Lowenstein Sandler

Client Alert / April 11, 2016

PRIVACY AND INFORMATION SECURITY PRACTICE |
HEALTH CARE LITIGATION, INVESTIGATIONS & COMPLIANCE GROUP | LIFE SCIENCES

BEWARE THE OCR

By: Mary J. Hildebrand, CIPP/US/EU, Esq., Maureen A. Ruane, Esq., Tara P. D'Orsi, Esq., and Cassandra M. Porter, Esq.

There are certain universal truths that we all can agree on, such as "Let a sleeping bear lie"; "Never poke an anaconda with a stick";[1] "Don't leave confidential health information in your car." We write to add a new universal truth to this list: "Don't ignore the OCR." Few of us will have the opportunity (or desire) to wake a sleeping bear or poke an anaconda with a stick. Yet under the new practices put into place by the Office of Civil Rights ("OCR") for the U.S. Department of Health and Human Services ("HHS"), many of us (or our clients) are likely to receive an inquiry concerning a possible violation of the Health Information Portability and Accountability Act of 1996 ("HIPAA"). Given the OCR's new protocols and based on recent developments, ignoring such an inquiry may well be the equivalent of poking an anaconda with a stick.

Until recently, this was not always the case. The OCR's authority to oversee and enforce HIPAA rules governing the privacy and security of patient information by "covered entities"[2] and their "business associates" began in the spring of 2003. Despite its decade-long power, the OCR's practice of oversight and enforcement has only recently taken on a renewed energy and focus. In 2013, HHS's Office of the Inspector General ("OIG") issued the first of three reports assessing the OCR's performance. The second and third OIG reports were issued in September 2015. In these reports, the OIG noted several deficiencies in the OCR's practices. Since the OIG issued its findings, the OCR has instituted a series of reforms in its approach to enforcing the Security, Privacy and Breach Notification Rules.

These OIG reports, combined with recent rulings upholding the OCR's authority to require covered entities to comply with HIPAA regulations (and levy substantial fines for failure to comply), demonstrate that the OCR has both the motivation and authority to fulfill its role as HIPAA "overseer." In light of these circumstances, we recommend that covered entities, business associates, and others subject to HIPAA regulations take this opportunity to revisit their compliance policies before they may receive an OCR letter.

Background

HIPAA required HHS to develop national standards for electronic health care transactions and code sets, unique health identifiers, and security protocols for the use, protection, and dissemination of patients' medical records and other protected health information ("PHI") maintained by covered entities. To satisfy these requirements, HHS published a series of rules and standards governing privacy[3] (the "Privacy Rule"), security[4] (the "Security Rule"), compliance with investigations[5] (the "Enforcement Rule"), and notifications in case of a breach of privacy or security[6] of PHI (the "Breach Notification Rule").

The Privacy Rule is intended to provide patients with access to their medical records and control over how their PHI is used and disclosed by a covered entity. This rule sets forth standards to protect the privacy of patients' medical records and other health information maintained by covered entities.

The Security Rule describes and establishes national, administrative, physical, and technical safeguards necessary to ensure the confidentiality, integrity, and availability of PHI, including electronic PHI.[7]

A breach of unsecured PHI is the unauthorized access or use of individually identifiable health information that was not first destroyed or otherwise rendered indecipherable.[3] The Breach Notification Rule requires that covered entities (which include doctors, pharmacies, and health insurance companies) make certain notifications when they discover a breach of unsecured PHI.

In November 2013, the OIG issued its first report[8] (the "Security Report"), in which it found that OCR "had limited assurance" that covered entities were complying with the Security Rule's protocols. The Security Report also found that OCR "missed opportunities" to encourage covered entities to strengthen electronic PHI security protocols. Among its recommendations, the OIG stated that OCR should conduct periodic

audits of covered entities to ensure their compliance with the Security Rule. Further, OIG found that OCR should take steps to ensure that sufficient controls are in place and that supervisory review of the investigations occurs.

Notably, OIG issued its report a few months before OCR imposed on Lincare Inc. ("Lincare"), a covered entity, a $239,800 civil monetary penalty[9] (more about the Lincare matter below).

In 2015, the OIG provided an overview of OCR's oversight and enforcement of HIPAA's Privacy Rule[10] ("Privacy Report") and Breach Notification Rule[11] (the "Breach Notification Report"). In each of these reports, the OIG found that OCR failed to review its investigation outcomes. Further, the reports found that OCR's staff did not maintain complete documentation of corrective actions that it required of covered entities to fulfill their respective HIPAA obligations. In its recommendations, the OIG suggested that OCR should implement an audit program and maintain complete documentation of corrective actions required of covered entities.

Why "Poking" the OCR Is a Bad Idea

In a recent ruling,[12] an administrative law judge upheld the civil monetary penalty OCR assessed against Lincare. Although OCR has been in charge of enforcing the Privacy and Security Rules for over a decade, this is only the second opinion that upholds OCR's authority to enforce HIPAA and impose a fine.[13] (In prior instances, companies settled with OCR and agreed to pay the fines.[14]) The Lincare example offers lessons and insights for us all.

Lincare operates hundreds of medical centers throughout the United States that provide respiratory care and medical equipment to patients at its facilities and through medical services delivered in-home. The spouse of a Lincare employee reported that he was able to access PHI and medical records left by his estranged wife in 2008 at their home. The OCR investigated the complaint and confirmed that Lincare patient PHI had been exposed. Moreover, Lincare did not have appropriate measures in place to protect the PHI. Further, even after Lincare was notified of the breach, it did not mitigate the issue or follow OCR's prescribed steps to rectify the deficiencies. In January 2014, OCR notified Lincare that it had violated the Privacy Rule and proposed a fine of $239,800. Lincare opposed OCR's decision and fine. In a January 2016 ruling, an administrative law judge upheld OCR's authority to enforce HIPAA regulations and impose a fine.

