

## Compliance Today – May 2018 Maintaining patient privacy during an emergency

---

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

**Terrie B. Estes** ([terrie.estes@YNHH.ORG](mailto: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](mailto:pkhoury@deloitte.com)) is a Deloitte Risk and Financial Advisory Senior Consultant in Deloitte & Touche LLP's Philadelphia office. **Kaitlin McCarthy** ([kaimccarthy@deloitte.com](mailto: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.

### 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.<sup>[1]</sup>

In 2000, HHS published the final Privacy Rule, and in 2002 modifications were made.<sup>[2]</sup> 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.<sup>[3]</sup> Outside of these two scenarios, there are other situations where the use and disclosure of PHI may be permitted without the individual's authorization.<sup>[4]</sup> 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.<sup>[5]</sup>

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.<sup>[6]</sup> 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.<sup>[7]</sup>,<sup>[8]</sup> 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.<sup>[9]</sup>

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.<sup>[10]</sup>,<sup>[11]</sup> 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.

This document is only available to members. Please log in or become a member.

[Become a Member Login](#)