Bloomberg Law

BNA's
Health Law Reporter™

HIPAA Turns 20: Looking Back at 2016 and at the Challenges Ahead

BY REECE HIRSCH

Last year marked the twentieth anniversary of the Health Insurance Portability and Accountability Act (HIPAA), and it was a landmark year, from the commencement of the Phase 2 audit program to the record amount of settlement and enforcement activity. 2017 promises to be just as eventful, from the uncertain impact of the Trump administration to OCR's efforts to ensure that HIPAA guidance keeps pace in a period of rapid health-care technological innovation. There were major HIPAA developments in 2016, but much remains on the regulatory horizon for 2017.

Looking Forward

The Trump Administration and HIPAA Enforcement: What's Next? As in so many other areas of government regulation, the incoming Trump administration creates uncertainty regarding the future direction of HIPAA enforcement. In the short term, the new administration is not likely to alter the course of the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) with respect to its ongoing HIPAA audit program and enforcement efforts. Decisions regarding enforcement of the HIPAA rules are largely made by career agency staff who are not political appointees.

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

Because the HIPAA audit program and new requirements regarding OCR enforcement activities are mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, there is unlikely to be any sort of major course-correction in the near term. OCR's enforcement actions in 2016 brought in a record-setting $23.51 million in settlements, which also suggests that OCR enforcement will remain on track in 2017 if it is viewed as a revenue-generating, or at least self-sustaining, government program. The long-term direction of the agency will be set after a new OCR director is appointed, which will likely occur several months into the new administration.

Further into the new administration, it is at least possible that OCR's HIPAA enforcement efforts may be scaled back as part of a general focus on lessening the role of government and encouraging the role of private enterprise in advancing privacy and cybersecurity. As Thomas Bossert, the newly appointed assistant to the president for homeland security and counterterrorism, stated, ''[W]e must work toward cyber doctrine that reflects the wisdom of free markets, private competition and the important but limited role of government . . .'' (Bloomberg BNA Privacy & Security Law Report, 1/2/2017, ''Trump Names Cybersecurity Advisor With Free Market Views.'')

Thus far the new administration has been silent on HIPAA and health-care privacy and security matters, but as a candidate Trump was uniquely vocal on cybersecurity issues. Late in the campaign, Trump dedicated a speech to the issue and stated, ''To truly make America safe, we must make cybersecurity a major priority.'' Trump also expressed strong support for the Federal Bureau of Investigation (FBI) in its dispute with Apple to unlock the encryption of the iPhone used by one of the San Bernardino shooters, suggesting that in balancing the needs of law enforcement against consumer privacy, Trump may tend to side with law enforcement.

Therefore, to the extent that it's possible to predict the Trump administration's impact on HIPAA privacy and security enforcement, it seems likely that the health-care industry may be invited to participate in general efforts to improve the nation's cybersecurity and information-sharing defenses. The industry would particularly benefit from participation in any such initiatives because in recent years the health-care sector, along with retail, has been a primary target for sophisticated, large-scale cybercrime, due largely to the high black market value of medical information.

 ISSN 1064-2137

OCR Aims to Modernize HIPAA in 2017. When HIPAA was enacted in 1996, electronic medical records, cloud computing and mobile apps were not part of the health-care landscape. OCR has made efforts to apply HIPAA standards to emerging technologies, issuing guidance on cloud computing and mobile apps in 2016. OCR's budget submission to Congress for 2017 continues that initiative, highlighting ''modernizing HIPAA and supporting innovation in health care'' as a priority for this year.

The modernization initiative will focus on three areas:

1. **Cybersecurity.** OCR intends to advance implementation of the Cybersecurity Information Sharing Act (CISA) of 2015 by issuing guidance mapping HIPAA regulations to the National Institute of Standards and Technology (NIST) Framework. OCR's 2017 funding will also be used to expand investigative staff in all OCR regions dedicated to cyber breaches.

2. **Big data.** OCR recognizes both the risks and rewards of using big data analytics in health care. As an enforcer of anti-discrimination laws affecting the health-care industry, OCR believes that it is uniquely suited to ensure that the use of big data does not violate the civil rights of health-care consumers. OCR also acknowledges the benefits of big data to advance medical research and transform health care delivery through efforts such as former President Barack Obama's Precision Medicine Initiative.

