GBS Compliance

HIPAA Privacy Rule and the Coronavirus Outbreak

The U.S. Department of Health and Human Services (HHS) issued a bulletin to remind covered entities and their business associates that the HIPAA Privacy Rule's protections still apply during a public health emergency, such as the current coronavirus (COVID-19) outbreak. The bulletin also outlines the different ways that patient information may be shared under the Privacy Rule during an outbreak of infectious disease or another emergency situation.

The Privacy Rule only applies to covered entities and their business associates, and not to employers. Covered entities include health plans, most health care providers and health care clearinghouses. In general, **medical information that is provided to an employer directly by an employee is not subject to the Privacy Rule,** although other federal and state privacy restrictions may apply, including the Americans with Disabilities Act (ADA). However, any medical information that employers receive from their health plans is subject to the Privacy Rule and generally cannot be used for employment purposes.

In addition, HHS announced that it will not impose penalties for HIPAA noncompliance against health care providers that serve patients through everyday communication technologies (such as FaceTime or Skype) during the COVID-19 nationwide public health emergency.

This Compliance Bulletin contains HHS's bulletin regarding HIPAA compliance during the COVID-19 outbreak.

Action Steps

Covered entities and their business associates should review HHS' guidance regarding the protection of health information during an outbreak of infectious disease.

HIPAA Privacy Rule

- The HIPAA Privacy Rule applies to covered entities and their business associates.
- The Privacy Rule sets limits on when an individual's protected health information (PHI) can be used or disclosed without his or her written authorization.
- HHS issued a bulletin to summarize how PHI may be shared under the Privacy Rule during an outbreak of infectious disease.

Impact on Employers

- Employers are not directly subject to the Privacy Rule.
- In general, medical information that employees provide to their employers is not subject to the Privacy Rule.
- This information may be subject to other privacy restrictions, such as the ADA.

Copyright © 2020 GBS Benefits, Inc.

Sharing Patient Information

Treatment

Under the Privacy Rule, covered entities may disclose, without a patient's authorization, protected health information (PHI) 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. See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of "treatment" at 164.501.

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 PHI that is necessary to carry out their public health mission. Therefore, the Privacy Rule permits covered entities to disclose needed PHI without individual authorization:

- **To a public health authority**, such as the 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 U.S. 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. See 45 CFR §§ 164.501 and 164.512(b)(1)(i). For example, a covered entity may disclose PHI to the CDC 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. 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 Family, Friends, and Others Involved in an Individual's Care and for Notification

A covered entity may share PHI 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. See 45 CFR 164.510(b).

- 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 interest.
- 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.

Copyright © 2020 GBS Benefits, Inc.

- In addition, a covered entity may share PHI 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. See 45 CFR 164.512(j). Thus, providers may disclose a patient's health information to anyone who is in a position to prevent or lesson 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. See 45 CFR 164.512(j).

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 this 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). See 45 CFR 164.508 for the requirements for a HIPAA authorization. Where a patient has not objected to or restricted the release of PHI, 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. See 45 CFR 164.510(a).

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 PHI 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 PHI to only those workforce members who need it to carry out their duties. See 45 CFR §§ 164.502(b), 164.514(d).

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 PHI.

Copyright © 2020 GBS Benefits, Inc.

HIPAA Applies Only to Covered Entities and Business Associates

The HIPAA Privacy Rule 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 PHI. Business associates also include subcontractors that create, receive, maintain or transmit PHI 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.

A business associate of a covered entity (including a business associate that is a subcontractor) may make disclosures permitted by the Privacy Rule, such as to a public health authority, on behalf of a covered entity or another business associate to the extent authorized by its business associate agreement.

Other Resources

- For more information on HIPAA and Public Health, please visit: https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html
- For more information on HIPAA and Emergency Preparedness, Planning, and Response, please visit: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergencypreparedness/index.html
- General information on understanding the HIPAA Privacy Rule may be found at: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- For information regarding how Federal civil rights laws apply in an emergency, please visit: https://www.hhs.gov/civil-rights/for-individuals/special-topics/emergencypreparedness/index.html

March 27, 2020

This information is provided as educational material only and is not intended as legal, financial or tax advice. Consult your legal counsel for complete details on your compliance requirements for your plan(s).

GBS
A Leavitt Group Company

Copyright © 2020 GBS Benefits, Inc.