Bloomberg BNA

BNA's Health Law Reporter™

The Year Ahead in HIPAA: Does 2017 Reflect the “New Normal” for Enforcement?

By Reece Hirsch

Reece Hirsch is a partner in the San Francisco office of Morgan Lewis & Bockius, and co-head of the firm's Privacy & Cybersecurity practice. He is also a member of the Advisory Board of Bloomberg BNA's Health Law Reporter. He can be reached at reece.hirsch@morganlewis.com.

The past year was marked by a number of significant new developments in Health Insurance Portability and Accountability Act (“HIPAA”) privacy and security enforcement and regulation, including noteworthy settlements, the conclusion of the Phase 2 audits, and new guidance issued in response to cyberattacks targeting the health-care industry and the opioid crisis. But the year in HIPAA enforcement and regulation was most defined by what did not happen – the absence of publicly announced HIPAA settlements by the HHS Office for Civil Rights (“OCR”) from June until late December. Many in the health-care industry are now wondering whether this lag in enforcement is an anomaly or the “new normal.”

How Vigorous Will HIPAA Enforcement Be in 2018?

In 2016, OCR entered into 13 resolution agreements arising from alleged HIPAA violations, totaling nearly $25 million in penalties. In 2017, the year began with HIPAA settlements occuring at a record pace, with nine resolution agreements totaling nearly $18 million in penalties between January and May.

And then, silence. OCR announced no new resolution agreements between June and December 27, 2017. In November 2017, Deven McGraw, former deputy director for health information privacy at OCR, stated that the pause did not reflect a pullback in enforcement, attributing it to the transition to the Trump Administration and time needed for new OCR Director Roger Severino to settle into his position. McGraw added that Director Severino has “the pedal to the metal on enforcement,” predicting more data breach settlements in the near future.

However, other factors suggest that OCR may be challenged to keep up its previous HIPAA enforcement pace. OCR's budget request for 2018 is $33 million, $6 million less than its 2017 funding, with FTEs reduced by 17 from 179 to 162. The budget request also contemplates that OCR will reduce overhead and non-personnel costs, and support its enforcement activities using civil monetary settlement funds. The Trump Administration's recent announcement of the creation of a new Conscience and Religious Freedom division at OCR could further deplete OCR's HIPAA enforcement resources.

In short, the outlook for OCR HIPAA enforcement in 2018 is unclear. However, based on recent developments, it would not be surprising to see fewer HIPAA enforcement actions in the coming year with, perhaps, OCR placing greater emphasis on larger civil monetary settlement amounts that would serve to both send signals to the industry on HIPAA compliance areas of concern and subsidize the agency's reduced enforcement budget.

Noteworthy HIPAA Settlement Agreements

While there was a decline in enforcement overall, 2017 was marked by a number of noteworthy HIPAA settlements.

Presence Health

On Jan. 9, 2017, OCR entered into a $475,000 settlement with Presence Health, one of the largest Illinois health systems. The enforcement action arose from a security breach in which the paper-based operating room records of 836 patients went missing. The enforcement action is significant because it is the first to be based on an asserted failure to comply with breach notification requirements. Presence Health allegedly failed to comply with the 60-calendar-day outer time limit for notification under the HIPAA Breach Notification Rule, notifying OCR 101 days after discovery of the breach, individuals at 104 days, and the media at 106 days. A key takeaway from the Presence Health settlement is that it is inadvisable to extend notifications beyond 60 days even if investigation is still uncovering new information. A supplemental, addendum notification is preferable to violating the 60-day rule.

MAPFRE Life Insurance Co. of Puerto Rico

OCR announced a $2.2 million settlement with MAPFRE Life Insurance Co. of Puerto Rico on Jan. 18, 2017. The precipitating incident was the theft of a data storage device, containing information of 2, 209 individuals, from the insurer's IT department in September 2011. MAPFRE represented to OCR that it would implement a security risk analysis and risk management plan and employ encryption of portable devices, but allegedly failed to do so until September 2014. Former OCR Director Jocelyn Samuels said the takeaway from this settlement was that “Covered entities must not only make assessments to protect ePHI, they must act on those assessments as well.” The MAPFRE settlement reflects perhaps the most prevalent theme in recent OCR enforcement, audits and investigations – the critical importance of an effective security risk analysis and risk management plan, which was also a key issue in the April 12 $400,000 settlement with Metro Community Provider Network.