3. **New Questions.** OCR realizes that new health-care technologies are raising questions that the HIPAA regulations are hard-pressed to address. The robust information sharing that is necessary to enable innovation can only occur if the public is assured of adequate privacy and security protections for their medical information, even when it is maintained by entities that are not currently regulated by HIPAA. OCR has committed to collaborate with other agencies to ensure that privacy and security protections extend throughout the health-care ecosystem, including the Office of the National Coordinator for Health Information Technology (ONC), the Food and Drug Administration (FDA) and the National Institutes of Health (NIH). Since the HITECH Act extended HIPAA regulation to business associates commencing as recently as 2013, it is unlikely that the HIPAA statute will be amended again to further extend its scope in the near future. Broadened privacy and security regulation of other entities maintaining medical information is more likely to come through agency guidance and inter-agency cooperation.

OCR and FTC Will Continue to Double-Team the Health-Care Industry. The Federal Trade Commission is the U.S. agency that has staked out the broadest jurisdiction to regulate privacy and security practices, based on its authority to regulate unfair and deceptive acts and practices under Section 5 of the FTC Act. While the FTC had taken enforcement action against HIPAA covered entities, it had traditionally done so in conjunction with OCR.

Since the FTC commenced a 2013 enforcement action against LabMD Inc., a medical testing laboratory, that approach has shown signs of change. In January 2016, the FTC announced a $250,000 settlement with Henry Schein Practice Solutions Inc., a leading dental office management software provider, to resolve claims that it deceptively marketed its products as having industry-standard encryption that would help clients meet HIPAA obligations.

Uncertainty regarding the nature of collaboration between OCR and FTC was clarified somewhat by a joint guidance document issued by the agencies in October 2016. The brief guidance document made clear that in this new world of mobile apps, activity trackers and personal health records, many companies face privacy regulation across a continuum of activities, some regulated by OCR and others regulated by the FTC. For example, even if a covered entity discloses protected health information (PHI) pursuant to a valid HIPAA authorization, the FTC may still consider whether other statements made to the individual beyond the authorization form are deceptive or misleading, in violation of the FTC Act.

The future direction of FTC privacy and security enforcement is somewhat unsettled. In November 2016, the Eleventh Circuit stayed enforcement of the FTC's *LabMD* order, suggesting that it may side with LabMD's challenge to the scope of the agency's regulation of security under the FTC Act. With the recent resignation of FTC Chairwoman Edith Ramirez, Trump will have a unique opportunity to fill three vacant commission seats, with a fourth term ending by the end of 2017. (*Bloomberg BNA Privacy & Security Law Report*, 1/23/17, ''Ramirez Exit Gives Trump Unprecedented Chance to Shape FTC.'') Despite these changes at the agency, it seems likely that the tag team approach of OCR and FTC to health-care privacy and security regulation will remain unchanged in the coming year.

Continued Focus on Security Risk Analysis. OCR has been very clear, in the Phase 2 desk audits, recent enforcement actions and public pronouncements, that it views risk analysis as the cornerstone of HIPAA Security Rule compliance. Covered entities are required to conduct ''[a]n accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of PHI.'' (45 C.F.R. § 164.308(a)(1)(ii)(A))

In the Phase 2 desk audits, risk analysis and risk management were the only standards addressed under the HIPAA Security Rule, and the questions were directed to both covered entities and business associates. That focus was driven in part by the fact that the Phase 1 audit findings showed that two-thirds of the audited entities lacked a complete or accurate security risk analysis program. If OCR finds in the Phase 2 audits that security risk analysis continues to be a common deficiency, continued enforcement activity targeting this area should be expected.

In 2016 and thus far in 2017, settlement agreements with the following entities have cited inadequate risk analysis and/or risk management processes: North Memorial Health Care of Minnesota, Feinstein Institute for Medical Research, Catholic Health Care Services of the Archdiocese of Philadelphia, Oregon Health & Science University (OHSU), Advocate Health Care Network, St. Joseph Health and MAPFRE Life Insurance Company of Puerto Rico. OHSU had performed risk analyses in 2003, 2005, 2006, 2008, 2010 and 2013, but OCR found that those analyses did not cover all electronic PHI maintained by OHSU's enterprise. Therefore, covered entities and business associates seeking to prioritize

  HLR ISSN 1064-2137

their HIPAA compliance efforts and expenditures in 2017 would be well served to start by confirming that their organization has performed an appropriate and current security risk analysis.

