HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

MAY 2018

Ensuring that rules and regulations are met

an interview with
Lynda S. Hilliard

by Terrie B. Estes, MHSA, MS, CHC, CHPC; Peter A. Khoury, MHA, MJ, CHC, CHPC; and Kaitlin McCarthy, CHC

Maintaining patient privacy during an emergency

» Emergency events can create risks to patient privacy.
» Various federal and state regulations outline privacy groundwork.
» Recent events have brought about important HIPAA clarification.
» Penalties continue to increase; assess preparedness now.
» Prepare and respond to emergencies by deploying a response plan.

Terrie B. Estes *(terrie.estes@YNHH.ORG) is Vice President, Corporate Compliance & Chief Compliance Officer, Yale New Haven Health, in New Haven, CT.* ***Peter A. Khoury*** *(pkhoury@deloitte.com) is a Deloitte Risk and Financial Advisory Senior Consultant in Deloitte & Touche LLP's Philadelphia office.* ***Kaitlin McCarthy*** *(kaimccarthy@deloitte.com) is a Deloitte Risk and Financial Advisory Senior Manager in Deloitte & Touche LLP's Boston office.*

In healthcare, every day brings about new emergencies, and compliance professionals are often tasked with assisting their organizations to navigate through them. To patients and their families, every emergency is significant and requires discretion and privacy of patient health information. A visit to a hospital often evokes fear and anxiety, not only for the patient, but also for their families and loved ones. Each type of emergency may require a different level of use and/or disclosure of protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), with the potential of requiring disclosure to government, public health, relief, or other entities. Some events may even bring about immense, and sometimes challenging interest from media outlets.

To prepare and respond efficiently to these situations, compliance professionals should:

- understand the governing rules and regulations associated with using and disclosing patient information;
- evaluate the need to create policies, procedures, and trainings that outline how to handle patient information; and
- plan and develop different scenarios with colleagues.

Recent events have also brought about clarification and reinforcement from Health and Human Services (HHS) to commonly accepted practices for disclosing patient information during emergency situations. Many emergencies are different in one element of the incident or another, and how one may respond can depend on various facts and circumstances. Establishing a management response plan with defined roles and a designated team may facilitate a faster and more coordinated proactive response.


Estes


Khoury


McCarthy

HIPAA Privacy Rule and recent guidance

HIPAA required the Secretary of Health and Human Services to create privacy regulations if Congress did not pass its own.[1]

In 2000, HHS published the final Privacy Rule, and in 2002 modifications were made.[2] Generally, the Privacy Rule creates standards for protecting health information, requires safeguards to protect this information, and establishes conditions for how and when this information can be used and disclosed by a covered entity. The Privacy Rule also restricts the information that healthcare organizations can release through facility directories and to the public, including news outlets, without written authorization.

The Privacy Rule outlines only two scenarios where a covered entity must disclose PHI: (1) when the individual, or their legal representative, requests access to or an accounting of disclosures of their PHI; and (2) to HHS as part of an investigation or enforcement matter.[3] Outside of these two scenarios, there are other situations where the use and disclosure of PHI may be permitted without the individual's authorization.[4] The scenarios frequently encountered by compliance professionals are:

- for treatment, payment, and operations purposes;
- to provide the individual or their representative the opportunity to agree or object;
- incident to an otherwise permitted use and disclosure;
- public Interest and Benefit Activities (within exceptions and conditions); and
- limited Data Set for purposes of research, public health, or healthcare.

The Privacy Rule also sets out various controls related to the Notice of Privacy Practices and content requirements for a notice, electronic notices, and a right to access information.[5]

Most recently, in response to Hurricane Harvey, the HHS Office for Civil Rights (OCR) published a bulletin that outlined HIPAA Privacy and disclosures in an emergency situation.[6] This bulletin provided information regarding the waiving of certain penalties for select provisions of the Privacy Rule to hospitals that had instituted a disaster protocol and reinforced permissible uses and disclosures of information without a waiver under the HIPAA Privacy Rule. This is not the first time HHS has provided guidance on the Privacy Rule related to an emergency situation. In 2005, after Hurricane Katrina, HHS published compliance guidance in a bulletin on HIPAA Privacy and disclosures in emergency situations, and in 2014, in the wake of the Ebola outbreak, HHS issued additional guidance.[7,8] Further, HHS has created a decision tool to assist compliance professionals when working through disclosure decisions in emergency situations.

