No Good Deed Goes Unpunished: Reporting Business Associate's HIPAA Breach Results in Liability for Covered Entity

H. Carol Saul and Madison M. Pool

A recent Resolution Agreement between a solo practitioner physician practice and the U.S. Department of Health and Human Services Office for Civil Rights (OCR) reveals how complying with HIPAA by reporting a business associate for a breach resulted in liability for the Utah covered entity. Following the breach report, OCR opened an investigation into the practice which resulted in a $100,000 settlement and robust corrective action plan.

Background

In its first Resolution Agreement of 2020, OCR announced a $100,000 settlement and corrective action plan with the practice of Steven A. Porter, M.D., on March 3, 2020. According to the press release, OCR began investigating Dr. Porter's medical practice after it filed a breach report with OCR on November 21, 2013, related to a dispute with a business associate. The practice's breach report claimed that the business associate was impermissibly using the practice's patients' electronic protected health information (ePHI') by blocking the practice's access to such ePHI until Dr. Porter paid $50,000.[1]

Apparently, OCR used the breach report as a launching pad to open an investigation into the practice. OCR's investigation determined that, both prior to the breach and despite technical assistance from OCR during the investigation, Dr. Porter failed to conduct a security risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI as required by the Security Rule. Further, he failed to implement security measures sufficient to reduce risks and vulnerabilities to ePHI to a reasonable and appropriate level, and the practice permitted another business associate to create, receive, maintain, or transmit ePHI on the practice's behalf at least since 2013, without obtaining satisfactory assurances that it would appropriately safeguard the ePHI.

OCR cited these failures as the basis for imposing the $100,000 settlement and two-year corrective action plan, which includes multiple compliance requirements – such as conducting a security risk analysis, implementing responsive risk mitigation measures, revising policies and procedures for business associate relationships, and conducting workforce training. The breadth of the corrective action plan suggests that the practice's HIPAA compliance overall may have been poor, but it is notable that the investigation was initiated not based on any action or breach by the practice, but rather in response to the practice's report of its business associate's noncompliance in withholding PHI to gain leverage in a business dispute.

Significance

This Resolution Agreement highlights a tension between the HIPAA regulatory framework and practical operations for covered entities. Covered entities are required to report a Breach of Unsecured PHI to the Secretary (see 45 C.F.R. 164.408). In addition, Covered entities must take corrective

1 For guidance from OCR regarding how such information blocking is inappropriate, see OCR FAQ 2074, available at https://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-termi-nate-access/index.html (last accessed 3/4/20).

actions if they suspect that a business associate has breached an obligation of their business associate agreement or the HIPAA rules. Specifically, 45 C.F.R. 164.504(e)(1)(ii) provides as follows:

> A covered entity is not in compliance with the standards in §164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

However, this Resolution Agreement shows that complying with reporting obligations or pursuing the regulatory remedy of filing a complaint with the Secretary in a dispute with a business associate can increase scrutiny on the covered entity and may ultimately lead to penalties.

Practical Takeaways

Despite the risk, there will be instances where a covered entity is required to report conduct to the Secretary, or in which such a report is a reasonable step the covered entity must take in pursuit of its own compliance efforts. So what can covered entities do to mitigate this risk?

1. **Compliance.** First, every covered entity should work to keep its own HIPAA house in order. All covered entities, no matter their size, should be aware of the risks of HIPAA non-compliance, and OCR remains serious about Security Rule compliance. Per OCR Director Roger Severino, "All health care providers, large and small, need to take their HIPAA obligations seriously. The failure to implement basic HIPAA requirements, such as an accurate and thorough risk analysis and risk management plan, continues to be an unacceptable and disturbing trend within the health care industry." The best defense in an OCR investigation is solid HIPAA compliance. Good-faith efforts and organized record-keeping can go a long way toward mitigating OCR enforcement risk, even if a covered entity's compliance is not perfect.

2. **Vetting.** Second, covered entities should carefully vet business associates prior to engaging them. Working with a vendor with a good track record of reputable business practices and strong HIPAA compliance may decrease the likelihood of a dispute that reaches an impasse where a report to the Secretary is necessary. Further, although no organization is immune to a breach, a business associate with solid security practices may be less vulnerable.

3. **Indemnification.** Third, Covered entities and business associates should give close attention to negotiation of indemnification provisions in their business associate agreements (BAAs). The parties should think about the structure of the relationship, the services to be provided by the business associate, and the amount and nature of the PHI to which the business associate will have access when determining how to allocate the risk and responsibility under the BAA. Covered entities may push for the business associate to be responsible for fines and penalties that arise from OCR investigations that relate to reports of business associate misconduct or breach of the business associate agreement. In contrast, business associates may want to limit such responsibility since fines and penalties can balloon well beyond the business associate conduct nexus once the door is open to OCR. Other areas to consider in indemnification negotiations are costs associated with investigation, mitigation, and reporting of HIPAA noncompliance, including but not limited to Breaches of Unsecured PHI.

For more information or to discuss risk mitigation and allocation strategies or HIPAA compliance in general, please contact H. Carol Saul or Madison M. Pool.

Authors and Contributors

H. Carol Saul
Partner, Atlanta Office
404.873.8694
carol.saul@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 (AGG) is an Am Law 200 law firm with offices in **Atlanta** and **Washington, DC**. Our client-service model is rooted in taking a "business sensibility" approach of fully understanding how our clients' legal matters fit into their overall business objectives. We provide industry knowledge, attention to detail, transparency and value to help businesses and individuals achieve their definition of success. Our transaction, litigation and regulatory counselors serve clients in healthcare, real estate, litigation and other dispute resolution, business transactions, fintech, global commerce, economic development, public finance, government investigations and logistics and transportation. With our rich experience and know-how, we don't ask "if," we figure out "how."
Visit us at 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/**