Center for Children's Digestive Health

On April 17, 2017, Center for Children's Digestive Health (CCDH), an Illinois pediatric digestive health practice, paid OCR $31,000 in a HIPAA settlement . CCDH allegedly disclosed protected health information (PHI) of at least 10,728 patients to document storage company FileFax, Inc. without entering into a written business associate agreement. The settlement required CCDH to establish (i) a process for assessing current and future relationships to determine whether each is a business associate and (ii) procedures for limiting disclosures of PHI to business associates to the minimum extent necessary. The CCDH settlement highlights the need for covered entities to thoughtfully manage business associate relationships. It also demonstrates that an incident involving a business associate (hundreds of files containing medical records were allegedly discovered in a dumpster outside FileFax's office, leading to a lawsuit against the company by the Illinois Attorney General) can lead to upstream enforcement against a covered entity.

CardioNet

On April 24, 2017, OCR announced a $2.5 million agreement with CardioNet, a wireless cardiac monitoring service, its first with a wireless health-care provider. The incident involved the theft of a workforce member's laptop containing ePHI of 1,391 individuals that was stolen from a parked vehicle outside the employee's house. As in so many other settlements, OCR concluded that CardioNet had an insufficient risk analysis and risk management process in place at the time of the event. Significantly, OCR noted that CardioNet's HIPAA security policies and procedures, including those relating to mobile devices, were still in draft form and had not been fully implemented at the time of the incident. Covered entities and business associates will clearly not receive much credit from OCR for HIPAA policies unless they have been fully finalized, adopted and implemented.

St. Luke's Roosevelt Hospital Center

On May 23, 2017, OCR announced a $386,000 settlement with St. Luke's-Roosevelt Hospital Center, Inc., based upon an incident that arose from a patient complaint at the affiliated Institute for Advanced Medicine, which treats chronic diseases like HIV. Investigation revealed that highly sensitive PHI of two patients was faxed to people who did not have a right to see it, including one patient's employer. The St. Luke's settlement is significant because it demonstrates that OCR may consider impermissible disclosures of sensitive information about HIV, AIDS and mental health conditions particularly egregious.

HIPAA Phase 2 Audits

2017 saw the completion of the HIPAA Phase 2 audits, which were mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act. As expected, the Phase 2 desk (i.e., document-focused) audits targeted a short list of compliance issues that included breach notification, as well as security risk analysis and risk management. The audit pool consisted of 166 covered entities (90% providers, 8.7% health plans, 1% health-care clearinghouses) and 41 business associates.

It was originally planned that the Phase 2 audits would conclude with a series of onsite audits. At the 2017 AHIMA national conference in Los Angeles, Yun-Kyung "Peggy" Lee, deputy regional manager for OCR, announced that the onsite audits would not take place in January 2018 as expected, saying that OCR is reevaluating the audit program's approach and focus.

In September 2017, Linda Sanches of OCR released preliminary results of the Phase 2 audits – and they were not encouraging. In the critical area of security risk analysis, out of 63 covered entities audited, 36 received the lowest scores of 4 or 5, none received the highest score of 1. On risk management, 46 out of 63 covered entities received the lowest scores of 4 or 5, and only one received the highest score of 1. Expect risk analysis, risk management, breach notification and other areas highlighted in the Phase 2 audits to remain priorities in future OCR HIPAA enforcement.

As the preliminary results (which did not include business associate findings) indicate, OCR has been a tough grader in the Phase 2 audits, making some fine distinctions in determining compliance deficiencies. For example, covered entities have been cited for failure to use breach notification letters that meet all content requirements, including (i) recommendations for actions the individual can take to protect against harm (such as information about reviewing credit reports), (ii) a description of what is being done to investigate the breach, (iii) what is being done to mitigate harm to the individual, and (iv) actions taken to protect against future breaches. Covered entities are understandably careful not to "overshare" in a breach notification letter because information can change quickly as an investigation progresses and being too forthcoming can degrade security. Nevertheless, covered entities should make best efforts to ensure that a breach notification letter addresses each of the required informational elements with some degree of specificity.

New "Situational" HIPAA Guidance

In 2017, OCR's new HIPAA guidance documents were often "situational" in nature, applying HIPAA standards to events that tested the limits of the regulation, from hurricanes to mass shootings to the opioid crisis.

Mass Shootings

In January 2017, OCR issued an FAQ response on permissible disclosures during emergency situations after the December 2016 shootings at the Pulse nightclub in Orlando. Although Orlando's mayor asked for a HIPAA waiver, OCR explained in the guidance that no waiver was needed, clarifying when PHI can be disclosed to a patient's family member, friend, spouse or partner. Gender identity of the patient or the person receiving the information, OCR explained, does not limit or impact who PHI can be disclosed to. OCR reiterated and expanded upon this guidance in October 2017 after the mass shooting in Las Vegas, emphasizing that a HIPAA waiver is rarely required for an emergency situation like a mass shooting.

