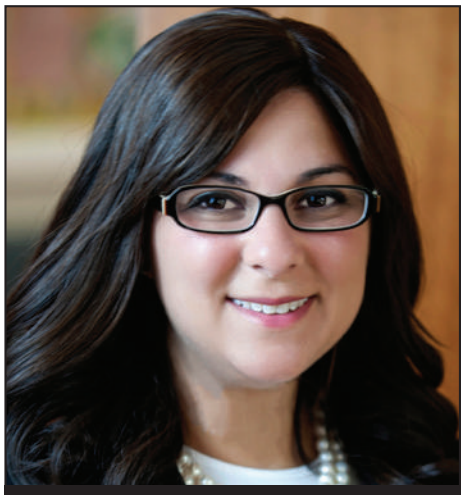
Connecticut Law Tribune
May 2, 2016 ctlawtribune.com An ALM Publication

Health Law

What's Hot in HIPAA Enforcement: A Year in Review

By MICHELLE DeBARGE and JODY ERDFARB


Michelle DeBarge


Jody Erdfarb

For entities that are required to comply with HIPAA, staying abreast of recent HIPAA developments is an essential risk management strategy. Given the complexity of the HIPAA regulations, the fast pace of technology development, and the austere ramifications of a violation, it may be difficult to decide how to best allocate compliance resources. Taking stock of recent and upcoming enforcement activity can help organizations prioritize.

OCR Enforcement Actions

Over the last several years, the Department of Health and Human Services Office for Civil Rights ("OCR") has steadily become more aggressive pursuing settlements and extracting higher settlement fines. This year in particular is shaping up to be OCR's most vigorous enforcement year to date. In the first four months of 2016, OCR has already entered into six settlement agreements to resolve alleged HIPAA violations – the same number of settlements it entered into for all of 2015.

During the last 12 months, OCR settled 10 cases for over $13.6 million. The risks associated with portable media continued to take center stage, with more than half of the OCR settlements over the last year involving stolen portable unencrypted electronic devices.

While not specifically involving portable media, compromised electronic protected health information was at the heart of another 2015 OCR settlement with the University Of Washington Medicine. On December 14, 2015, the University agreed to pay $750,000 and enter a two-year corrective action plan to settle an investigation triggered by a self-reported breach caused when an employee downloaded an email attachment that contained malicious malware. The breach affected 90,000 individuals.

Failure to obtain patient authorization was the focus of two additional OCR settlement agreements over the last year. On February 16, 2016, Complete P.T., Pool & Land Physical Therapy, Inc., a physical therapy practice located in the Los Angeles

The following chart shows the various types of entities with which OCR settled, the settlement amount and the portable media involved in those cases.

Date	Name	Organization Type	Settlement	Portable Media
July 10, 2015	St. Elizabeth's Medical Center	Tertiary care hospital	$218,400 and one-year corrective action plan	USB flash drive and laptop
August 21, 2015	Cancer Care Group, P.C	Private 13-member radiation oncology practice	$750,000 and three-year corrective action plan	Backup media
November 24, 2015	Lahey Hospital and Medical Center	Teaching hospital affiliated with Tufts Medical School	$850,000 and two-year corrective action plan	Laptop that operated a portable computerized tomography scanner
March 16, 2016	North Memorial Health Care	Health care system	$1,550,000 and two-year corrective action plan	Laptop
March 17, 2016	Feinstein Institute for Medical Research	Biomedical research institute	$3.9 million and a three-year corrective action plan	Laptop

area, agreed to pay $25,000 and enter into a three-year corrective action plan for allegedly disclosing the full names, photographic images, and testimonials of numerous patients on its public website without obtaining a HIPAA-compliant authorization from the individuals. And, most recently, on April 21, 2016, OCR announced a $2.2 million settlement with New York Presbyterian Hospital for what OCR termed as an "egregious disclosure" that occurred when a film crew for the ABC show "NY Med" recorded two patients without their authorization. In its press release, OCR stated that a patient who was dying, and another in significant distress, were both filmed even after a medical professional urged the crew to stop. The Hospital allegedly provided the production crew "unfettered" access to its health care facility. In response to this settlement agreement, OCR issued new guidance on the application of HIPAA in situations involving media access to protected health information.

