LOS ANGELES
Daily Journal
www.dailyjournal.com
TUESDAY, JULY 19, 2016

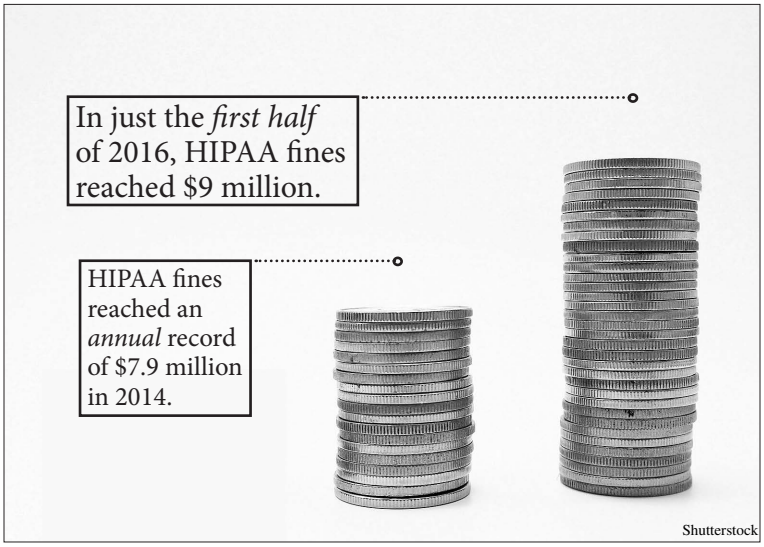
PERSPECTIVE

HIPAA enforcement reaches historic level

By Mary Ellen Callahan and David P. Saunders

The first half of 2016 saw a historic level of Health Information Portability and Accountability Act (HIPAA) enforcement actions brought by the Office of Civil Rights of the Department of Health and Human Services and as well as the first enforcement action against a business associate. In the first half of the year, OCR collected more than $9 million in HIPAA fines, a number that surpasses the previous *annual* record, which was $7.9 million in 2014. These numbers are driven in no small part by the fact that OCR fines have become much stiffer in 2016 than they were in the past. In 2016, covered entities and business associates paid millions in fines for actions that in the past may have been accompanied only with minor or even no fines.

While some of these fines are associated with data breaches such as lost or stolen laptops, an increasing number of OCR fines are for administrative failures, and specifically, for a lack of a Business Associate Agreement with vendors. This is unlikely to be a coincidence given the HHS announcement in April 2016 of Phase II of its HIPAA Privacy, Security and Breach Notification Audit, a component of which will be verifying that business associate relationships are properly documented. The increased enforcement focus on administrative failures, OCR's first enforcement action against a business associate and HHS' launch of the Phase II audit all appear to be the crescendo of the 2013 omnibus rule changes to HIPAA, which in large part subjected business associates to the same HIPAA standards as a covered entity.



Shutterstock

Enforcement Actions

2016 has already seen seven enforcement actions by OCR. While the majority of those actions relate to technical or physical security violations, three of the actions are novel, and worth analyzing. In addition to the enforcement action against a business associate, OCR took two enforcement actions related to covered entities' failures to have appropriate business associate agreements.

In a historic first, on June 24 OCR entered into a resolution agreement with a business associate, Catholic Health Care Services of the Archdiocese of Philadelphia. CHCS is a provider of management and IT services as a business associate for several nursing facilities. During the course of CHCS's engagement, an unencrypted, non-password protected CHCS mobile phone was stolen, compromising the PHI of 412 nursing residents. Compounding this theft was the fact that CHCS did not have appropriate administrative, physical and technical safeguards related to its handling of PHI. As a result of these breaches, CHCS agreed to a $650,000 fine and entered into a corrective action plan, which includes multi-year oversight by HHS.

PIG Tales

This regular column is devoted to issues of critical importance to the Privacy and Information Governance (PIG) communities. Provided by the former Chief Privacy Officer of the U.S. Department of Homeland Security, PIG Tales discusses cutting edge issues while offering valuable insight and practical advice to companies on how to collect, use, store, protect and share their sensitive data in an efficient, effective, and compliant manner.