Hurricane Harvey

On August 2017, HHS Secretary Tom Price, M.D. declared a public health emergency in Texas and Louisiana in response to Hurricane Harvey. OCR issued related guidance on the applicability of HIPAA privacy and disclosure rules in emergency situations, and the ability of providers to share information with friends and family, public health officials, and emergency personnel. In the wake of Hurricane Harvey, Secretary Price granted a limited waiver of HIPAA sanctions and penalties for violations of requirements relating to (i) distributing the Notice of Privacy Practices, (ii) honoring a request to opt out of a facility directory, (iii) obtaining the patient's agreement to disclose information to family members or friends involved in the patient's care, and (iv) the patient's right to request privacy restrictions and confidential communications.

Cyber Threat Monitoring

In February 2017, OCR released guidance on reporting and monitoring cyber threats, in response to a September 2016 Government Accountability Office (GAO) report recommending updated OCR guidance for protecting ePHI in light of a reported increase in large health-care data breaches. The guidance recommends that covered entities and business associates report suspicious activity, including cybersecurity incidents, cyber threat indicators, phishing incidents, and similar events to the United States Computer Emergency Readiness Team (US-CERT), which is a branch of the National Cybersecurity and Communications Integration Center within the Department of Homeland Security.

However, disclosures of PHI to US-CERT must still fit within a HIPAA exception, such as the one found at 45 C.F.R. § 164.512(k)(2) for disclosures for national security and intelligence activities. Often, the nature of a cyber threat may be shared without sharing PHI.

OCR also recommends that covered entities and business associates monitor US-CERT's website and sign up for email alerts reporting current threats and for prompt access to patches and mitigations, when available. This is good advice because entities subject to HIPAA should be cognizant of the latest cyber threats when they update their periodic HIPAA security risk analyses.

Cyberattack Response Checklist

In June 2017, OCR released a Quick-Response Checklist for cyberattacks, which contained guidance that was high-level and not particularly surprising. OCR stated that entities experiencing a cyberattack "should" report the crime to law enforcement agencies, which may include state or local law enforcement, the FBI or the Secret Service. The decision to report a cyberattack to law enforcement, however, is not always so clear-cut. Organizations should also consider whether a particular law enforcement agency is likely to vigorously respond to the type of the cyberattack that has occurred.

The checklist also states that entities should report all "cyber threat indicators," as defined by the Cybersecurity Information Sharing Act of 2015 (CISA), to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security and the HHS Assistant Secretary for Preparedness and Response. Such reports should not include PHI. It is important to note that not all HIPAA breaches involve cyber threat indicators under CISA. OCR notes that it will consider all mitigation efforts taken by an entity when conducting an investigation of a security breach, including whether the organization voluntarily shared breach-related information with law enforcement agencies and ISAOs.

The Opioid Crisis and Behavioral Health

On Oct. 27, 2017, OCR issued guidance on situations in which health-care providers may share a patient's PHI with family members or friends when the patient may be in crisis and possibly incapacitated, such as following an opioid overdose. The guidance appeared the day after President Trump directed Acting HHS Secretary Eric Hargan to declare the opioid crisis a public health emergency, and days later the president's Commission on Combating Drug Addiction and the Opioid Crisis issued its final report with recommendations for responding to the crisis.

The guidance does not address whether health-care providers may report to law enforcement suspicions that a patient is diverting or selling prescription opioids or illicit drugs. Providers facing that dilemma must largely rely upon a narrow HIPAA exception for disclosures of PHI "in order to prevent or lessen a serious and imminent threat to the health or safety of a person or the public."

In December 2017, OCR significantly expanded on its October guidance, launching an array of new tools and initiatives in response to the opioid crisis, and implementing the 21st Century Cures Act. This package of documents is the most comprehensive set of guidance the OCR has issued focusing on a single topic.

In this guidance, OCR seeks to ensure that patients and their family members can get the information they need to prevent and address emergency situations, such as an opioid overdose or mental health crisis. For example, let's consider a 19-year-old adult patient who is addicted to opioids and misses important medical appointments without any explanation. In this case the patient's parents are not personal representatives of the patient under HIPAA because the patient is not a minor. The patient's primary care physician believes there is an emergency related to the opioid addiction and may use professional judgment to determine that it is in the patient's best interests to reach out to emergency contacts, such as parents or family, to inform them of the situation. The OCR guidance suggests that parents should establish themselves with the child's physician as a helper or caregiver involved

in care. The physician then knows not only whom to notify in an emergency, but also whom to call about the patient's care. In cases involving significant impairment, parents may need to gain legal recognition as guardians or obtain a medical power of attorney to establish status as personal representatives. It is also important to remember that other federal and state laws, such as 42 C.F.R. Part 2 relating to substance abuse disorder information, may offer greater protections than HIPAA for patient information in these situations.

