HHS Office for Civil Rights to Increase Investigation of Small HIPAA Breaches

Sherman A. Cohen, Kevin L. Coy, and Madison M. Pool

The Office for Civil Rights within the U.S. Department of Health and Human Services (OCR) recently announced that it has increased its review of breaches of protected health information affecting fewer than 500 individuals.[1] This increased scrutiny is likely to result in increased enforcement actions, fines, and other penalties for both covered entities and business associates.

Background

The HIPAA Privacy Rule applies to covered entities and their business associates, and it limits access, use and disclosure of individuals' protected health information (PHI) by these entities.[2] When PHI is accessed, acquired, used, or disclosed in a way not permitted under HIPAA, the presumption under the HIPAA Breach Notification Rule is that a breach has occurred unless it can be shown that there is a low probability that PHI has been compromised based on a breach risk assessment that complies with HIPAA requirements.[3] If the incident is a breach, covered entities are required to report it to OCR, in addition to other obligations. All breaches must be reported to OCR; however, the timing of that notice depends on the number of individuals affected by the breach. For a breach requiring notice to 500 or more individuals, OCR must be notified contemporaneously with notice to affected individuals. For breaches affecting fewer than 500 individuals, notice to OCR is not required until the first 60 days of the following calendar year. These "smaller" breaches traditionally have received less scrutiny from OCR.

Increase in Small Breach Investigations

Investigations of reported breaches are conducted by the OCR Regional Offices. The Regional Offices have historically investigated all breaches involving the PHI of 500 or more individuals, and have investigated smaller breaches at their discretion (and less often). However, OCR's announcement makes clear that both covered entities and business associates should expect to see increased activity around reviews of smaller breaches. OCR calls this increase an "initiative" and indicates that the investigations will attempt to identify and assess "root causes" of these smaller breaches.

Regional Offices will not be required to investigate all reported small breaches, but OCR stated that "each office will increase its efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches." OCR also provided a list of factors that Regional Offices will consider in determining which small breaches to investigate, including:

- The size of the breach;
- The amount, nature and sensitivity of the PHI involved;
- Whether there was theft of or improper disposal of unencrypted PHI; and
- Whether the breach involved unwanted intrusions to IT systems (for example, by hacking).

1 HHS Office for Civil Rights Listserv posting, *OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals*, from OCR HIPAA Security Rule information distribution [mailto:OCR-SECURITY-LIST@LIST.NIH.GOV] On Behalf Of OS OCR SecurityList, OCR (HHS/OS) to OCR-SECURITY-LIST@LIST.NIH.GOV, sent Aug. 18, 2016 11:06 AM (copy on file with author) [hereinafter OCR E-mail].

2 *See generally* 45 C.F.R. §§ 160 and 164, Subparts A and E.

3 *See generally* 45 C.F.R. § 164, Subpart D.

OCR added that Regional Offices may also consider "[i]nstances where numerous breach reports from a particular covered entity or business associate raise similar issues . . . [or] the lack of breach reports affecting fewer than 500 individuals when comparing a specific covered entity or business associate to like-situated covered entities and business associates."

OCR's announcement cites several small breach settlements as examples, with the earliest dating back to January 2, 2013—the first ever HIPAA breach settlement involving unsecured electronic PHI of fewer than 500 individuals. The most recent of the cited examples was announced in June of this year. The financial components of the settlements range from a low of $50,000 for the first-ever such settlement, to a high of $3.5 million for a settlement in November 2015.

Risks of Investigation & Steps to Take Now

Risks from an OCR breach investigation include an increased likelihood of a full audit by OCR, a potential resolution agreement with stringent terms, and possible civil monetary penalties. All of these sanctions may be imposed against both covered entities and business associates. Civil monetary penalties under HIPAA are tiered and can vary from $100 to $50,000 per violation, with a cap of $1.5 million per calendar year for identical violations. Separate violations may be separately subject to the cap.

Accordingly, covered entities and business associates should take steps to ensure that they are compliant with HIPAA's requirements generally, and, specifically, in relation to any reported breaches. HIPAA provides a six-year timeframe from the date of the violation for HHS to commence an action in response, so the following steps are important both retrospectively for already-reported breaches and prospectively for breaches that may be reported in the future:

- Ensure that documentation of the breach assessment and mitigation steps is created and retained.
- Ensure that corrective actions identified as part of the breach assessment have been implemented.
- Ensure that policies related to breach analysis and response are up to date and are being implemented and enforced.
- Review ongoing HIPAA compliance efforts because an OCR breach investigation may extend beyond the facts of the particular breach(es) being investigated to all aspects of HIPAA compliance.

Should you have any questions about lessening the risk of a HIPAA breach, evaluating whether a breach has occurred, or responding properly to an identified breach, please feel free to contact Sherman Cohen, Kevin Coy or Madison Pool on AGG's Healthcare Information Technology Team.

Authors and Contributors

Sherman A. Cohen
Partner, Atlanta Office
404.873.8630
sheman.cohen@agg.com

Kevin L. Coy
Partner, Atlanta Office
202.677.4034
Kevin L. Coy@agg.com

Madison M. Pool
Associate, Atlanta Office
404.873.8514
madison.pool@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**