There are several takeaways from the Lincare investigation and the upholding of the subsequent fine. First, appropriate procedures for enforcing the Privacy Rule should be in place for all covered entities. Second, if OCR suggests a course of action, an entity should follow that suggestion as closely as possible.[15]

According to the OCR, Phase 2 of its HIPPA Privacy, Security and Breach Notification Audit Program is underway.[16] As of March 2016, reports of OCR fines for violating (and/or ignoring) HIPAA rules are becoming regular news. To date, about 30 organizations have agreed to sanctions after OCR determined that they were ignoring HIPAA.[17] Moreover, the fines imposed are escalating.[18] Further, at least 200 OCR audits are planned for 2016 alone. According to OCR, "[e]very covered entity and business associate is eligible for an audit."[19]

What Can a Covered Entity Do to Avoid Poking an Anaconda?

Given OCR's mandate to improve its oversight function, recent confirmation of its authority to issue civil monetary penalties for failure to comply with HIPAA, and increased funding as a result of civil monetary fines being enforced, covered entities should anticipate more oversight and a greater number of inquiries. This is an ideal time to review HIPAA compliance policies with staff, conduct internal "mock" audits, ensure that business associate agreements are in place and up to date, and revisit any open compliance issues.

Covered entities, business associates, and others subject to HIPAA compliance should consider this period an opportunity to review their compliance practices and policies to ensure that they are not (even unintentionally) poking the OCR with a stick.

Lowenstein Sandler is available to assist clients and friends as they consider, prepare for, and ultimately comply with the new HIPAA Privacy, Security, and Breach Notification Audit Program discussed in this alert. We will continue to monitor and report on developments relating to OCR's new initiative, as well as other legislative, regulatory, and industry developments that may be of importance to our clients and friends. Please contact any of the attorneys listed in this alert for further information on the matters discussed herein.

contacts

Please contact any of the attorneys named below for more information on this matter.

PRIVACY AND INFORMATION SECURITY PRACTICE

Mary J. Hildebrand, CIPP/US/EU, Esq.
973 597 6308
mhildebrand@lowenstein.com

Cassandra M. Porter, Esq.
646 414 6876
cporter@lowenstein.com

HEALTH CARE LITIGATION, INVESTIGATIONS & COMPLIANCE GROUP

Maureen A. Ruane, Esq.
212 419 5855; 973 597 6374
mruane@lowenstein.com

LIFE SCIENCES

Tara P. D'Orsi, Esq.
973 597 6202
tdorsi@lowenstein.com

[1] If you have any doubts about whether this is a wise action, please take a look at the videos on YouTube concerning this subject.

[2] The definition of "covered entities" includes health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with transactions defined in the regulations – in other words, most doctors, hospitals, pharmacies, and many other health care providers. See 45 CFR § 160.103.

[3] *See* 45 CFR § 164, subpt. E.

[4] *See* 45 CFR § 164, subpt. C.

[5] *See* 45 CFR §§ 160, subpts. C, D, and E.

[6] *See* 45 CFR §§ 164.400-414.

[7] The authority to administer and enforce the Security Rule was transferred to OCR on July 27, 2009.

[8] "The Office for Civil Rights Did Not Meet All Federal Requirements in Its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule," November 2013, A-04-11-05025.

[9] We don't know whether the proximity of the two events is a coincidence. In any event, we take all civil monetary penalties seriously, especially in amounts that trump the annual salary of most chief executive officers in the United States. Source: PayScale.com, Chief Executive Officer (CEO) Salary (United States) (the average salary for a chief executive officer in the United States is around $160,000 per year) (accessed March 25, 2016).

[10] "OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards," September 2015, OEI-09-10-00510.

[11] The Breach Notification Rule was established by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which was enacted as part of the American Recovery and Reinvestment Act of 2009, P.L. No. 111-5. 45 CFR pt. 164, subpt. D.

[12] *Director of the Office for Civil Rights v. Lincare, Inc.*, Docket No. C-14-1056, Decision No. CR4505, January 13, 2016.

[13] The prior instance involved Cignet Health of Prince George's County, Maryland ("Cignet"), where Cignet refused to cooperate with an OCR investigation. As a result, OCR imposed a civil penalty of $4.3 million for HIPAA violations, including violations of the Privacy Rule.

[14] *See* "Cignet Health Fined $4.3 Million for Privacy Violations" HealthData Management, Feb. 23, 2011.

[15] Third, covered entities may wish to review the Lincare situation with their employees. It's hard to predict if and when an employee's immediate family will be compelled to seek revenge. However, training employees to prevent unauthorized access to patient's PHI, even by trusted family members, may be the best offense in these situations.

[16] "OCR Launches Phase 2 of HIPAA Audit Program" (accessed March 25, 2016).

[17] Joseph Goedert, "HIPAA Violations Lead to $1.55 Million Fine of Hospital System" HealthData Management, March 17, 2016.

[18] As North Memorial Health Care of Minnesota learned when it was fined $1.55 million related to a business associate's laptop being stolen in 2011. *See* Resolution Agreement between U.S. Dept. of Health and Human Services and North Memorial Health Care. Again, all fines get our attention; however, a fine that is almost 10 times an average CEO's salary is particularly attention grabbing.

[19] See the "Who Will Be Audited?" section of the HIPAA Privacy, Security, and Breach Notification Audit Program, (accessed March 25, 2016).

© 2016 Lowenstein Sandler LLP.

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation.