OCR to Investigate More HIPAA Breaches Affecting Fewer Than 500 Individuals

SUMMARY
On August 18, 2016, the U.S. Department of Health and Human Services (“HHS”), Office for Civil Rights (“OCR”) announced plans to expand its investigations of reported breaches of the Health Insurance Portability and Accountability Act (“HIPAA”) that affect fewer than 500 individuals. OCR’s announcement is a reminder for covered entities and business associates to ensure that all breaches are taken seriously and that a comprehensive HIPAA compliance plan is in place and regularly reviewed.

The HIPAA Breach Notification Rule describes two categories of breaches: (1) those involving 500 or more individuals (“large” breaches); and (2) those involving fewer than 500 individuals (“small” breaches). The notification requirements for large breaches are more onerous: the media must be notified of the breach and prompt notification must be made to the HHS Secretary. For small breaches, there is no media notification requirement and the entity need only submit a cumulative small breach report (all small breaches that occurred during the prior calendar year) to the HHS Secretary within 60 days of the close of the calendar year.

By policy, OCR investigates large breaches. Historically, OCR had discretion in opening an investigation of small breaches. While OCR has investigated and entered into settlements for small breaches (http://tinyurl.com/Health-settlements), these investigations and settlements are less common than those for large breaches. When OCR investigates a covered entity or business associate following a breach report, OCR seeks to determine whether underlying HIPAA compliance deficiencies contributed to the breach.

According to OCR’s press release announcing the expansion of small breach investigations, OCR retains discretion with respect to small breach investigations, but “each [OCR regional] office will increase its efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches.” According to OCR, factors that it will consider are:

• The size of the breach;
• Theft of or improper disposal of unencrypted protected health information (“PHI”);
• Breaches that involve unwanted intrusions to IT system (e.g., hacking);
• The amount, nature and sensitivity of PHI; or
• Instances where there are numerous breach reports involving similar issues for the same covered entity or business associate.
OCR’s increased emphasis on small breach reporting was fore- shadowed less than a year ago. In September 2015 the HHS Office of Inspector General (“OIG”) released a report (http://tinyurl.com/Health-report1) that reviewed OCR’s oversight of the HIPAA Breach Notification Rule. The OIG recommended that OCR strengthen its follow up of breach reports, including better monitoring of small breach reports. Saul Ewing’s summary of the OIG report is available at http://tinyurl.com/HealthAlert100515.

Important Takeaways and Next Steps

OCR’s announcement will increase the attention given to small breaches. Covered entities and business associates should review their HIPAA compliance plans and address all compliance gaps. Covered entities and business associates would also be well served to review recent OCR settlements to understand the factual scenarios that led to the settlements, and to take appropriate action to prevent the same circumstances from occurring. If a small breach does occur, it should be taken seriously, and timely and appropriate changes should promptly be made to prevent a potential recurrence.