ROPES & GRAY

ALERT

Health Care

September 1, 2016

# OCR Announces Initiative to Amplify Investigations of Breaches Affecting Fewer than 500 Individuals

Taking another step toward more aggressive enforcement under the Health Insurance Portability and Accountability Act ("HIPAA"), on August 18, 2016, the U.S. Department of Health & Human Services ("HHS") Office for Civil Rights ("OCR") announced that it will begin to "more broadly investigate" breaches of protected health information ("PHI") affecting fewer than 500 individuals. Despite statutory authority to investigate all PHI breaches, OCR has, to date, focused primarily on large-scale breaches and entered into only a handful of settlement agreements with entities experiencing these so-called "small breaches." By this initiative, OCR's Regional Offices have been instructed to "increase efforts to identify and obtain corrective action to address entity and systemic noncompliance related to [small] breaches."[1] As a result, health care providers and other covered entities and their business associates should expect an uptick in the volume of enforcement actions triggered by, and OCR settlements reached in connection with, small-scale PHI breaches.

## Background

Since the passage of the Health Information Technology for Economic and Clinical Health Act of 2009 and the subsequent implementation of the HIPAA Breach Notification Rule, OCR has prioritized investigations of reported PHI breaches affecting more than 500 individuals, and imposed fines, penalties, and, with increasing frequency, corrective action plans ("CAPs") on the responsible entities.

More recently, OCR has expanded its enforcement arsenal to include proactive steps as well as reactive ones. OCR has imposed higher fines, steeper penalties, and more onerous CAPs on entities that have failed to conduct adequate risk analyses, to implement reasonable electronic safeguards to protect PHI, or to enter into required business associate agreements ("BAAs").

OCR's record-breaking settlement with Advocate Health Care Network ("Advocate") in early August, under which Advocate must pay $5.55 million and enter into a two-year CAP with independent third-party oversight, illustrates the escalating financial impact that OCR HIPAA investigations can have on affected entities. The Advocate settlement also marks the tenth OCR enforcement action in the first eight months of 2016— compared to OCR's previous high of just seven settlements in one year.

Prior to this new initiative, OCR's Regional Offices investigated all reported breaches involving the PHI of 500 or more individuals, and exercised discretion over whether to investigate reports of small breaches. In practice, Regional Offices conducted investigations based on the breaches reported annually by covered entities, or based on reports pursuant to state-level notification requirements. Those efforts have resulted in some settlements with entities for small breaches (including, since 2013, settlements with Catholic Health Care Services, Triple-S, St. Elizabeth's Medical Center, QCA Health Plan, Inc., and Hospice of North Idaho), but relatively fewer than for entities with larger breaches. OCR's new initiative, which will increase the number of investigations into small breaches, fits within the agency's overarching trend of more expansive HIPAA regulation.

[1] Email Notification, *OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals*, OCR SecurityList (August 18, 2016), available here.

## New Initiative

Starting this month, OCR Regional Offices will increase investigatory and enforcement efforts with respect to small breaches on the theory that "the root causes of [such] breaches may indicate entity-wide and industry-wide noncompliance with HIPAA's regulations, and … [provide] 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."[2]

While Regional Offices will retain discretion to prioritize which small breaches to investigate, OCR has directed that the following factors should be considered in determining whether to launch an investigation:[3]

- The size of the breach;
- The amount, nature and sensitivity of the PHI involved;
- Theft or improper disposal of unencrypted PHI;
- Breaches involving unwanted intrusions (*i.e.*, hacking) into information technology systems; and
- Instances where *numerous breach reports* from a particular covered entity or business associate raise similar issues, or, in contrast, instances where a *lack of breach reports* for small breaches are reported by a specific covered entity or business associate (relative to the number of small breaches reported by "like-situated covered entities and business associates"[4]).

## Implications for Health Care Entities

These factors illustrate the ever-expanding scope of OCR HIPAA investigations. By directing Regional Offices to investigate HIPAA-covered entities and business associates for both an over-abundance of breach reports and a dearth of breach reports, OCR appears to corral as possible targets all entities not achieving the Goldilocks of breach reporting. This generally calls on entities subject to HIPAA regulation to redouble efforts to ensure they are following best practices, including in the performance of HIPAA risk analyses, the adoption of data security and encryption measures, and the execution of BAAs (including between business associates and their subcontractors). But more specifically, it calls on health care entities to ensure that each security incident is sufficiently documented, including, if the incident is not reported, the rationale for determining that the incident did not rise to the level of a reportable breach under HIPAA.

[2] Email Notification, *OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals*, supra note 1.
[3] *Id.*
[4] *Id.*