HIPAA and Disasters: What Emergency Professionals Need to Know

Updated September 11, 2017

Disasters and emergencies can strike at anytime with little or no warning and the local healthcare system in the midst of an emergency response can be rapidly inundated with patients, worried family and friends looking for their loved ones, and media organizations requesting patient information. Knowing what information can be released, to whom, and under what circumstances, is critical for healthcare facilities in disaster response. This guide is designed to answer frequently asked questions regarding the release of information about patients following an incident.

NOTE: This guide does NOT replace the advice of your facility Privacy Officer and/or legal counsel who should be involved in planning for information release prior to an event, developing policy before a disaster that guides staff actions during a disaster, and during an emergency when contemplating disclosures.

This guide does address what information can be disclosed and under what circumstances. Covered entities can disclose needed patients' protected health information (PHI) without individual authorization:

- If necessary to treat the patient or a different patient or if the information would help treat a different patient
- To a public health authority, as outlined below
- At the direction of a public health authority, to a foreign agency acting in collaboration with the public health authority
- To persons at risk of contracting or spreading a disease or condition (if authorized by other law)
- With certain people involved with patient's care/ responsible for the patient
- When there is imminent threat to public health/ safety

Covered entities:

- Health plans
- Healthcare clearinghouses
- Healthcare providers (e.g. hospitals, clinics, pharmacies, nursing homes) who conduct one or more covered healthcare transactions electronically.

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 PHI.
- Subcontractors that create, receive, maintain, or transmit PHI on behalf of another business associate.

What is HIPAA and the Privacy Rule?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing regulations, the HIPAA Privacy, Security, and Breach Notification Rules, protect the privacy and security of patients' PHI, but is balanced to ensure that

appropriate uses and disclosures of the information may still be made when necessary to treat a patient, to protect the nation's public health, and for other critical purposes.

Does HIPAA Apply to Me or My Organization?

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, healthcare clearinghouses, and those healthcare providers that conduct one or more covered healthcare transactions electronically, such as transmitting healthcare claims to a health plan.

Business associates generally include 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.

HIPAA does not apply to disclosures made by those 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).

When Can PHI Be Shared?

Patient health information, or PHI, can be shared under the following circumstances:

Treatment. Under the HIPAA Privacy Rule, covered entities may disclose, without a patient's authorization, PHI about the individual as necessary to treat the patient or to treat a different patient. Treatment includes the coordination or management of healthcare and related services by one or more healthcare providers and others, consultation between providers, providing follow-up information to an initial provider, 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 PHI that is necessary to carry out their public health mission. Therefore, the HIPAA Privacy Rule permits covered entities to disclose needed PHI without individual authorization:

- **To a public health authority** that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, or to a person or entity acting under a grant of authority from or under contract with such public health agency,. This could 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.
- **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 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 may also 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—if 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 interest.
- In addition, a covered entity may share PHI with disaster relief organizations such as the American Red Cross, which 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.

Covered entities can disclose needed PHI without individual authorization:

- If necessary to treat the patient or a different patient
- To a public health authority authorized by law to collect or receive such information
- At the direction of a public health authority, to a foreign agency acting in collaboration with the public health authority
- To persons at risk of contracting or spreading a disease or condition (if authorized by other law)
- With certain people involved with patient's care/ responsible for the patient for reunification or when in the patient's best interest
- When there is imminent threat to public health/ safety

Imminent Danger. Healthcare 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.

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 healthcare

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. Reference 45 CFR 164.510(a). In general, except in the limited circumstances described elsewhere, affirmative reporting 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 legally authorized to make healthcare decisions for the patient).

General or aggregate information in mass casualty events that does not identify an individual or meets the requirements of the HIPAA Privacy Rule's de-identification provisions is *not* considered PHI (e.g., X number of casualties were received by the hospital with the following types of injuries).

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.

Note: The disclosures listed above are at the discretion of the covered entity and are not required disclosures under the Rule. Some of these disclosures may be required by other federal, state or local laws (for example, mandatory reporting of positive infectious disease test results).

Does the HIPAA Privacy Rule Permit Disclosure to Public Officials Responding to a Bioterrorism Threat or other Public Health Emergency?

