

# Health Information Compliance Alert

## Enforcement: Get the Facts on HIPAA Violations and Penalties

**Even low-tier penalties can add up to millions, recent case illustrates.**

You might think you're in the clear as long as you have a good grip on HIPAA requirements in your organization. Not so fast: A recent summary judgment suggests that the feds aren't afraid to go after those that ignore the rules.

**Details:** In a recent HIPAA case, an HHS Administrative Law Judge (ALJ) ruled on the side of the HHS Office for Civil Rights (OCR) against the University of Texas MD Anderson Cancer Center (MD Anderson), said an agency release on the subject. MD Anderson sidestepped its own risk analyses, failing to encrypt devices that contained electronic protected health information (ePHI) (See p.49).

The ALJ decision was in line with the OCR's Notice of Determination and "stated that MD Anderson's 'dilatory conduct is shocking given the high risk to its patients resulting from the unauthorized disclosure of ePHI,' a risk that MD Anderson 'not only recognized, but that it restated many times,'" the OCR release mentioned.

### Consider this Compliance Refresher

A few years back, the HIPAA Omnibus Final Rule introduced and solidified a new penalty structure, as well as new definitions relating to HIPAA violations. The definitions for three terms in particular are pivotal under the penalty system.

**1. Reasonable Cause:** An act or omission in which a covered entity 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.

**What's more:** Willful neglect violations must be investigated and penalties are mandatory, points out HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems LLC** in Charlotte, Vermont. And the HITECH provisions allow continued corrective actions, even if there's no penalty. Plus, your state Attorney General can bring HIPAA actions, too.

### Review the Tiered Penalty Structure

The ALJ put MD Anderson's actions within the Tier 2 level of HIPAA violations, according to the ALJ decision. "This is the second summary judgment victory in OCR's history of HIPAA enforcement, and the \$4.3 million is the fourth largest amount ever awarded to OCR by an ALJ or secured in a settlement for HIPAA violations," stated the agency release on the subject.

The size of such a large Civil Monetary Penalty (CMP) for a second level HIPAA violation is significant, and may be a harbinger of things to come.

Remember, the feds instituted section 13410(D) of the HITECH Act, which became effective for HIPAA violations on or after Feb. 18, 2009. Sheldon-Dean breaks down the penalty tiers:

**Tier 1:** Did not know and, with reasonable diligence, would not have known - \$100 to \$50,000 per violation.

**Tier 2:** Violation due to reasonable cause and not willful neglect - \$1,000 to \$50,000 per violation.

**Tier 3:** Violation due to willful neglect and corrected within 30 days of when known or should have been known with reasonable diligence - \$10,000 to \$50,000 per violation.

**Tier 4:** Violation due to willful neglect and not corrected within 30 days of when known or should have been known with reasonable diligence - \$50,000 per violation.

**Inflation:** However, don't forget HHS tweaked these baseline fines in the name of inflation back in 2016 as mentioned in an interim final rule published in the Federal Register. The changes are applicable to violations occurring after November 2, 2015. Here's the maximum amount each HIPAA violation may cost you under the CMP adjustment:

- \$55,010 per HIPAA violation
- \$1,650,300 annual cap
- The adjusted CMP is an increase from \$50,000 per HIPAA violation with a past annual cap of \$1,500,000.

**Resource:** Read the ALJ's decision with CMP details at [www.hhs.gov/sites/default/files/alj-cr5111.pdf](http://www.hhs.gov/sites/default/files/alj-cr5111.pdf).