Long-Term Care Survey Alert

HIPAA Compliance: Don't Let Emergencies Become a HIPAA Breach Disaster

Least possible information is the gold standard.

Remember your obligations to public health reporting don't override your patients' privacy rights. If you have been wondering how much is too much or just enough, you can look to the **HHS Office for Civil Rights** (OCR) for direction.

OCR recently released a directive on HIPAA compliance in emergency and public health situations in the backdrop of the recent Ebola outbreak. The guidance explains the ways in which covered entities (CEs) may share protected health information (PHI) under the HIPAA Privacy Rule in emergency situations.

Know Your State's Requirements

"Federal laws and regulations permit, and many state laws require, the disclosure of patient information without a patient's consent or authorization for certain public health activities," pointed out partner attorney **Laurie Cohen** in an Oct. 29 blog posting for the law firm **Nixon Peabody LLP.**

According to the OCR guidance, the HIPAA Privacy Rule allows CEs to disclose necessary PHI 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 authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability.
- 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 CE 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.

Stick to the 'Minimum Necessary'

But when you're disclosing PHI to a public health authority, keep in mind that the disclosure is subject to HIPAA's "minimum necessary" standard, Cohen reminded. The standard provides that the CE will limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

According to HIPAA, when making disclosure to public health officials, a CE "may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary ... if the public official represents that the information requested is the minimum necessary."

Example: A CE 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 Ebola is the minimum necessary for the public health purpose, OCR says.

Remember: Also, don't forget to include the disclosure in the accounting of disclosures of patients' PHI this HIPAA requirement includes disclosures for public health purposes, Cohen stated.

Public Health Reports: Safeguard Patients' Privacy Rights

Although HIPAA permits disclosures of PHI without patient authorization for public health activities, you "cannot disregard a patient's right to privacy in those cases where a patient's information has been the subject of a public health report," Cohen warned.

"Put another way, the public disclosure of a patient's information, including the identity of a patient, by a covered entity is not permissible even in cases where a public health report has been made and a public health official subsequently releases information about the patient as part of its public health surveillance, investigation or intervention," Cohen explained. If you were to release a patient's information, you would need to have a valid authorization signed by the patient or the patient's authorized representative.

Consider Other Disclosures & Imminent Danger

The HIPAA Privacy Rule also allows you to "share patient information with anyone necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public," OCR notes. But even in "imminent danger" situations, you must still comply with applicable laws, such as state statutes, regulations or case law, and your own standards of ethical conduct.

When it comes to sharing a patient's PHI with family members, friends and others involved in the individual's care, you should try to get verbal permission or otherwise reasonably infer that the patient does not object, when possible in an emergency situation, OCR instructs. If the patient is incapacitated or not available, you can share PHI if your professional judgment is that doing so is in the patient's best interest.

What's more: You can also share PHI with disaster relief organizations like the **American Red Cross** for the purpose of coordinating notification of family member or other individuals involved in the patient's care, of the patient's location, general condition or death, OCR notes. "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."

Understand the 'Limited Waiver'

Finally, the HHS Secretary may provide a "limited waiver" of certain HIPAA Privacy Rule provisions under the Project Bioshield Act of 2004 and Section 1135(b)(7) of the Social Security Act. This waiver can occur when the U.S. President declares an emergency or disaster and the HHS Secretary declares a public health emergency.

In this case, the HHS Secretary may waive sanctions and penalties against a covered hospital that doesn't comply with the following Privacy Rule provisions:

- The requirement to obtain a patient's agreement to speak with family members or friends involved in the patient's care.
- The requirement to honor a request to opt out of the facility directory.
- The requirement to distribute a Notice of Privacy Practices (NPP).
- The patient's right to request privacy restrictions.
- The patient's right to request confidential communications.

Caveats: According to OCR, if the Secretary issues this waiver, it applies only:

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, or until the Presidential or Secretarial declaration terminates (even if 72 hours has not elapsed).

Bottom line: Despite certain special allowances in emergency situations and public health considerations, you should never think that you can set aside HIPAA Privacy Rule protections during an emergency.

Resources: To read the OCR guidance, go to

www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/hipaa-privacy-emergency-situations.pdf. For more information on HIPAA in emergency situations, visit www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/index.html.