Yes. The HIPAA Privacy Rule recognizes that various agencies and public officials will need PHI to deal effectively with a bioterrorism threat or emergency. The public health threat does not have to reach a declared emergency status. If information is needed by a government agency to protect the health of the public (e.g., a food-borne outbreak), the agency may request and receive appropriate clinical and other information about the patient's disease, care, and response to treatment. To facilitate the communications that are essential to a quick and effective response to such events, the HIPAA Privacy Rule permits covered entities to disclose needed information to public officials in a variety of ways. Further, if the covered entity has obligations to report test results and other information to public health agencies by statute, rule, or ordinance, the HIPAA Privacy Rule generally permits these disclosures.

Covered entities may disclose PHI, without the individual's authorization, to a public health authority acting as authorized by law in response to a bioterrorism threat or public health emergency (reference 45 CFR 164.512(b)), public health activities). The HIPAA Privacy Rule also permits a covered entity to disclose PHI to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism (reference 45 CFR 164.512(j)), to avert a serious threat to health or safety). In addition, disclosure of PHI, without the individual's authorization, is permitted where the circumstances of the emergency implicates law enforcement activities (reference 45 CFR 164.512(f)); national security and intelligence activities (reference 45 CFR 164.512(k)(2)); or judicial and administrative proceedings (reference 45 CFR 164.512(e)).

Is the HIPAA Privacy Rule "Waived" or "Suspended" During an Emergency?

The HIPAA Privacy Rule is not suspended during a public health or other emergency; however, under certain conditions the Secretary of the U.S. Department of Health and Human Services may waive certain provisions of the HIPAA Privacy Rule section 1135(b)(7) of the Social Security Act, if such a waiver is deemed necessary for the particular incident when the Secretary declares a public health emergency and the President declares an emergency or disaster under the Stafford Act or National Emergencies Act. For more information, access "Is the HIPAA Privacy Rule suspended during a national or public health emergency?" Access Hurricane Irma and HIPPA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Declared Emergency for an example of how sanctions and penalties could be waived in a declared emergency.

Does the HIPAA Privacy Rule Permit Disclosure to Law Enforcement?

A HIPAA-covered entity may disclose PHI to law enforcement with the individual's signed HIPAA authorization. A covered entity may disclose directory information as mentioned above to law enforcement upon request. Further disclosures to law enforcement for purposes of re-unification and family notification are permitted as discussed above.

A HIPAA-covered entity also may disclose PHI to law enforcement without the individual's signed HIPAA authorization in certain incidents, including:

- To report to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.
- To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the premises of the covered entity.
- To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.
- When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity.
- To report PHI to law enforcement when required by law to do so (such as reporting gunshots or stab wounds).
- To comply with a court order or court-ordered warrant, a subpoena or summons issued

by a judicial officer, or an administrative request from a law enforcement official (the administrative request must include a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used).

- To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person, but the information disclosed must be limited to certain basic demographic and health information about the person.
- To respond to a request for PHI about an adult victim of a crime when the victim agrees (or in limited circumstances if the individual is unable to agree). Child abuse or neglect may be reported, without a parent's agreement, to any law enforcement official authorized by law to receive such reports.

How Does the HIPAA Privacy Rule Apply to Disclosures Involving Foreign Nationals?

Covered entities may disclose PHI for all persons, regardless of nationality, according to the disclosures listed in the Privacy Rule and discussed above. Disclosure of PHI to embassies, consulates or other third parties, such as the American or International Red Cross acting in a capacity to facilitate notifications or repatriation following an emergency, is permitted under the existing disclosures of the HIPAA Privacy Rule, as referenced above.

For More information

- Bulletin: HIPAA Privacy in Emergency Situations
- Can healthcare information be shared in a severe disaster?
- Health Information Privacy – Is HIPAA Privacy Rule Suspended during a National or Public Health Emergency?
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement
- HIPAA Privacy Rule: Disclosures for Emergency Preparedness – A Decision Tool
- Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations
- Incorporating Active Shooter Incident Planning into Health Care Facility Emergency Operations Plans. Appendix A: Information Sharing. (Page 29 of 33)
- When does the Privacy Rule allow covered entities to disclose PHI to law enforcement officials?
- HIPAA Policy Brief

For more information on HIPAA and Public Health:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html
For more information on HIPAA and Emergency Preparedness and Response:
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