Bloomberg BNA

BNA's
Health Law Reporter™

Beyond HIPAA: Five Health-care Privacy Trends for 2016

BY REECE HIRSCH

Health care, like financial services, has traditionally been one of the most extensively regulated sectors with respect to privacy and cybersecurity. That does not mean, however, that the industry is adequately prepared to defend against new cyber threats and regulatory scrutiny. 2016 promises to bring new challenges for health-care privacy and compliance professionals seeking to keep pace with a rapidly evolving regulatory landscape marked by increasingly sophisticated hackers and cybercriminals, new regulatory agencies targeting health care and new wearable devices collecting health information in new and powerful ways. Here are five health-care privacy and security trends to watch in the coming year.

1. Cybersecurity: Applying Old Standards to New Threats.

In 2015 it became clear that health-care organizations are not immune to the large, high-profile cyber attacks that have plagued major retailers. Major health-care industry breaches stemming from hacking or IT incidents have included Anthem (78.8 million individuals affected), Premera Blue Cross (11 million individuals) and UCLA Health System (4.5 million individuals). The Ponemon Institute's 2015 Study on Privacy and Data Security of Healthcare Data (the ''Ponemon Healthcare Study'')[1] identified ''criminal attacks'' as the number one cause of health-care data breaches.

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. He can be reached at (415) 442-1422 or rhirsch@morganlewis.com.

It is no secret that the Department of Health and Human Services Office for Civil Rights (OCR) 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 risk and vulnerabilities to the confidentiality, integrity and availability of electronic PHI.''[2] In order to accurately and thoroughly assess current security risks, health-care organizations must familiarize themselves with the latest cyber threats and exploits. OCR and the National Institute of Standards and Technology (NIST) emphasized the importance of the risk analysis and encryption at the annual security conference that they co-hosted in September 2015, as well as in several recent OCR enforcement actions.

In the Ponemon Healthcare Study, 70 percent of the respondents said the greatest security threat facing their organizations was employee negligence. That might have been true in the past, but it is probably not accurate for most health-care organizations today. An organization that misunderstands its primary security threats is likely to misallocate its security resources and fall short in its security risk analysis. A health-care organization that does not have internal IT and security staff who have their fingers on the pulse of current cyber threats should consider engaging external resources that have that expertise.

The health-care industry is likely to continue to face increasingly sophisticated cyber threats in 2016. Cybercriminals are focusing on the industry because it is a ''target-rich environment.'' Exploits may target personally identifiable information for fraud and medical identity theft, research and manufacturing data, and even market-moving information on public company transactions (as demonstrated by the FIN4 malware that extracted data from law firms representing pharmaceutical and medical device companies). Increasing digitization of medical records and connectivity of medical devices only increases the number of areas where health-care organizations are vulnerable. In order to

[1] *See* http://www.ponemon.org/news-2/66.
[2] 45 C.F.R. § 164.308(a)(1)(ii)(A).

 ISSN 1064-2137

face these new cyber threats, health-care organizations must incorporate an understanding of those threats into their HIPAA security risk analysis.

2. HIPAA Phase 2 Audits: It's All About the Documentation.

OCR will soon begin a second phase of audits of compliance with HIPAA privacy, security and breach notification rules, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Phase 2 audits have been delayed for more than a year but are expected to commence sometime in early 2016. The sample size for the Phase 2 audits is relatively small (350 covered entities and 50 business associates), making the odds that any particular organization will be audited relatively low. Nevertheless, 2016 is a good time for HIPAA-covered entities and business associates to review their HIPAA compliance programs—even if they are lucky enough to avoid audit.

Unlike the Phase 1 audits, which were a one-off exercise performed by contractor KPMG, the Phase 2 audits will set the stage for ongoing HIPAA auditing by OCR. Phase 2 will reflect a more sustainable approach, with audits conducted by OCR regional investigators and relying upon data collection through a new OCR web portal.