The December 2017 guidance also contains new materials on a wide range of subjects. OCR created two new web pages focused on information related to mental and behavioral health, one for professionals and one for consumers, which does not break new ground, but reorganizes existing guidance and provides a user-friendly, one-stop resource. The agency also announced a new collaboration with partner agencies within HHS to identify and develop model programs and materials for training health-care providers, patients and families regarding permitted uses and disclosures of PHI of patients seeking or undergoing mental health or substance abuse disorder treatment.

Research

The December 2017 OCR publications also included new guidance on research , as called for by the 21st Century Cures Act, including a specific guidance sheet. The guidance states that a research authorization need not describe each specific future study if the particular studies to be conducted are not yet determined. Instead, the authorization must describe future purposes such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research.

In addition, OCR launched a new working group to study and report on the uses and disclosures of PHI for research purposes, which will include representatives from federal agencies, researchers, patients, health-care providers, and experts in health-care privacy, security and technology. The working group will release a report addressing whether uses and disclosures for research purposes should be modified to facilitate research while protecting patient privacy rights.

Shoring Up the "Wall of Shame"

In July 2017, OCR launched a revised HIPAA Breach Reporting Tool (HBRT) that helps individuals better identify recent HIPAA breaches and learn how breaches are investigated and resolved, the so-called "Wall of Shame." New features of the HBRT include:

- Enhanced functionality that highlights breaches currently under investigation and reported within the last 24 months;
- A new archive that includes all older breaches and information about how breaches were resolved;
- Improved navigation to additional breach information; and
- Breach response tips for consumers.

What to Expect from OCR in 2018 and Beyond

Proposed HIPAA Whistleblower Regulations

At the October 2017 Privacy + Security Forum in Washington, D.C., Deven McGraw stated that OCR will probably issue an Advance Notice of Proposed Rulemaking in 2018 addressing the HIPAA whistleblower concept. The proposed regulation would respond to the HITECH Act's mandate that HHS establish a methodology to distribute a percentage of HIPAA civil monetary penalties to individuals harmed by an improper breach of PHI or another HIPAA violation. The fact that the proposed regulations will be issued as an "advance" NPRM suggests that the regulation will be very much a work-in-progress, with significant industry input anticipated.

Proposed Accounting of Disclosures Regulation

The HITECH Act also mandated modifications to HIPAA's accounting of disclosures requirement, seeking to expand those patient rights to reflect the enhanced capabilities of electronic health records. A Notice of Proposed Rulemaking issued in 2011 on the subject was met with widespread criticism from the health-care industry and seemed to have been tabled in recent years. McGraw also stated at the Privacy + Security Forum that OCR is working on another Advance Notice of Proposed Rulemaking on the accounting of disclosure rules to fulfill the HITECH Act requirement. McGraw stated that this regulation, soliciting industry input, is expected to be published in 2018.

Applying the Executive Order on Regulatory Cuts

President Trump's January 2017 Executive Order requires that federal agencies cut two regulations for every new regulation that is enacted. As OCR rolls out new HIPAA regulations in 2018, the agency will have to grapple with the meaning of that order. How should a “regulation” be defined? Clearly, none of the HIPAA Privacy, Security, Breach Notification, Enforcement and Transactions and Code Sets Rules are going to be struck down in their entirety. OCR may consider “pruning” one or more of the less practical Privacy Rule standards, such as the requirement to enter into business associate agreements, as a qualifying regulatory cut.

The Regulatory Horizon

At the Privacy + Security Forum in October, Deven McGraw also spoke to what OCR is working on in the longer term. The agency is preparing long-awaited guidance on HIPAA's minimum necessary rule to fulfill the HITECH Act mandate in this regard.

Surprisingly, McGraw also that that business associate agreements (BAAs) are “a candidate for elimination.” This statement seems to recognize the amount of effort that the health-care industry devotes to negotiating and entering into BAAs, even though business associates have been legally required to adhere to the business associate rules since the compliance date of the HIPAA Final Rule in September 2013. No one should get their hopes up that BAAs will be eliminated any time soon, but it is interesting that OCR appears to be at least considering whether the current regulatory approach to business associates is appropriate.