April 11, 2017

Year 2016 Was Biggest Yet for HIPAA Privacy Enforcement

By David Slaughter, JD, Senior Legal Editor

The year 2016 was by far the biggest yet for monetary settlements under the Health Insurance Portability and Accountability Act's (HIPAA) privacy and security rules, and 2017 thus far is proceeding apace, a leading HIPAA attorney told a recent conference.

The U.S. Department of Health and Human Services (HHS) announced 12 such settlements in 2016, averaging nearly $2 million, said Adam Greene of Davis Wright Tremaine LLP. Three more were concluded in the first 2 months of 2017, along with an outright penalty of $3.2 million in a fourth case.

Overall, since it began enforcing HIPAA, the HHS' Office for Civil Rights (OCR) has collected nearly $60 million from 48 monetary settlements and penalties, Greene said. Eight of these have required appointment of an internal or external "monitor," he noted, which doesn't necessarily get the headlines but can be the most onerous item in terms of time and resources.

The cases that result in settlements or penalties "are a statistically insignificant percentage of the work we do," said Iliana Peters, OCR senior advisor for HIPAA compliance and enforcement. "We pick cases that highlight for you the industry

compliance issues we're seeing." But don't think that because the OCR has brought one case on risk analysis, for example, the agency won't go there again, added Deven McGraw, the OCR deputy director for health information privacy.

The OCR investigates HIPAA privacy complaints, and conducts compliance reviews on its own initiative—for example, when it receives breach reports. "We're still getting roughly 17,000 complaints a year," so people obviously are still concerned about their privacy, Peters said.

"We in the health care sector frankly have not done a very good job taking cybersecurity seriously," Peters said. Moreover, cybersecurity is "just one of many risks we unfortunately have to deal with," and the risk assessment should cover all of them.

In addition to being required by the HIPAA rules, an enterprise-wide risk assessment is “your best defense in determining where the risks are,” and many breaches of protected health information (PHI) occur in areas that the risk assessment missed, Peters said. “The breach brings us to your door,” but if you have your ducks in a row the OCR won’t stay, she added. It’s the underlying problems that can result in monetary settlements.

For example, it was a malware incident that triggered the OCR’s investigation of the University of Massachusetts, but when the agency investigated, it found underlying problems with the institution’s “hybrid entity” designation. An entity may subdivide itself into a HIPAA-covered and noncovered component for HIPAA compliance purposes, but the covered component must include any part of the organization that handles PHI. UMass failed to identify all of these parts, Peters said; “they did not have a good idea of their own corporate structure.”

Hybrid entity status “is not a paperwork exercise,” McGraw said. An entity needs to identify its data flows before determining whether parts of the organization can effectively be “walled off” from the HIPAA-covered component.

In the recent case involving Memorial Healthcare System, which resulted in a $5.5 million settlement, “there were multiple breaches affecting a large number of individuals,” Peters said. This case highlights the importance of audit and access controls in countering “insider threats.”

The $2.2 million penalty against health insurer MAPRE might have been greater, given the severity of its risk analysis and management failings, but the OCR took into consideration that the company is one of Puerto Rico’s few remaining health insurers, Peters said. “OCR has never been in the business of putting companies out of business.”

January saw the first settlement for alleged violations of HIPAA’s breach notification requirements. “It is incredibly important that these notices are made timely,” and Presence Health had a pattern of trouble getting the notifications out on time, Peters said.

Audit Program Status

The OCR is finishing up its Phase 2 desk audits of covered entities, and most of these auditees have gotten draft audit reports back by now, McGraw said. The agency is still in the process of auditing business associates.

While these audits are primarily a learning, rather than enforcement, exercise, “we reserve the right to move you from an auditee into compliance review status” if you don’t respond at all, or “it looks like you really have no idea what you’re supposed to be doing,” McGraw said.

The OCR plans to finish the desk audits, and complete a wrap-up report evaluating desk audits as a tool, before considering the onsite phase, McGraw said.

The OCR welcomes the covered entity’s comments on its draft audit report, but not additional documentation, McGraw said. The audits are supposed to be just “a snapshot in time” rather than a full compliance review, she explained, so “please don’t be upset with us if we don’t want any more of your stuff.”

The privacy officers for two audited hospitals discussed their organizations' experiences with the audit process.

Privacy notices are one area where the OCR auditors seem to have taken a hard line, according to Mayo Clinic privacy officer April Carlson. "The results that came back seem to go beyond what the law required," she said. It's always a challenge to write the notice of privacy practices (NPP) in plain English and still include all the required content, but the OCR has promised to provide examples of the type of NPPs it is looking for, she added.

"People need to be looking at their notices," agreed Janelle Burns, who oversaw the audit response for Baptist Memorial Health Care Corp. For example, the OCR expected more specifics on the process and timing for granting individual access to PHI, including any stricter state requirements, she said.

Direction under Trump Administration

New HIPAA regulatory initiatives are unlikely under the new administration, but so is any kind of substantial rollback, because the healthcare industry is not pushing for one, suggested Kirk Nahra, an attorney with Wiley Rein LLP. "Most people these days are fine … dealing with HIPAA."

The OCR enforcement is unlikely to increase, and could decline if the agency's budget is cut, Nahra said. However, privacy investigations take a long time to finish, and there's no reason to think current staff won't follow those through to completion, he added. States, plaintiffs' attorneys, and the media will still be out there as well, so privacy officers need to "make sure your people continue to pay attention to this stuff."

Business associate enforcement is one area to watch, Nahra said. "Many business associates are not in compliance with the HIPAA security rule," especially the documentation requirements, and vary enormously in size, range of clients, and amount of PHI, he said. The OCR expects to learn more about them from its audit program but might not have a big enough sample.

Burns, Carlson, Greene, McGraw, Nahra, and Peters spoke March 29 at the 26th National HIPAA Summit in Washington, D.C.