Codify
BY AAPC

Eli's Hospice Insider

HIPAA: HHS Focuses Investigations On Small HIPAA Breaches

Reporting no breaches is also a red flag, though.

If you thought being a small provider would keep you out of HIPAA trouble, you'd better think again.

Many hospice providers might be at increased risk of HIPAA investigation and enforcement efforts, thanks to OCR's recent announcement that it will redouble its regional offices' efforts in investigating smaller HIPAA breaches involving fewer than 500 individuals.

Old way: Up until now, OCR's regional offices focused their enforcement attentions on investigating larger breaches involving the protected health information of 500 or more individuals, but investigated smaller breaches only "as resources permit," an August announcement from OCR stated.

New way: Now, the ROs will more widely investigate these smaller breaches. "The root causes of breaches may indicate entity-wide and industrywide noncompliance with HIPAA's regulations," OCR says. "And investigation of breaches provides ... an opportunity to evaluate an entity's compliance programs, obtain correction of any deficiencies, and better understand compliance issues in HIPAA-regulated entities more broadly."

This announcement emphasizes that OCR can detect both large-scale trends among HIPAA-regulated entities as well as entity-specific compliance issues by investigating breaches, notes New York City-based attorney **Lindsay Borgeson** of **Epstein Becker & Green**. The announcement should also serve as a warning to ensure that your "breach reporting and other HIPAA compliance efforts are up-to-date and ready to withstand any potential scrutiny from OCR."

Beware Laptop, Device Thefts

Although ROs will still have discretion to prioritize their investigations of smaller breaches, OCR has directed each office to increase its efforts to identify and deliver corrective action to address breach-related noncompliance. OCR has instructed regional offices to consider specific factors, such as:

- The size of the breach;
- Theft or improper disposal of unencrypted PHI;
- Breaches involving unwanted intrusions to IT systems (for example, by hacking);
- The amount, nature, and sensitivity of the PHI involved; and/or
- Instances where numerous breach reports from a particular covered entity (CE) or business associate (BA) raise similar issues.

Spotless Breach Record Also Red Flag

In announcing increased scrutiny of small breach report cases, the OIG also states that its regional offices may consider whether or not a Covered Entity (CE) or Business Associate (BA) has any breach reports impacting fewer than 500 individuals when compared with other CEs or BAs, according to Chicago-based attorney **Valerie Breslin Montague** of **Nixon Peabody**. "This implies that it is not only breach reports that may trigger an investigation, but, likely for large systems or organizations, the lack thereof as compared to peer entities."

"In other words, if everyone else like you reports breaches and you don't, why not?" points out **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems**.

Another layer to this change is that OCR has noted that it may consider the lack of breach reports for a region, suggesting that OCR is interested in investigating the possibility of under-reporting, Borgeson notes.

CPT® 2023 American Medical Association. All rights reserved.

OCR's new interest in investigating smaller breaches may arise from the multitude of such incidents in recent months. In the announcement, OCR highlighted recent investigations and settlements involving small-scale breaches like the **Catholic Health Care Services** case, based on an employee's iPhone theft.

Recap: Back in June, OCR announced a $650,000 settlement with CHCS to settle potential HIPAA violations including a breach. At the time of the incident, CHCS provided management and IT services as a Business Associate to six skilled nursing facilities. In April 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.

Other lessons to learn from the case include:

- "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**. Expect more BA scrutiny in the pipeline.
- The settlement plus a two-year Corrective Action Plan and the $650,000 settlement is significant, given that the breach involved only 412 records. Don't expect small breaches to carry small penalties.
- A charitable structure and mission also won't save you. CHCS was slapped with the hefty penalty despite its non-profit status and religious affiliation, and despite providing "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, notes **Colin Zick**, an attorney with **Foley Hoag**.

CPT® 2023 American Medical Association. All rights reserved.