Looking Back

OCR Gets Tough on Enforcement in 2016. 2016 may be remembered as the year that the gloves finally came off with respect to OCR's enforcement of HIPAA. Settlement amounts totaled $23.51 million in 2016, up drastically from $6.19 million in 2015 and the previous high of $7.9 million in 2014. There was no anomalous, blockbuster settlement that skewed these 2016 figures—the average settlement amount was $1.81 million, not that much higher than 2014's previous high of $1.32 million per settlement.

The increase in enforcement activity is attributable to a couple of factors. First, OCR has had several years to educate the health-care industry on HIPAA privacy and security requirements, and several more to help the industry address the new provisions of the HITECH Act. Early enforcement actions were largely complaint-driven and typically concluded by requiring the covered entity to adopt improved privacy or security safeguards. OCR's less forgiving enforcement posture could reflect a view that covered entities have now had ample opportunity to implement HIPAA safeguards and benefit from industry guidance following the level-setting exercise of the HIPAA Phase 1 audits in 2011 and 2012.

Second, OCR may be responding to a history of criticism that it has not adequately enforced HIPAA. The HHS Office of Inspector General has issued multiple reports urging OCR to take a more aggressive approach to HIPAA enforcement. Partially in response to such criticism, the HITECH Act imposed new requirements regarding when OCR must investigate HIPAA complaints and conduct compliance reviews. (*See Bloomberg BNA Privacy & Security Law Report*, 2/4/2013, Reece Hirsch and Heather Deixler, ''Final HIPAA Omnibus Rule Brings Sweeping Changes to Health Care Privacy Law.'') In November 2015, a bipartisan group of U.S. senators sent a letter pressing OCR on its handling of certain large health plan breaches.

Settlement payments to OCR in 2016 included a $5.55 million payment from Advocate Health Care Network, a Chicago-area hospital and health-care provider network, the largest settlement amount ever received from a single covered entity. OCR alleged that Advocate did not have adequate data security measures or HIPAA-compliant policies and procedures, enabling a breach that involved the personal health information of about 4 million individuals. Although it's certainly possible that the Trump administration could bring a ''limited government'' approach to health-care privacy regulation that would curtail OCR's HIPAA compliance ramp-up, it seems more likely that OCR's 2016 banner year reflects the ''new normal'' of HIPAA enforcement.

Phasing In the Phase 2 Audits. In July 2016, the HIPAA Phase 2 audits commenced when 167 covered entities received notice of a desk audit from OCR. Desk audits of business associates began in the fall. The third round of Phase 2 audits will commence sometime in early 2017 and will involve more comprehensive onsite audits of both covered entities and business associates.

One of the primary takeaways from the Phase 2 desk audit process is that OCR is very focused on two areas of HIPAA compliance: security breach notification and security risk analysis and risk management. These two areas have been a recurring theme in recent OCR enforcement actions and public comments, and the Phase 2 desk audit questions confirmed that focus.

In 2017, it will be interesting to see how OCR judges the current state of HIPAA compliance among business associates. The Phase 2 desk audits provide OCR with the first opportunity to systematically examine HIPAA compliance practices among this broad class of newly regulated entities. If the audited business associates' compliance efforts are found lacking, that could lead to a new round of industry guidance and perhaps enforcement actions. Even though OCR Director Jocelyn Samuels emphasized that the Phase 2 audits are intended as an information-gathering exercise rather than a punitive process, it will also be interesting to see how OCR responds to the discovery of significant HIPAA deficiencies among audited entities.

OCR Guidance: From Ransomware to Cloud Computing. OCR produced a number of timely and useful guidance documents in 2016, often grappling with the application of HIPAA to new technologies and cyber threats.