The Phase 2 audits will make HIPAA Security Rule compliance an area of focus. In the Phase 1 audits conducted in 2011 and 2012, more than 60 percent of OCR's findings or observations were Security Rule violations. Fifty-eight of 59 audited health-care provider covered entities had at least one Security Rule finding or observation—even though the Security Rule represented only 28 percent of the total audit items. Significantly, two-thirds of the entities audited lacked a complete and accurate risk analysis.

Phase 2 will be comprised largely of ''desk audits'' that emphasize review of an organization's policies, procedures and other documentation rather than the labor-intensive on-site reviews of Phase 1. Organizations that will fare well in a Phase 2 audit, and future OCR audits, will take a rigorous, ***documented*** approach to HIPAA compliance. Organizations seeking to prepare for this new regulatory environment should ensure that their HIPAA policies and procedures have been approved, implemented and updated on a regular basis. Even minor deficiencies, such as a failure to sign and formally adopt a policy, can create a presumption of noncompliance. Phase 2 audits will be all about the documentation.

3. The Role of the Board: Privacy and Cybersecurity Compliance Begins at the Top.

In a June 2014 speech at the New York Stock Exchange on ''Cyber Risks and the Boardroom,'' SEC Commissioner Luis Aguilar made a statement that has become a recurring theme for the agency: ''Given the significant cyberattacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyberattacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk-oversight responsibilities.'' [3]

While Commissioner Aguilar's statement was directed at public company boards, it is equally applicable to all health-care organizations because it is premised upon the fiduciary duty of a corporate board to protect corporate assets. Increasingly, corporate assets take the form of information—and that is especially true in the health-care industry.

In the wake of a significant data breach, it is likely that companies will see more so-called *Caremark* shareholder derivative claims, premised on the seminal case *In re Caremark International Inc. Derivative Litigation.*[4] Under Delaware law, a *Caremark* claim charges a lack of board oversight of compliance functions. A *Caremark* claim is based on violation of the duties of loyalty and good faith, which is significant because while the business judgment rule may shield directors from monetary damages for breaches of the duty of care, it does not protect them from breaches of the duties of loyalty and good faith.

Some health-care boards may be vulnerable to *Caremark* claims because privacy and cybersecurity can seem like a highly technical subject that some directors don't feel comfortable, or qualified, to address. This may be particularly true of community-based boards of nonprofit health-care organizations. It is important to remember that directors are not required to become cybersecurity experts; they are entitled to rely upon the advice of management and outside experts. Boards should emphasize process over perfection when it comes to cybersecurity and should consider how oversight of cybersecurity is managed, whether through the full board, the audit committee, an enterprise risk committee, or through a dedicated ''cyber director.''

Although it can be highly technical, cybersecurity is in the end just another organizational risk (and a growing one) that boards must manage. A board that never devotes time in its agendas to privacy and cybersecurity matters may be increasing its exposure to *Caremark* and other theories of liability. As Commissioner Aguilar notes, ''Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril.''[5]

4. The FTC Takes Aim at Health Care.

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.[6] While the FTC had taken enforcement action against HIPAA-covered entities, it had traditionally done so in conjunction with OCR. That approach seemed to change in 2013 when the FTC filed an administrative action against LabMD, a medical testing

[3] SEC Commissioner Luis A. Aguilar, ''Board of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus,'' Cyber Risks and the Boardroom Conference, New York Stock Exchange, June 10, 2014, available at www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[4] 698 A.2d 959 (Delaware Chancery, 1996).

[5] SEC Commissioner Luis A. Aguilar, ''Board of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus,'' *supra*.

[6] 15 U.S.C. § 45.

   ISSN 1064-2137

laboratory, after discovering that the company's patient information was available on a file-sharing network.[7]

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 their HIPAA obligations.[8] Therefore, it appears that HIPAA-covered entities and business associates must take into account two active regulatory agencies with different priorities and areas of focus when developing privacy and security compliance programs. An awareness of FTC guidance is particularly important for health-care organizations that are offering mobile apps or engaging in other digital health ventures.