In addition, in response to confusion after the Orlando Pulse nightclub incident, the OCR provided clarification for covered entities, describing when covered entities are permitted to share patient health status information, treatment, or payment arrangements with a person who is not married to the patient or is otherwise not a relative under applicable law. In January 2017, HHS clarified that the location, general condition, or death of a patient may be shared with a patient's family member, relative, guardian, caregiver, friend, spouse, or partner.[9]

Penalties for non-compliance and privacy violations are increasing, and with the passage of the Federal Civil Penalties Inflation Adjustment Act of 2015, they will likely continue to increase in line with inflation annually.[10,11] However, if the President declares

an emergency and a public health emergency is declared by the Secretary of HHS, sanctions for non-compliance with the Privacy Rule may be waived for a defined time period so as not to interfere with emergency responses to the incident.

Interacting with the media

Emergency situations can bring about a frenzy of activity inside and outside of a hospital. Media outlets may become interested in reporting on the developing story, and—in some cases—organizations may decide to hold news conferences to update the media and the public on the situation. In today's digital age, online social media creates an additional layer of risk. At times, media outlets will use official and unofficial communication channels and contacts, including hospital staff, to obtain the latest updates in hopes of reporting the information first. This sometimes can undermine and jeopardize the privacy and security of patient information. Inappropriate access, use, and disclosure should not be tolerated and should be met with consequences in line with established organizational policies. Hospitals can take a few important steps to prepare for emergency situations that may require interaction with media outlets.

Understand the rules and educate staff

At all times, a patient's right to privacy surpasses the media's desire for information. Patients have a right to opt out of providing information that can be used for public release, and patients may choose not to authorize their information being disclosed or publically displayed in public records such as a patient directory. If a patient's written authorization has not been obtained or a patient is not able to provide written authorization due to their condition, hospitals should take caution and seek experienced advice before providing information about a patient. In disaster situations, implementation of a defined protocol may provide clear procedures on how to handle patient health information.

Specific policies and procedures should be reviewed at staff meetings of specific departments, including the Emergency department, as part of the organization's policy review process. In addition to policies and procedures, developing other easy-access resources (e.g., an Emergency Department Patient Privacy Frequently Asked Questions brochure that cites various tools and resources from the OCR and contact information for the compliance team) can assist staff in the event of an emergency.

Follow the established response plan

Creating, accepting, and disseminating an emergency response plan that details the roles and responsibilities of specific clinical and administrative teams and establishes protocols and company policies for interacting with the media are helpful proactive steps that can be taken to reduce the risk of PHI becoming compromised. Reminding staff, as part of their annual compliance training, of the organization's commitment to the confidentiality and security of patient information is an important reinforcement message. So is providing staff with a contact person or department to refer media and other inquiries from those who do not have a legitimate need to know. This can be a risk-mitigating step in bringing awareness to staff not directly involved in the emergency response plan. The physical security of the hospital should also be considered during these events, and staff should be appropriately credentialed with name badges for identification purposes.

Establish a spokesperson to communicate with the public

Assigning a spokesperson who is tasked with serving as the liaison to the media

during emergency situations can help channel inquires and requests for information. The spokesperson should be an individual who has received media training, has established relationships with media outlets, and has adequate access to executives and clinical staff so that they are able to obtain accurate information. Many times the spokesperson will be a member of the public relations, marketing, or governmental affairs staff. This individual is responsible for keeping the response team and specific leadership regularly updated about media activity and responses. This individual should work closely with the chief compliance officer and have a strong understanding of privacy rules and requirements in order to safeguard patient information and protect against providing identifiers that can be linked to a specific patient.

