

# Health Information Compliance Alert

## Toolkit: OCR Tool Explains PHI Disclosure Rules During an Emergency

**Ask yourself these 3 questions to ensure HIPAA compliance.**

The care and treatment of patients comes first in an emergency. But even in the most dire situation, healthcare workers are always encouraged to keep HIPAA protocols intact to ensure the privacy, safety, and security of the injured. Luckily, the HHS Office for Civil Rights (OCR) offers a handy, interactive decision tool for emergency preparedness and recovery planning.

Check out the OCR online resource at

[www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/decision-tool-overview/index.html](http://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/decision-tool-overview/index.html).

The advance planning tool "presents avenues of information flow that could apply to emergency preparedness activities," notes the OCR. The agency maintains that the guidance is not just for recovery planners, but for anyone with questions regarding disaster preparedness.

**How it works:** The OCR decision tree guides you through a series of questions specifically designed to address emergency situations that might pertain to the HIPAA Privacy Rule. These questions are organized around three general questions:

### 1. Who is the source of the information to be disclosed?

If the source of the information is a covered entity, then the Privacy Rule would apply. Examples of covered entities that would be impacted are: healthcare providers or hospitals, health plans (private payers and federal healthcare programs), or healthcare clearinghouses (billing, coding, or health IT organizations that deal with PHI).

**Tip:** Refer to section 160.103 of the Privacy Rule to determine if you're a covered entity or utilize this helpful CMS covered entity chart at

[www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf](http://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf).

### 2. To whom is the information being disclosed?

If the PHI is being routed to a public health authority (PHA), the information can be shared. However, if the organization is not a PHA or is not one that normally deals with PHI, then proceed with caution, the guidance suggests. The OCR gives full descriptions of what constitutes a PHA and what does not in the tool discourse.

**Tip:** For a better understanding of what exactly a PHA is and what kind of PHI it is permitted to receive, you can review sections 164.501 and 164.512 (b)(1)(i) of the HIPAA Privacy Rule.

### 3. Is there a signed authorization permitting the disclosure?

If you have a data use agreement (DUA) with the PHA you plan to forward PHI to, covered entities "may make a disclosure subject to minimum necessary," OCR says. But, if you don't, you'll need to get written permission "unless the disclosure is otherwise permitted by another provision of the Privacy Rule," the guidance warns.

**Tip:** For an in-depth look at why you'll need written authorization, read section 164.508 of the Privacy Rule.

**Resource:** For more information on contingency planning and HIPAA compliance, visit [www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html](http://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html).