The regulatory landscape is further complicated by the ongoing LabMD case. While challenges by LabMD and Wyndham Worldwide Corp. to the FTC's authority to regulate data security under Section 5 of the FTC Act have been unsuccessful thus far, LabMD won a surprising victory when an administrative law judge ruled in November that a ''preponderance of evidence'' in the case failed to show that the company's allegedly unreasonable data security caused, or was likely to cause, substantial consumer injury.[9]

Although the FTC is appealing the ALJ's dismissal of the LabMD case, the ruling may encourage companies targeted for privacy and security deficiencies to follow the lead of LabMD and Wyndham in challenging the agency in court, rather than acceding to an onerous settlement and corporate integrity agreement. 2016 has already begun with the FTC settling an enforcement action involving a health-care organization and that probably won't be the last time that the agency flexes its muscle in the industry in the coming year.

5. Wearable Devices, Big Data, the Internet of Things and the Gray Areas of Privacy Regulation.

The past year has seen a boom in digital health, resulting in part from the growing popularity of activity trackers, smart watches, networked glucose monitors and mobile apps that harness the computing power of the smart phone. These new digital health products raise a host of new privacy questions. The extent to which these new products are regulated under HIPAA can sometimes be unclear. For example, a fitness tracker sold to an individual consumer is not regulated by HIPAA because there is no covered entity involved, but its privacy and security representations would fall within the FTC's jurisdiction. However, if the same activity tracker is sold to a health plan so that the health plan may provide it to one of its members, the tracker would likely be to a business associate subject to HIPAA obligations.

The FTC has taken a keen interest in this new world of ''consumer-generated health data,'' but thus far the agency seems content to rely on its existing authority under Section 5 of the FTC Act to regulate this area. Digital health devices are also part of the so-called Internet of Things (IoT), the decentralized network of ''smart objects.'' In May 2015, FTC Commissioner Julie Brill called on industry to develop best privacy practices ''right now'' to address the most urgent consumer protection issues raised by IoT.[10]

Health-care organizations venturing into the digital health arena should take that message to heart. Privacy regulation is based on traditional notions of notice and consent. Those concepts must be adapted to apply to IoT. Wearable fitness trackers typically don't have a user interface to serve as a means to present consumers with choices about data collection. Connected devices may in some environments be too numerous for consumers to effectively manage their information. Commissioner Brill urges IoT and digital health companies to ''get creative'' about providing privacy transparency and control for consumers to manage their data through techniques such as a ''command center'' that provides privacy information for multiple devices.[11]

The new generation of digital health devices also presents a new means of achieving ''big data,'' applying emerging techniques in big data analytics to enormous databases of medical information, including both protected health information (PHI) subject to HIPAA and consumer-generated health information. For HIPAA business associates that have access to large volumes of medical information—such as electronic medical record, personal health record and revenue cycle management companies—big data strategies must rely on interpretation of some fairly ill-defined HIPAA rules relating to use of PHI for ''management and administration,'' ''data aggregation services'' and de-identification.[12]

In August 2015, the Health IT Policy Committee approved draft recommendations from its Privacy and Security Workgroup on privacy and security challenges associated with big data. The committee encouraged use of voluntary codes of conduct to achieve transparency and accountability with respect to big data. As with so many of 2016's emerging health-care privacy issues, creativity will be needed to adapt existing laws to new technologies.

---

[7] *In the Matter of LabMD, Inc.*, available at www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[8] ''Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data,'' available at www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled.

[9] ''Administrative Law Judge Dismisses FTC Data Security Complaint Against Medical Testing Laboratory LabMD, Inc.,'' available at www.ftc.gov/news-events/press-releases/2015/11/administrative-law-judge-dismisses-ftc-data-security-complaint.

[10] FTC Commissioner Julie Brill, ''Protection and the Internet of Things,'' EuroForum European Data Protection Days, May 4, 2015, available at https://www.ftc.gov/system/files/documents/public_statements/640741/2015-05-04_euroforum_iot_brill_final.pdf.

[11] *Id.*

[12] *See* ''HIPAA Business Associates and Health-Care Big Data: Big Promise, Little Guidance'' by Reece Hirsch and Heather Deixler, 23 HLR 267, 2/20/14.