Control the message and correct the record

The hospital should provide factual information about the situation, as permitted, without compromising a patient's right to privacy. Organizations are not obligated to respond to media inquiries. They may choose to intake questions and distribute individual responses, or hold larger briefings where questions may or may not be entertained. The spokesperson serves an important role to not only provide updates, as permitted, but also to correct the record with respect to inaccurately reported information. With the advent of social media, instant access to news and the instantaneous ability of anyone in the public to post about an event, whether correct or incorrect, pose additional challenges. The spokesperson should serve as the main contact for inquiries related to the event and the patients being treated. This, at times, may require coordination with law enforcement officials.

The hospital should provide factual information about the situation, as permitted, without compromising a patient's right to privacy.

Remind leadership and staff of company policies and enforce them

At the outset of an emergency situation, remind staff of established protocols and company policies related to maintaining patient privacy and where to direct questions regarding patients being treated from those without a need to know. Many hospitals run drills for events like these with their staff. Enforcing these policies demonstrates a strong commitment to maintaining trust between the hospital and the public, while also setting an example for other employees that breaches of patient information will not be tolerated and will be handled in accordance with established company policies and procedures.

Disaster situations

Disaster situations can be particularly chaotic. Situations may arise where patient consent cannot be obtained. As has been reinforced through multiple HHS publications, when a patient is incapacitated, it is up to the covered entity to determine if sharing this information would be in the patient's interest. This is important guidance that is intended to empower hospitals to provide critical health information for treatment purposes, notify loved ones of a patient's general condition or death, inform anyone necessary to prevent or lessen a serious threat to a person or the public, or to include patient information in a facility directory.

It is also permissible, when circumstances dictate, to disclose the minimum necessary PHI for care and notification purposes to

disaster relief agencies, such as the American Red Cross, when authorized by law.

Hospitals should establish and activate an incident response team so that all personnel who need to be aware and involved are included once the incident response plan has been activated.

The OCR has released guidance and tools about the HIPAA Privacy Rule's application during emergency situations. With that said, patient identifiers that are released should be done carefully so as to not be linked to a specific patient. Hospitals may tell the media the number of patients brought to the facility by gender or age group and the general cause of their treatment needs. The same rules under HIPAA apply in these disaster situations. Patients must provide authorization for their information to be used and disclosed, unless an exception is met, or a patient is unable to do so because of their condition, or if doing so would interfere with an organization's ability to respond to the emergency, in which case, the hospital must obtain a patient's authorization as soon as practicable.

Learn and adjust

At the conclusion of a situation where an emergency response plan has been deployed, the team should debrief and gather intelligence from the incident. The team should revisit their plans and adjust them as needed. This may include holding an in-service for response team members to walk through the scenario and outline barriers that were encountered and opportunities to overcome those barriers in future situations to improve the efficiency of the response.

Final thoughts

With careful preparation, hospitals can respond with confidence during emergency events. Central to this response is the role of the compliance professional prior to, during, and after an emergency incident. Frequent messaging to hospital staff (based on roles and responsibilities) about privacy policies and procedures, as well as proper response scenarios detailing what to do if contacted by the media, may assist in reinforcing the organization's commitment to protecting patient information. This messaging can also be coupled at the conclusion of an event where gaps or areas of improvement have been identified. Various federal and state laws and regulations set the ground rules for privacy compliance, and a close assessment of those requirements and protections should be undertaken when creating a response plan.

1 Public Law 104-191 (Health Insurance Portability and Accountability Act)
2. 67 FR 53182 (Standards for Privacy of Individually Identifiable Health Information)
3. 45 C.F.R. § 164.502(a)(2) (Uses and disclosures of protected health information)
4. 45 C.F.R. § 164 (Security and Privacy)
5. 45 C.F.R. §§ 164.520, 164.524 (Notice of Privacy Practices)
6. U.S. Department of Health and Human Services, Hurricane Harvey Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Declared Emergency. Available at http://bit.ly/2wMq8V8
7. HHS: Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations. Available at http://bit.ly/2FDMGPJ
8. HHS: Bulletin: HIPAA Privacy in Emergency Situations. Available at http://bit.ly/2HBdwnT
9. 45 C.F.R. 164.510(b) (HIPAA FAQ). Available at http://bit.ly/2DwuEsw
10. Public Law 114-74 § 701 (Bipartisan Budget Act of 2015)
11. 45 C.F.R. Part 102 (Adjustment of Civil Monetary Penalties)