Frequently Asked Questions

Use of health care information during disaster or emergency

(July 2018)

Question 1: Can health care information be shared in a severe disaster?

Answer:

Providers and health plans covered by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule can share patient information in all of the following ways:

TREATMENT: Health care providers can share patient information as necessary to provide treatment.

Treatment includes:

- sharing information with other providers (including hospitals and clinics),
- referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
- coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).

Providers can also share patient information to the extent necessary to seek payment for these health care services.

NOTIFICATION: Health care providers can share patient information as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.

The health care provider should get verbal permission from individuals, when possible; but if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgement, doing so is in the patient's best interest.

- Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify, or otherwise notify family members and others as to the location and general condition of their loved ones.
- In addition, when a health care provider is sharing 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, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.

IMMINENT DANGER: Providers can 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 and the provider's standards of ethical conduct.

FACILITY DIRECTORY: Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.

Of course, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information.

Question 2: Is the HIPAA Privacy Rule suspended during a national or public health emergency?

Answer:

No; however, the Secretary of U. S. Department of Health and Human Services (HHS) may waive certain provisions of the Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

What provisions may be waived?

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 certain 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 (45 CFR § 164.510(b))
- the requirement to honor a request to opt out of the facility directory (45 CFR § 164.510(a))
- the requirement to distribute a notice of privacy practices (45 CFR § 164.520)
- the patient's right to request privacy restrictions (45 CFR § 164.522(a))
- the patient's right to request confidential communications (45 CFR § 164.522(b))

When and to what entities does the waiver apply?

If the Secretary issues such a waiver, it only applies:

- In the emergency area and for the emergency period identified in the public health emergency declaration.
- To hospitals that have instituted a disaster protocol. The waiver would apply to all patients at such hospitals.
- 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.

Regardless of the activation of an emergency waiver, the HIPAA Privacy Rule permits disclosures for treatment purposes and certain disclosures to disaster relief organizations. For instance, the Privacy Rule allows covered entities to share patient information with the American Red Cross so it can notify family members of the patient's location. See 45 CFR 164.510(b)(4).

The U. S. Department of Health and Human Services (HHS) provides additional information regarding whether provisions of HIPAA may be "suspended" during a severe disaster on the HHS website (https://www.hhs.gov/hipaa/for-professionals/faq/1068/is-hipaa-suspended-during-a-national-or-public-health-emergency/index.html).

Question 3: Does Part 2 permit a healthcare provider to disclose information without consent when there is an immediate threat to the health or safety of an individual or the public?

Answer:

Part 2 permits the disclosure of information under certain circumstances without consent during a medical emergency or in other limited situations. If a Part 2 program (or a healthcare provider that has received Part 2 patient information) believes that there is an immediate threat to the health or safety of any individual, there are steps described below that the Part 2 program or healthcare provider can take in such a situation:

Notifications to medical personnel in a medical emergency:

A Part 2 program can make disclosures to medical personnel if there is a determination that a medical emergency exists, i.e., there is a situation that poses an immediate threat to the health of any individual and requires immediate medical intervention (42 CFR § 2.51(a)). Information disclosed to the medical personnel who are treating such a medical emergency may be re-disclosed by such personnel for treatment purposes as needed.

Notifications to law enforcement:

Law enforcement agencies can be notified if an immediate threat to the health or safety of an individual exists due to a crime on program premises or against program personnel. A Part 2 program is permitted to report the crime or attempted crime to a law enforcement agency or to seek its assistance (42 CFR § 2.12(c)(5)). Part 2 permits a program to disclose information regarding the circumstances of such incident, including the suspect's name, address, last known whereabouts, and status as a patient in the program.

Immediate threats to health or safety that do not involve medical emergencies or crimes on programs premises or against program personnel:

Part 2 programs and health care providers and Health Information Organizations (HIOs) who have received Part 2 patient information, can make reports to law enforcement about an immediate threat to the health or safety of an individual or the public if patient-identifying information is not disclosed. Immediate threats to health or safety that do not involve a medical emergency or crimes (e.g., a fire) are not addressed in the regulations. Programs should evaluate those circumstances individually.

Reports of child abuse and neglect:

The restrictions on disclosure do not apply to the reporting under State law of incidents of suspected child abuse and neglect to the appropriate State or local authorities. However, Part 2 restrictions continue to apply to the original alcohol or drug abuse patient records maintained by the program including their disclosure and use for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect (42 CFR § 2.12(c)(6)). Also, a court order under Part 2 may authorize disclosure of confidential communications made by a patient to a program in the course of diagnosis, treatment, or referral for treatment if, among other reasons, the disclosure is necessary to protect against an existing threat of life or of serious bodily injury, including circumstances which constitute suspected child abuse and neglect (42 CFR § 2.63(a)(1)).

Court ordered disclosures:

Under the regulations, Part 2 programs or "any person having a legally recognized interest in the disclosure which is sought" may apply to a court for an order authorizing disclosure of protected patient information (42 CFR § 2.64). Thus, if there is an existing threat to life or serious bodily injury, a Part 2 program or "any person having a legally recognized interest in the disclosure which is sought" can apply for a court order to disclose information.

Substance Abuse and Mental Health Services Administration (SAMSHA) provides additional clarity on this topic on the SAMSHA website (https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs).