Health Information Compliance Alert

Toolkit: Understand These HIPAA Violation Basics

Warning: Some HIPAA violations carry criminal penalties, too.

If your organization is digging out from under the COVID-19 avalanche, you're not alone. Many covered entities (CEs) and business associates (BAs) have been hit hard by the pandemic, and the last thing on their minds is HIPAA compliance. But as the feds start to ramp up their enforcement, it's essential to review the fundamentals.

Bolster Your HIPAA Glossary With 3 Important Definitions

To better implement HITECH provisions, the Department of Health and Human Services (HHS) finalized the HIPAA Omnibus rule in 2013. The HIPAA Omnibus final rule introduced and solidified a new tiered penalty structure, as well as new definitions relating to HIPAA violations.

First: "A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information [PHI]," according to HHS Office for Civil Rights (OCR) guidance. Moreover, a CE or BA that fails to take the appropriate steps to curb or manage any impermissible uses and disclosures of PHI could easily find itself on the wrong side of a HIPAA violation - and the financial and professional price can be very steep.

"The costs of non-compliance are usually far greater than the costs of compliance with HIPAA - the Rules are, for the most part, common-sense based," maintains **Jim Sheldon-Dean**, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, Vermont.

Here are the three important terms to know that impact OCR's decision making on HIPAA violations and penalty amounts:

1. Reasonable Cause: An act or omission in which a CE or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

2. Reasonable Diligence: Business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

3. Willful Neglect: Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

Heads up: Willful neglect violations must be investigated and penalties are mandatory, Sheldon-Dean points out.

Take a look at an overview of the CMP limits and HIPAA violation tiers based on OCR guidance:

Tiers and Civil Monetary Penalties for HIPAA Violations

There Are Criminal Penalties for HIPAA Violations, Too

Though criminal cases aren't common in HIPAA, they can happen. Oftentimes criminal violations happen when employees use patients' data for their own gain. As with civil penalties, OCR looks at different aspects of the violation before determining the penalty. The list of criminal penalties for HIPAA violations includes the following three tiers:

Critical insight: Staff are often nervous to tell practice management about their hunches, accuse other employees of wrongdoing, or verify breaches. "Train in incident management, top to bottom," Sheldon-Dean says. "Staff need to feel like they are empowered to report their suspicions of information security incidents, the handling of incidents needs to be clearly defined, and top management needs to understand the impacts of incidents and the necessity to prevent them as reasonably practicable."

Resource: See OCR's HIPAA Enforcement Rule guidance at www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html.