November 2014
U.S. Department of Health and Human Services, Office for Civil Rights
BULLETIN: HIPAA Privacy in Emergency Situations

In light of the Ebola outbreak and other events, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), is providing this bulletin to ensure that HIPAA covered entities and their business associates are aware of the ways in which patient information may be shared under the HIPAA Privacy Rule in an emergency situation, and to serve as a reminder that the protections of the Privacy Rule are not set aside during an emergency.

The HIPAA Privacy Rule protects the privacy of patients' health information (protected health information) but is balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary to treat a patient, to protect the nation's public health, and for other critical purposes.

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. 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 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. See 45 CFR §§ 164.501 and 164.512(b)(1)(i). 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 Ebola virus disease.
- ***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 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. 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.
- 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.

Imminent Danger 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).

Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification Upon request for information about a particular patient by name, a hospital or other health care facility may release limited facility directory information to acknowledge an individual is a patient at the facility and provide basic information about the patient's condition in general terms (e.g., critical or stable, deceased, or treated and released) if the patient has not objected to or restricted the release of such information or, if 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). 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.

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. 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 Ebola virus disease is the minimum

necessary for the public health purpose. 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. See 45 CFR §§ 164.502(b), 164.514(d).

Business Associates 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.

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.

Other Information

Limited Waiver The HIPAA Privacy Rule is not suspended during a public health or other emergency; however, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act. If the President declares an emergency or disaster and the Secretary declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with the following 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).

If the Secretary issues such a waiver, it only applies: (1) in the emergency area and for the emergency period 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. When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours has not elapsed since implementation of its disaster protocol.

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 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.

Other Resources

For more information on HIPAA and Public Health, please visit:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html

For more information on HIPAA and Emergency Preparedness and Response, please visit:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/index.html

General information on understanding the HIPAA Privacy Rule may be found at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html