Policing PHI Privacy and Security: Prepare for Increased Scrutiny of Smaller Breaches

10.24.2016

According to the **Ponemon Institute**, almost all health care providers and other "covered entities" will experience a data breach. If protected health information is compromised by the breach, the entity would be required to report the breach under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"). HIPAA's breach notification structure requires reporting to the individual whose record was affected, the Department of Health and Human Services ("HHS") and/or the media. HHS recognizes a difference between "larger" breaches, or those affecting 500 or more individuals, and "smaller" breaches, or those affecting fewer than 500. *See* 45 C.F.R. 164.404-408.

Covered entities experiencing a breach affecting 500 or more individuals must notify HHS and all affected individuals (and the media, if over 500 individuals are in the same locality) within a 60-day window post-discovery. If the breach affects fewer than 500, HHS is not notified until after the end of the calendar year, and the entity would not be required to involve the media. 45 C.F.R. 164.406-408. All individuals affected must be notified of the breach within that 60-day period. 45 C.F.R. 164.404.

OCR has pursued investigations and enforcement differently for larger and small breaches as well, with its regional offices traditionally having a greater focus on the larger breaches, tackling smaller breaches only on rare occasion due to resource constraints. As of August 18, 2016 that focus has changed. OCR **announced** that, beginning in August, its regional offices are directed to expend greater effort investigating smaller breaches.

With the high number of breaches reported to OCR each year, OCR has provided guidance to its Regional Offices as to how to prioritize the cases, looking at the following factors:

- the number of individuals affected,
- the disposition of the data (e.g., whether they were destroyed or stolen),
- the nature and sensitivity of the PHI affected,
- whether the breach was caused by hacking, malware, or other high-tech attack, and
- whether the covered entity or business associate is linked to a high number of reported breaches.

As with larger breaches, OCR has the ability to assess or settle fines upon concluding an

investigation of smaller breaches, and the **influx of recent settlements** shows that OCR is ready and willing to do so after breaches of any size.

Related People