Two recent settlements also emphasized the importance of entering into business associate agreements with vendors. In the North Memorial settlement--also listed in the above chart because it involved portable media stolen from an employee of a vendor--OCR discovered that North Memorial had not entered into a business associate agreement with the vendor who had access to the hospital's protected health information. Additionally, on April 14, 2016, Raleigh Orthopedic Clinic, a group practice that operates clinics and an orthopedic surgery center in North Carolina, agreed to pay $750,000 and enter into a two-year corrective action plan to settle charges that it failed to have in place a business associate agreement with a contractor that was engaged to transfer x-ray films and related protected health information to electronic media. OCR Director Jocelyn Samuels underscored the importance of business associate agreements by explaining that "HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise. . . .it is critical for entities to know to whom they are handing [protected health information] and to obtain assurances that the information will be protected."

Only one settlement over the last year involved an insurance company. On November 30, 2015, Triple-S Management Corporation agreed to pay $3.5 million and enter into a three-year corrective action plan. Based in San Juan, Puerto Rico, the insurance holding company reported at least five different breaches to OCR from 2010-2015 involving varied circumstances: failure to terminate the access rights of former employees who accessed protected health information of beneficiaries to benefit a competitor; failure to enter into a business associate agreement; misappropriation of a CD containing unencrypted protected health information; and disclosure of member IDs to the wrong beneficiaries.

In addition to these settlements, on January 13, 2016, a Department of Health and Human Services Administrative Law Judge (ALJ) affirmed OCR's imposition of civil monetary penalties against Lincare, Inc. Lincare, headquartered in Clearwater, Florida, is a provider of respiratory care, infusion therapy, and medical equipment to in-home patients, with 850 branch locations in 48 states. This was the second of only two OCR HIPAA enforcement actions that have been heard (and upheld) by an ALJ. The first was in 2011, involving Cignet Health's alleged failure to cooperate with OCR's investigation. In the Lincare case, the husband of a Lincare manager reported to OCR that his then estranged wife moved out and left protected health information of 278 individuals in their home. Lincare claimed that the husband had stolen the protected health information and that there was no HIPAA violation. The ALJ disagreed and upheld OCR's imposition of $239,800 in civil money penalties.

The FTC's Battle with LabMD

OCR is not the only federal agency making waves concerning the protection of healthcare information. The Federal Trade Commission (FTC), which has a long history of investigating and commencing enforcement actions against companies for failure to adequately protect consumer data, has forayed into OCR's enforcement territory. The FTC asserts that the failure to adequately protect consumer data is an unfair or deceptive trade practice in violation of Section 5 of the FTC Act. In two past cases, in 2009 and 2010, the FTC and OCR jointly entered into settlement agreements with large nationwide health care pharmacy chains for data breaches involving both protected health information and other personally identifiable sensitive data. Since that time, the FTC has revealed a burgeoning interest in pursuing data security cases involving entities subject to HIPAA and has pursued at least four different companies for fines.

In one such case, the FTC accused LabMD, a clinical laboratory, of failing to reasonably protect the security of consumers' personal data, including medical information. LabMD, a HIPAA-covered entity, challenged the FTC's authority to bring an enforcement action, claiming that OCR, not the FTC, has jurisdiction over LabMD. After a long legal battle that caused LabMD to close its operations, an ALJ ruled in favor of LabMD in November 2015. Although LabMD was unsuccessful in challenging the FTC's authority to bring an action against a HIPAA-covered entity for failure to meet certain security standards, the ALJ did find against the FTC on the merits. The ALJ concluded that the FTC "failed to carry its burden of proving its theory that [LabMD's] alleged failure to employ reasonable data security constitutes an unfair trade practice because [the FTC] has failed to prove . . . that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers." The FTC has recently appealed and continues to maintain that it has broad enforcement authority to pursue entities employing practices that it deems unfair and deceptive, including entities subject to HIPAA.

