Codify
BY AAPC

Health Information Compliance Alert

Case Study: Paradigm Shift: Don't Expect A Small Penalty For A Small Breach

OCR starts treating BAs the same as CEs when it comes to HIPAA enforcement.

Look out, business associates (BAs): The **HHS Office for Civil Rights** (OCR) is taking aggressive action against you for breach incidents. And the consequences are real the OCR's first resolution agreement with a BA well-exceeded a half-million dollars.

On June 30, OCR announced a $650,000 settlement with a BA for a data breach of PHI. **Catholic Health Care Services of the Archdioceses of Philadelphia** (CHCS) agreed to the hefty penalty to settle potential HIPAA violations including a breach.

"This settlement agreement sets an important milestone as OCR's first resolution agreement with a BA," notes attorney **Rick Hindmand** of Chicago-based **McDonald Hopkins LLC**. OCR is expanding its recent enforcement focus on BAs, following three resolution agreements with CEs within the last eight months for failure to enter into BA agreements (BAAs) with their BAs.

Another Mobile Device Theft Causes a HIPAA Breach

Background: At the time of the incident, CHCS provided management and IT services as a BA to six skilled nursing facilities (SNFs). On April 17, 2014, OCR launched an investigation after receiving notification that CHCS had a breach involving the theft of a CHCS-issued employee iPhone.

The iPhone contained hundreds of SNF residents' PHI, including Social Security numbers, diagnoses and treatment information, medical procedures, names of family members and legal guardians, and other medical information. The iPhone was not encrypted nor password protected.

OCR's investigation revealed that, at the time of the breach incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility, nor what to do in the event of a security incident. CHCS also had no risk analysis and risk management plan, OCR claims.

'Much-Needed Services' Won't Exempt You from Big Penalties

In addition to the $650,000 monetary payment under the resolution agreement, OCR also imposed a Corrective Action Plan (CAP) and two years of monitoring the BA to help ensure that CHCS remains HIPAA compliant while acting as a BA. Interestingly, as key factors in determining the resolution amount, OCR stated:

"OCR considered that CHCS provides unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS."

Beware: The two-year CAP and the $650,000 settlement is significant, given that CHCS is a non-profit with religious affiliation, provided "much-needed services," and had only 412 records involved in the breach, notes **Colin Zick**, an attorney with **Foley Hoag LLP**. This sends a clear message that OCR is going to treat BAs involved in breaches the same as CEs when it comes to resolving breach incidents.

OCR's press release stated that CHCS provides "unique and much-needed services" and this was a factor in determining the resolution, hinting that this presumably lowered the payment amount, Hindmand notes. So for CHCS to still get such a large penalty for a relatively small-scale breach, it's clear that "doing important charitable work does not excuse HIPAA noncompliance."

Other considerations may have also factored into the settlement terms. "It is unclear from the press release what impact (if any) CHCS's role as parent of the nursing homes, or the transfer of CHCS's ownership during the course of the investigation, had in the settlement," Hindmand says. "It is possible that this may have had an impact on the dynamics of the negotiations."

Watch for More BA Enforcement Actions

Another point: The fact that the underlying breach related to this resolution agreement dates back to more than two years ago "suggests a significant backlog at OCR in resolving open matters," Zick points out.

But perhaps this was a more calculated move after all, OCR began its investigation only seven months after the HIPAA Omnibus Rule compliance date, Hindmand observes. And keep in mind that other investigations of BAs may be in the pipeline in light of the typical investigation/settlement timeframe of two-plus years, as well as the September 2013 extension of the HIPAA Privacy and Security Rules to BAs.

BAs will also be subject to scrutiny in the Phase 2 HIPAA audits.

Lesson learned: "Expect additional scrutiny and enforcement actions against BAs," Hindmand warns. "The diligence and sophistication of BAs vary widely with respect to HIPAA and related data privacy and security safeguards, so BA noncompliance may be viewed as a tempting enforcement target (low-hanging fruit)."

"This case provides another reminder that enterprise-wide risk analysis and risk management are not optional," Hindmand adds. Additionally, "even breaches that affect fewer than 500 individuals (and therefore fall below the threshold for routine OCR investigations) can create extensive exposure."

Link: To read the resolution agreement and CAP, go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html.