Health Information Compliance Alert

Compliance: Prepare Yourself For Heightened OCR Scrutiny Of Small Breaches

Regional offices will frown on any entities that fail to report security incidents.

Beginning immediately, the **HHS Office for Civil Rights** (OCR) will greatly expand its investigation and enforcement efforts involving HIPAA compliance. The new target? Smaller-scale breaches.

Breach Size Doesn't Matter Anymore

What to expect: On Aug. 18, OCR announced that it will redouble its regional offices' efforts in investigating smaller HIPAA breaches (involving fewer than 500 individuals). Up until now, OCR's regional offices focused their enforcement attentions on investigating larger breaches involving the protected health information (PHI) of 500 or more individuals, but investigated smaller breaches only "as resources permit," the announcement stated.

Now, the regional offices will more widely investigate these smaller breaches. "The root causes of breaches may indicate entity-wide and industry-wide noncompliance with HIPAA's regulations," OCR says. "And investigation of breaches provides OCR with 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 associate attorney **Lindsay Borgeson of Epstein Becker & Green, P.C.** 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 of 5 Key Factors

Although regional offices 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:

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

The reasons behind 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** (see "Paradigm Shift: Don't Expect a Small Penalty for a Small Breach," Health Information Compliance Alert, Vol. 16, No. 7, page 49).

Not only was this case the first OCR resolution agreement with a BA, it was also a case involving a whopping $650,000 penalty for a relatively small breach affecting only 412 individuals.

Report Even the Smallest Breaches

Brace yourself: Interestingly, OCR also states that its regional offices may consider whether or not a CE or BA has any breach reports impacting fewer than 500 individuals when compared with other CEs or BAs, according to Chicago-based partner attorney **Valerie Breslin Montague of Nixon Peabody LLP**. "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 LLC**.

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.

Resource: For more information about OCR's enforcement initiatives, visit www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.