HINSHAW

Alerts

Small Breaches Matter Too: OCR Broadens HIPAA Breach Investigations

August 26, 2016
Health Law Alert

The Regional Offices of the Department of Health and Human Services Office for Civil Rights (OCR) already investigate every reported Health Insurance Portability and Accountability Act (HIPAA) breach affecting 500 or more individuals, but now they will intensify efforts to scrutinize smaller breaches too. According to OCR, the root causes of small breaches may indicate entity-wide and industry-wide noncompliance with HIPAA regulations. By investigating the breaches of fewer than 500 individuals, OCR can evaluate an entity's compliance programs, obtain correction of any deficiencies, and better understand compliance issues in HIPAA regulated entities.

For breaches involving less than five hundred individuals, a covered entity is required to maintain a log and collectively report to OCR all such breaches occurring during a calendar year within sixty days of the end of the calendar year. OCR regional offices still retain discretion to prioritize which smaller breaches to investigate. In assessing breaches, the factors OCR Regional Offices will consider include:

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

Regions may take into account the lack of small breach reports when comparing a specific covered entity or business associate to others that are similarly situated. OCR regional offices may also consider covered entities with multiple small breaches as a better target of an investigation.

What It Means for You

The announcement emphasizes the importance of HIPAA compliance and the continued rise of HIPAA enforcement. Covered entities and business associates should assess, audit, and monitor HIPAA compliance on a regular basis, and any entity that reports a breach should be prepared for an audit and/or investigation. HIPAA financial penalties can be substantial, so all reasonable

Attorneys

Michael A. Dowell

safeguards to avoid HIPAA privacy or security breaches should be instituted.

Hinshaw attorneys have significant experience in advising health care organizations on HIPAA privacy and security compliance matters. For further information, please contact Michael A. Dowell or your regular Hinshaw attorney.

This alert has been prepared by Hinshaw & Culbertson LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship.