POLSINELLI

in the news

Health Care

May 2016

Polsinelli HIPAA Audit Program

In this Issue:

Dear Clients and Friends,

As you are aware, HIPAA enforcement is on the rise. In 2015, the Office for Civil Rights ("OCR") – the agency charged with enforcing HIPAA – settled **6 cases** formally with penalty amounts ranging from **$125,000 to $3.5 million per settlement.** In 2016, OCR has already settled **5 additional cases** and successfully imposed **civil monetary penalties** in **1 case**, with penalty amounts ranging from **$25,000 to $3.9 million**.

Very shortly after announcing these costly settlements, OCR announced that it is commencing its formal and permanent Audit Program for HIPAA covered entities and business associates. If your organization received an email from OCR asking you to verify or update the organization's contact information, your organization has already been placed in the OCR's potential audit pool. Organizations that are covered entities under HIPAA may also be asked to provide OCR with a list of all of their business associates so that OCR can select its pool of business associates for the Audit Program.

Recently, OCR released the revised Audit Protocol, which lists the HIPAA requirements it will be focusing on during the audits. OCR will be assessing the compliance of covered entities and business associates against a number of HIPAA Privacy Rule requirements, Security Rule requirements and Breach Notification requirements. The OCR Audit Protocol can be found at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html.

We highly recommend that you review the revised Audit Protocol as OCR has indicated organizations selected for an audit will have to respond to an OCR initial document request within **10 business days** of receipt of the request. OCR has also stated that if the audit uncovers a serious compliance issue then it will conduct a more thorough compliance review.

Your organization may not be the subject of an OCR audit this year. However, it may be next year. If you wait until you receive notice of an audit from OCR to shore up your HIPAA policies and procedures, it may be too late.

Whether your organization is a covered entity or a business associate, now is the time to take a closer look at your organization's HIPAA compliance program and ask yourself – are you ready for an OCR audit? How are your HIPAA policies and procedures? Have you ever developed them? Can you find them? Will they pass an OCR review? Have you conducted and documented HIPAA security risk analyses to identify your risks and vulnerabilities and implemented risk management plans to reduce risk?

Even if your organization never receives a notice of an audit from OCR, reviewing and strengthening your HIPAA compliance program can help you to minimize the risk of patient complaints or costly data breaches by improving your HIPAA privacy and security policies, procedures and other compliance measures. The large OCR settlements have arisen from OCR investigations opened as a result of data breaches or patient complaints. **See attached summary of significant settlements.**

If enhancing your HIPAA compliance program is something you have been putting off, we highly recommend you make it this year's project so as to avoid being the next headline or big settlement. To help you tackle your HIPAA compliance issues and prepare for a potential audit, Polsinelli now offers (for a flat fee) a **HIPAA Audit Program** exclusively to its clients. After working with our team of attorneys (which includes a former in-house privacy attorney as well as a former OCR attorney who assisted in conducting OCR audits during the pilot phase), we will provide you with a **HIPAA Audit Binder** that will put you in a better position to respond to OCR within a short timeframe if the government should come knocking.

Here is a sample layout of the framework we use when conducting HIPAA privacy and security audits for our clients:

Phase 1:

A) Off-site, review of your organization's HIPAA privacy and security materials (BAAs (for organizations that are business associates, your sub-contractor BAAs), NPPs, privacy and security policies and procedures, risk analyses, etc.) in preparation for on-site audit.

B) On-site audit/mock OCR audit at your organization.

Phase 2:

A) Analysis and findings from Phase 1. We will identify any deficiencies, best practices, areas of risk, and make recommendations for changes and improvement.

B) Conference call with your compliance or legal team to discuss findings, recommendations, and prepare for Phase 3.

Phase 3:

Provide a formal report of audit findings and recommendations. Provide an educational in-service to your compliance team relating to the audit, areas of risk, recommendations for improvement, etc. The educational in-service may be presented in person or as a webinar.

To learn more about Polsinelli's **HIPAA Audit Program** or to set up a free 30 minute consultation with attorneys from our HIPAA Audit Team**,** please contact:

- Jason Lundy | jlundy@polsinelli.com,
- Katie Kenney | kdkenny@polsinelli.com,
- Lisa Acevedo | lacevedo@polsinelli.com,
- Erin Fleming Dunlap | edunlap@polsinelli.com,

or your Polsinelli attorney.

POLSINELLI

real challenges. real answers. SM

Performing a risk analysis is an essential step in protecting your organization from OCR scrutiny and multi-million dollar penalties. In some of the largest HIPAA settlements to date, OCR repeatedly cites to an entity's failure to conduct an accurate and thorough risk analysis in its decision:

Raleigh Orthopedic Clinic, PA, *April 2016* **(recent)**: Raleigh Orthopedic Clinic entered into a settlement of **$750,000** after it filed a breach report and OCR determined that Raleigh Orthopedic Clinic released x-ray films and related PHI of 17,300 patients to a vendor to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. OCR found that Raleigh Orthopedic Clinic had failed to execute a business associate agreement with the vendor prior to turning over the x-rays and PHI.

Feinstein Institute for Medical Research, *March 2016* **(*recent!*):** Feinstein Institute entered into a settlement of **$3.9 million** after it filed a breach report indicating that a laptop containing ePHI of approximately 13,000 patients and research participants was stolen from an employee's car. OCR found that Feinstein Institute lacked a sufficient security management process; lacked policies and procedures for authorizing access to ePHI; failed to implement safeguards to restrict access to unauthorized users; and lacked policies and procedures to govern the receipt and removal of laptops.

North Memorial Health Care of Minnesota, *March 2016* **(*recent!*):** North Memorial Health Care entered into a settlement of **$1.55 million** after it submitted a breach report indicating that an unencrypted, password-protected laptop was stolen from a business associate's locked vehicle, impacting the ePHI of 9,497 individuals. OCR found North Memorial failed to have a business associate agreement in place, **and failed to complete a risk analysis** to address all potential risks and vulnerabilities to ePHI.

Triple-S Management Corporation, *November 2015*: Triple-S entered into a settlement of **$3.5 million** after it self-reported widespread non-compliance across its subsidiaries. OCR found a **failure to conduct an accurate and thorough risk analysis;** failure to implement appropriate safeguards; impermissible disclosure of its beneficiaries' PHI to an outside vendor; and use or disclosure of more PHI than was necessary.

New York Presbyterian and Columbia University, *May 2014*: New York Presbyterian and Columbia University entered into a collective settlement of **$4.8 million** after a physician deactivated a server on the network containing ePHI, which caused the information to be accessible on internet search engines. OCR found that **neither entity had conducted an accurate and thorough risk analysis** or risk management plan; neither of the hospitals assured that the server was secure; and the entities failed to implement appropriate policies and procedures.

Concentra, *April 2014*: Concentra entered into settlements of **$1.72 million** after it reported that an unencrypted laptop was stolen from one of its facilities. OCR found that Concentra had previously recognized that lack of encryption was a critical risk; took incomplete and inconsistent efforts to encrypt; and failed to have sufficient security management processes in place to protect patient information.

Affinity Health Plan, *August 2013*: Affinity Health plan entered into a settlement of **$1.21 million** after it returned photocopiers to leasing agents which contained PHI of 344,589 individuals. OCR found that Affinity **failed to incorporate the ePHI stored on the photocopier in its analysis of risks and vulnerabilities**; failed to erase the data containing the copier hard drives; and failed to implement policies and procedures when returning the photocopier to its leasing agents.

WellPoint, Inc., *July 2013*: WellPoint, Inc. entered into a settlement of **$1.7 million** after WellPoint reported that a security weakness in its online application database left the ePHI of 612,402 individuals accessible to

POLSINELLI

real challenges. real answers. SM

unauthorized individuals over the internet. OCR found that WellPoint **failed to adequately implement policies and procedures for authorizing access to the database;** failed to perform an appropriate technical evaluation; and failed to have technical safeguards in place.

Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc., *September 2012*: Massachusetts Eye and Ear entered into a settlement of **$1.5 million** after it reported theft of an unencrypted personal laptop containing PHI**.** OCR found that Massachusetts Eye and Ear **failed to conduct a thorough risk analysis of the confidentiality of ePHI**; failed to have sufficient security measures; and failed to adequately adopt and implement appropriate policies and procures.

