In $3 Million HIPAA Settlement, OCR Again Emphasizes Importance of Security Rule Compliance and Timely Breach Response

H. Carol Saul and Madison M. Pool

In its second HIPAA resolution agreement of 2019,[1] the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) again emphasizes the importance of compliance with the HIPAA Security Rule and of both timely breach response and timely cooperation and response to an OCR investigation.

Overview

On May 6, 2019, OCR announced that it has entered into a Resolution Agreement with Touchstone Medical Imaging ("Touchstone"), a diagnostic medical imaging company based in Franklin, Tennessee which provides services in Nebraska, Texas, Colorado, Florida, and Arkansas. According to OCR, Touchstone "impermissibly disclosed the [protected health information (PHI)] of 307,839 individuals through the provision of access to an insecurely configured server." In a key insight from the Resolution Agreement and press release, OCR notes that Touchstone was notified of the exposure by the FBI and by OCR, yet allegedly failed to take timely corrective measures. The Resolution Agreement imposes a $3 million settlement and a two year corrective action plan.

Background

On May 9, 2014, OCR "received an email alleging that social security numbers of [Touchstone] patients were exposed online via an insecure file transfer protocol (FTP) web server. On May 12, 2014, OCR confirmed that PHI for [Touchstone] patients, including some social security numbers, was visible via a Google search." Through its investigation, OCR confirmed that "the name, date of birth, phone number, address (and in some instances, social security numbers) of 307,839 individuals had been accessible to the public through the insecure FTP server. It was determined that the server was configured to allow anonymous FTP connections to a shared directory."

Alleged Violations

The FBI notified Touchstone of the incident on May 9, 2014, and OCR notified Touchstone of its investigation on August 19, 2014. However, "OCR's investigation found that Touchstone did not thoroughly investigate the security incident until several months after notice of the breach from both the FBI and OCR. Consequently, Touchstone's [eventual] notification to individuals affected by the breach was also untimely." In addition to delayed responses to the notification of the security incident and breach notification to individuals (which was not provided until 147 days following discovery, well in excess of the maximum 60 day regulatory time frame), OCR outlines a laundry list of other alleged Security Rule violations, including: failing to conduct an accurate and thorough security risk analysis, failing to enter into compliant business associate agreements with its vendors (including its IT support vendor and a data center provider), and failing to implement sufficient policies and procedures to address technical safeguards. All such measures are longstanding legal requirements of HIPAA.

1 www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html

OCR Director Roger Severino summarized OCR's position, saying, "Covered entities must respond to suspected and known security incidents with the seriousness they are due, especially after being notified by two law enforcement agencies of a problem. Neglecting to have a comprehensive, enterprise-wide risk analysis, as illustrated by this case, is a recipe for failure."

Conclusion

OCR has repeatedly emphasized the importance of compliance with the HIPAA Security Rule, especially the requirement to conduct and document an accurate and thorough security risk analysis. Other HIPAA requirements that have received significant OCR attention include: entering into compliant business associate agreements, conducting timely breach risk assessments and providing timely notification where required, and implementing compliant policies and procedures. This Resolution Agreement comes on the heels of OCR's announcement of enforcement discretion regarding maximum annual penalty caps for violations. However, the Touchstone settlement may signal that the moderated maximum penalty tiers do not indicate a modified position on the importance of good-faith compliance with the HIPAA requirements.

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, 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/**