Ransomware. OCR issued a fact sheet addressing the relatively new threat posed by ransomware. Ransomware is a type of malware that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

Key Takeaway: The presence of malware on a covered entity or business associate's systems is a security incident under the HIPAA Security Rule. It is also a potential breach under the HIPAA Breach Notification Rule because OCR considers the unwanted encryption of data by ransomware to be an unauthorized ''acquisition'' of ePHI and thus a disclosure not permitted by HIPAA (even when the data is not actually exfiltrated). Whether that ''disclosure'' requires notification of affected individuals must be determined based upon an analysis of the factors set forth in the Breach Notification Rule.

Cloud Computing. In response to the proliferation of cloud-based EMRs and cloud services offering access to networks, servers, storage and applications, OCR issued guidance on the use of cloud computing solutions by HIPAA covered entities and business associates.

Key Takeaway: A covered entity or business associate may utilize a cloud service provider that stores ePHI on servers outside the United States provided that applicable HIPAA requirements are satisfied. However, if ePHI is being maintained in a country where there are documented increased attempts at hacking or other malware attacks, such risks should be taken into account in the entity's risk analysis and risk management processes.

Patient Access Rights. In February 2016, OCR issued an extensive guidance document addressing many practical issues relating to an individual's right to obtain access to PHI under HIPAA, from fees for copies to the form and format for providing records.

Key Takeaway: While covered entities are required to implement reasonable safeguards to protect trans-

missions of PHI, individuals have a right to receive their PHI by unencrypted email if the individual requests access in that manner. In such situations, the covered entity must provide a brief warning to the individual that there is some degree of risk that the unencrypted email could be read or accessed, and confirm that the individual still wants to receive PHI by unencrypted email.

Mobile Apps. In February 2016, OCR also came out with guidance setting forth hypothetical scenarios and key questions to help app developers determine when they are subject to HIPAA regulations.

Key Takeaway: In the guidance OCR confirmed the assumptions regarding HIPAA regulations that many in the mobile health app space had been operating under. When a consumer downloads a health app on her smartphone and populates it with her own health information without any involvement by her health-care providers, the consumer and the app developer are not subject to HIPAA.

Noteworthy OCR Enforcement Actions. As discussed above, 2016 was a record year for HIPAA enforcement by OCR. Here are a few noteworthy settlements and what made them significant:

■ Advocate Health Care Network: The largest HIPAA settlement amount paid to date, in which OCR emphasized Advocate's alleged failure to perform comprehensive risk analysis and risk management (settlement amount: $5.5 million).

■ Presence Health: The first HIPAA enforcement action for lack of timely breach notification within 60 days of discovering a breach (settlement amount: $475,000).

■ Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS): The first resolution agreement entered into by OCR with a business associate for alleged violations of HIPAA standards (settlement amount: $650,000).

■ Care New England Health System: OCR emphasized in this settlement that even a failure to update business associate agreements to include revisions required by the HIPAA Final Rule may be grounds for enforcement (settlement amount: $400,000).

■ Raleigh Orthopaedic Clinic, P.A. of North Carolina and North Memorial Health Care of Minnesota: In both of these settlements, OCR highlighted an alleged failure by the entity to enter into a business associate agreement with a vendor or business partner receiving a significant volume of PHI. (settlement amounts: $750,000 and $1.55 million, respectively).

■ St. Joseph Health: OCR emphasized in this settlement that a security risk analysis cannot be performed in a ''patchwork fashion,'' must be enterprise-wide, and must be updated to evaluate and address potential security risks when there are enterprise changes affecting ePHI, such as implementation of a new server for a meaningful use project (settlement amount: $2.14 million).

■ University of Massachusetts Amherst (UMass): In this settlement, OCR underlined that covered entities that elect ''hybrid entity'' status must properly designate all of their health-care components performing HIPAA covered functions, and ensure that those components are complying with HIPAA. This settlement is particularly relevant for educational institutions, even if they are not part of an academic medical center and do not operate a medical school (settlement amount: $650,000).

Conclusion

2016 was a landmark year for HIPAA regulation, marked by audits, record enforcement activity and new guidance intended to show that the health-care privacy and security law and its regulations are flexible enough to keep pace in a period of rapidly evolving health-care IT innovation. Although it is difficult to predict the impact of the Trump administration on HIPAA enforcement and regulation at this early stage, it's a safe bet that by this time next year we will be looking back on at least a few new developments in health-care privacy and security regulation that surprised even the experts.

  HLR ISSN 1064-2137