Accretive Health, *July 2012*: Accretive Health entered into a settlement of **$2.5 million** after an unencrypted laptop was stolen from the rental car of an employee. OCR found that Accretive violated federal security laws by failing to encrypt ePHI on laptops; failed to effectively train its workforce; and failed to identify and respond to the theft of PHI.

Alaska Department of Health and Social Services, *June 2012*: Alaska Department of Health and Social Services entered into a settlement of **$1.7 million** after it reported a theft of a portable electronic storage device (USB hard drive) potentially containing ePHI from the vehicle of an employee. OCR found that the Department **failed to complete a thorough risk analysis;** failed to implement sufficient risk management measures; failed to complete security training; and failed to implement device and media controls and encryption.

Blue Cross Blue Shield of Tennessee, *March 2012*: BCBST entered into a settlement of **$1.5 million** after it reported that 57 unencrypted computer hard drives containing PHI of over 1 million individuals had been stolen from a leased facility. OCR found that BCBST failed to implement appropriate administrative safeguards by not performing the required security evaluation, and failed to implement appropriate physical safeguards by not having adequate facility access controls.

Massachusetts General Hospital, *February 2011***:** Massachusetts General entered into a settlement of **$1 million** following an OCR investigation when a patient complained that the hospital lost his PHI. OCR found that Massachusetts General failed to develop and implement a comprehensive set of policies and procedures to ensure PHI is protected when removed from the premises.

For More Information

For questions regarding this information, to learn more about Polsinelli's **HIPAA Audit Program** or to set up a free 30 minute consultation with attorneys from our HIPAA Audit Team**,** please contact:

- Jason T. Lundy | 312.873.3604 | jlundy@polsinelli.com
- Kathleen D. Kenney | 312.463.6380 | kdkenney@polsinelli.com
- Lisa J. Acevedo | 312.643.6322 | lacevedo@polsinelli.com
- Erin Fleming Dunlap | 314.622.6661 | edunlap@polsinelli.com

To contact a member of our Health Care team, click here or visit our website at www.polsinelli.com > Services > Health Care Services > Related Professionals.

To learn more about our Health Care practice, click here or visit our website at www.polsinelli.com > Services > Health Care Services.

POLSINELLI

real challenges. real answers. SM

About Polsinelli's Health Care Practice

The Polsinelli Health Care practice represents one of the largest concentrations of health care attorneys and professionals in the nation. From the strength of its national platform, the firm advises clients on the full range of hospital-physician lifecycle and business issues confronting health care providers across the United States.

Recognized as a leader in health care law, Polsinelli is ranked as "Law Firm of the Year" in Health Care by *U.S. News & World Report* (November 2014), no. 1 by *Modern Healthcare* (June 2015) and nationally ranked by *Chambers USA* (May 2015). Polsinelli's attorneys work as a fully integrated practice to seamlessly partner with clients on the full gamut of issues. The firm's diverse mix of attorneys enables our team to provide counsel that aligns legal strategies with our clients' unique business objectives.

One of the fastest-growing health care practices in the nation, Polsinelli has established a team that includes former in-house counsel of national health care institutions, the Office of Inspector General (OIG), and former Assistant U.S. Attorneys with direct experience in health care fraud investigations. Our group also includes current and former leaders in organizations such as the American Hospital Association. Our strong Washington, D.C., presence allows us to keep the pulse of health care policy and regulatory matters. The team's vast experience in the business and delivery of health care allows our firm to provide clients a broad spectrum of health care law services.

About Polsinelli

real challenges. real answers.[SM]

Polsinelli is an Am Law 100 firm with more than 800 attorneys in 19 offices, serving corporations, institutions, and entrepreneurs nationally. Ranked in the top five percent of law firms for client service*, the firm has risen more than 100 spots in Am Law's annual firm ranking over the past six years. Polsinelli attorneys provide practical legal counsel infused with business insight, and focus on health care, financial services, real estate, intellectual property, mid-market corporate, and business litigation. Polsinelli attorneys have depth of experience in 100 service areas and 70 industries. The firm can be found online at www.polsinelli.com. Polsinelli PC. In California, Polsinelli LLP.

** 2016 BTI Client Service A-Team Report*

About this Publication

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. The choice of a lawyer is an important decision and should not be based solely upon advertisements.

Polsinelli PC. In California, Polsinelli LLP.

POLSINELLI

real challenges. real answers. SM