HIPAA Audits

The HITECH Act of 2009 for the first time required the federal government to periodically audit covered entities and business associates to ensure HIPAA compliance. In 2011 and 2012, OCR performed an initial round of 115 audits of covered entities. While rumors have been swirling for some time about additional audits, OCR finally announced that the second round of audits is underway. This new round of audits will cover both covered

entities and business associates and will cover a broad spectrum of entities in order to allow OCR to better assess HIPAA compliance across the industry. OCR initially will conduct only desk reviews, requiring entities to upload policies and procedures and other requested data, such as a list of business associates, via a secure online portal. OCR then plans to conduct a more limited number of onsite audits, where auditors will spend three to five days onsite, depending on the size of the entity. In connection with these audits, OCR also released an updated audit protocol, which reflects the 2013 Omnibus HIPAA Rule. The new protocol is 212 pages long and is much more detailed than its predecessor. OCR recommends that organizations use the audit protocol as a tool to conduct their own internal self-audits as part of their HIPAA compliance activities.

Lessons

While these recent cases and settlement agreements involve a multitude of noteworthy issues, certain themes are worth highlighting, especially in light of the looming new round of HIPAA audits. First, electronic portable devices pose a significant risk that must be ameliorated by the implementation of appropriate safeguards, such as encryption, training, and appropriate policies and procedures, including those addressing the removal and tracking of electronic media containing protected health information.

Second, OCR closely reviews breach notification reports to determine if further investigation is warranted. Entities reporting breaches, and any involved business associates, should be prepared for an OCR investigation, or even an inquiry from their local attorney general. Seven out of the ten OCR settlement agreements over the last 12 months involved self-reported breaches.

Third, size does not matter. Covered entities and business associates of every shape and size are vulnerable to investigation. The settlements over the last year involved a small 13-member physician group, a large company that provides in-home services in 48 different states, and companies of various sizes in between.

Finally, entities subject to HIPAA must remain vigilant in data security efforts. HIPAA requires the revision of policies, procedures, and security assessments "in response to environmental or operational changes affecting the security of electronic [protected health information]." Updating Security Rule risk assessments periodically to ensure that they reflect current threats and vulnerabilities and industry-wide best practices is of utmost importance. Be aware that while obtaining cyber insurance coverage is a prudent risk management measure, it cannot replace conducting a thorough risk assessment and adopting best practices when it comes to information security management. In a recent California lawsuit, Columbia Casualty Company sued its insured, Cottage Health System, a southern California hospital network. The insurer claimed it had no obligation under Cottage's cyber insurance policy to cover Cottage's losses because Cottage failed to implement critical information security policies. Mere "paper compliance," evidenced by written policies, procedures, and assessments that fail to reflect on-the-ground realities, will not suffice. In addition, HIPAA-covered entities and business associates should ensure compliance with the FTC's security expectations in addition to ensuring they are compliant with the HIPAA Security Rule.

Michelle DeBarge *is a Partner and* ***Jody Erdfarb*** *is an Associate in Wiggin and Dana's HIPAA Practice Group and can be reached at mdebarge@wiggin.com and jerdfarb@wiggin.com.* *For years, Wiggin and Dana's HIPAA Practice group has worked with noted health care providers, payers and clearinghouses – and vendors that provide IT (information technology), consulting and other services to these entities – employing their deep understanding of privacy, security and data exchange issues. Wiggin and Dana has also counseled local health information exchanges and RHIOS (regional health information organizations) on the complex array of regulatory and contracting matters applicable to those arrangements.*