CALLAHAN


SAUNDERS

Business associate relationships were the focus of two other enforcement actions by OCR earlier in 2016. In March, OCR announced a $1.5 million fine of North Memorial Health Care System for failing to have a proper business associate agreement with a vendor. And in April 2016, OCR fined the Raleigh Orthopaedic Clinic $750,000 for providing PHI to a business associate "without first executing a business associate agreement."

In the case of North Memorial, a business associate's employee's computer was stolen, which caused North Memorial to report a breach to OCR in 2011. During the course of its investigation, OCR discovered that North Memorial did not have a Business Associate Agreement with the company in question. In addition to the fine, North Memorial agreed to enter into a corrective action plan, including multi-year oversight by HHS of its HIPAA compliance programs.

Similarly, with respect to Raleigh Orthopaedic, the Covered Entity reported a breach to OCR in 2013. In the course of investigating that breach, OCR identified the fact that Raleigh Orthopaedic did not have a Business Associate Agreement with its vendor. In the relevant Press Release, the OCR Director explained that "HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise." As with North Memorial, Raleigh Orthopaedic was required to pay a fine and enter into a corrective action plan with multi-year HHS oversight.

Each of these actions demonstrate that OCR is focused on business associates, their relationships to covered entities, and the security that business associates are providing related to PHI.

HHS Announces Phase II HIPAA Audit

On April 25, HHS announced that OCR "has begun its next phase of audits of covered entities and their business associates." This

next phase of audits "will review the policies and procedures adopted by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security and Breach Notification Rules." In sum, OCR is looking into the administrative safeguards adopted by both covered entities and business associates.

Although OCR has indicated that it will not identify any entity that is subject to the Phase II audit, HHS has said that "OCR is identifying pools of covered entities, and business associates that represent a wide range of health care providers, health plans, health care clearinghouses and business associates." There is thus no question that business associates are squarely within the scope of Phase II. The audit will have multiple parts, including both information collection, document review and on-site reviews by OCR, and the target end date for Phase II is December 2016. Afterwards, if "an audit report indicate[s] a serious compliance issue, OCR may initiate a compliance review to further investigate."

With the rollout of the Phase II audit, the specter of an OCR auditor on site, and the possibility of a compliance review if any issues are identified during the audit, now is the opportunity for covered entities and business associates alike to ensure that they are implementing all of the technical, physical, and administrative safeguards that HIPAA requires.

Business Associate Next Steps

For business associates, 2016 seems as if it is the end of a long journey of HIPAA oversight that began with the omnibus rule amendments in 2013. When those rules were put into force, business associates became equally liable for HIPAA violations as covered entities under certain circumstances. In the intervening three years, OCR had not taken any enforcement actions against business associates. Until now.

So what can you do if you are a business associate facing the prospect of a Phase II Audit or other inquiry from HHS? Make sure your house is in order. If you are a vendor for, have clients who are, or do work with covered entities, make sure you ask the question of whether your relationship with the covered entity or even an upstream business associate includes that entity providing PHI to you. If it does, make sure you have an appropriate Business Associate Agreement in place. Of course, having a Business Associate Agreement is only the start. Business associates must also comply with HIPAA's Privacy, Security and Breach Notification Rules, all of which require the implementation of an array of technical, physical, and administrative safeguards. If you work at or do work for a business associate, now is the time to become compliant before the hammer of OCR enforcement could come down.

Mary Ellen Callahan *chairs Jenner & Block's Privacy and Information Governance Practice and provides privacy and data security counseling to a broad range of clients, including some of the most visited online properties. She served as chief privacy officer of the US Department of Homeland Security from 2009 to 2012 and was named a Cybersecurity & Privacy Trailblazer by the National Law Journal in 2015. She can be reached at mecallahan@jenner.com.*

David P. Saunders *focuses his practice on a unique mixture of litigation and privacy matters. He counsels Fortune 100 companies and small businesses alike on their HIPAA, HITECH, GLBA and state law privacy obligations. He also assists in creating and updating privacy policies, drafting vendor and business associate agreements as well as managing the response to a data breach. He can be reached at dsaunders@jenner.com.*