Health Information Compliance Alert

Breaches: When Self-Reporting A Breach Leads To An Even More Serious Investigation

HIPAA compliance practices practically non-existent? That'll cost you millions.

Your organization suffers a HIPAA breach, and you do the right thing and report that breach appropriately. But what happens when the **HHS Office for Civil Rights** (OCR) swoops in and conducts further investigations? For some healthcare organizations, this can open up a proverbial can of worms.

OCR Searches for 'Widespread Noncompliance'

Case in point: Yet another "robust" Corrective Action Plan (CAP) and a whopping $3.5-million payout arose from a recent settlement agreement between OCR and **Triple-S Management Corporation, formerly American Health Medicare Inc.**, an insurance holding company based in San Juan, P.R.

Triple-S made multiple breach notifications to HHS involving unsecured protected health information (PHI), which triggered OCR to investigate, according to a Nov. 30 OCR announcement. After investigating the company's compliance with the HIPAA Rules, OCR found "widespread noncompliance throughout the various subsidiaries of Triple-S." The alleged HIPAA violations included:

- Failure to implement appropriate administrative, physical, and technical safeguards to protect its beneficiaries' PHI;
- Impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement (BAA);
- Use or disclosure of more PHI than was necessary to carry out mailings;
- Failure to conduct an accurate and thorough risk analysis that incorporates all IT equipment, applications, and data systems utilizing ePHI; and
- Failure to implement security measures sufficient to reduce the risks and vulnerabilities to its ePHI to a reasonable and appropriate level.

In addition to the hefty $3.5-million payout, the settlement also involves a CAP that requires Triple-S to establish a comprehensive HIPAA compliance program, which includes:

- A risk analysis and a risk management plan;
- A process to evaluate and address any environmental or operational changes that affect the security of the ePHI it holds;
- Policies and procedures to facilitate compliance with the HIPAA Rules' requirements; and
- A training program covering the HIPAA Privacy, Security, and Breach Notification Rules' requirements, intended for all workforce members and business associates providing services on Triple-S premises.

Expect Breach Reporting to Earn You OCR's Attention

Interestingly, this settlement and the settlement in the case of Lahey Hospital and Medical Center (see "Protect Yourself: Mobile & Medical Devices Are Ripe For HIPAA Breaches" on the cover)"were the outgrowth of privacy breaches that these entities had reported to OCR, which, in turn, triggered further investigations by the agency," noted partner attorney **Laurie Cohen** in a Dec. 7 blog posting for **Nixon Peabody LLP**. "In both cases, the OCR investigations uncovered

'widespread noncompliance' with the HIPAA Rules."

Takeaway: This case and other recent settlement agreements are "a reminder that when investigating a breach, OCR may look beyond the particular incident and review the covered entity's or business associate's overall compliance with HIPAA," warned attorneys **Elizabeth Hodge** and **Thomas Range** of **Akerman LLP** in a Dec. 1 analysis. And the next round of HIPAA audits will begin in early 2016, which will only increase the scrutiny of covered entities' and business associates' compliance efforts.

Link: The OCR's Resolution Agreement and CAP with Triple-S is available at www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/TRIPLES.html.