

- Julie A. Sullivan | +1 303.685.7412 | sullivanjul@gtlaw.com
- Renae M. Nanna | +1 303.572.6575 | nannar@gtlaw.com
- Loreli Wright | +1 303.685.7417 | wrightl@gtlaw.com