Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Learn 3 Important Lessons From HIPAA Breach At A Research Institution

Plus: Another breach prompts you to get a BA's signature before providing access to PHI.

If the latest big breach case tells you anything, you should see that breaches are increasingly leading to compliance investigations and that means more fines.

Case in point: On March 17, the **HHS Office for Civil Rights** (OCR) announced that **Feinstein Institute for Medical Research** has agreed to pay $3.9 million to settle potential HIPAA violations and will undertake a substantial corrective action plan (CAP) to bring its operations into compliance. Feinstein is a biomedical research institute and not-for-profit corporation, sponsored by **Northwell Health, Inc.** located in Manhasset, N.Y.

Back in September 2012, Feinstein filed a breach report alerting that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 13,000 patients and research participants was stolen from an employee's car. The ePHI included the research participants' names, birth dates, addresses, Social Security numbers, diagnoses, laboratory results, medications, and other medical information.

Following the breach notification, OCR launched an investigation that revealed that Feinstein's security management process was limited, incomplete, and insufficient to address potential vulnerabilities to ePHI. According to OCR, Feinstein also:

- Lacked policies and procedures for authorizing access to ePHI by its staff;
- Failed to implement safeguards to restrict access to unauthorized users;
- Lacked policies and procedures governing the receipt and removal of laptops that contain ePHI into and out of its facilities;
- Failed to implement proper mechanisms for safeguarding ePHI required under the Security Rule, specifically relating to electronic equipment procured outside its standard acquisition process.

Lessons learned: According to a March 30 analysis by attorney **Sam Barnes** of Seattle-based **Ogden Murphy Wallace Attorneys**, this breach case provides three lessons. First, HHS holds research institutes to the same standards as other covered entities (CEs). "To the extent a research institute maintains PHI, it is essential to develop adequate policies and procedures to protect the PHI," he noted.

Second, encrypting ePHI can greatly reduce liability, Barnes said. "Had Feinstein's laptop been encrypted to the NIST standard, Feinstein's ePHI would have been secured and Feinstein wouldn't have been required to report a breach." And not encrypting ePHI led to the OCR's investigation, which revealed multiple additional HIPAA violations.

Third, CEs and business associates (BAs) that choose not to encrypt must document why encryption is not reasonable nor appropriate, Barnes added. Like in this case, "failing to do so is a HIPAA violation" and subjects you to liability.

Link: To read more about the Feinstein breach case, go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/Feinstein/index.html.

OCR To Providers: Take A More Deliberate Approach To Identify BAs

Getting even a little lax on executing business associate agreements (BAAs) is a very costly mistake. And one healthcare provider is paying dearly for this mistake.

On March 16, the **HHS Office for Civil Rights** (OCR) announced a $1.55-million settlement and corrective action plan (CAP) with **North Memorial Health Care of Minnesota** to resolve charges of allegedly violating HIPAA by failing to execute a BAA with a major contractor. OCR also charged that North Memorial failed to institute an organization-wide risk analysis to address the risks and vulnerabilities of its protected health information (PHI).

Trend? With worrisome similarity to the Feinstein case, this settlement came about following a breach report. North Memorial filed the breach notification in September 2011, reporting that an unencrypted (but password-protected) laptop was stolen from the locked vehicle of a BA's staff member. The laptop contained the electronic PHI (ePHI) of nearly 9,500 individuals.

OCR initiated an investigation following the breach report. The OCR's investigation revealed that North Memorial failed to execute a BAA as required under the HIPAA Privacy and Security Rules with its BA **Accretive**. North Memorial also failed to complete a comprehensive risk analysis, OCR claimed.

OCR also found that North Memorial had provided Accretive access to the PHI of at least 289,904 patients before entering into a BAA with the vendor, according to a March 18 analysis by attorneys **Laurie Cohen** and **Valerie Breslin Montague** of **Nixon Peabody LLP**. "In fact, the parties did not execute a business associate agreement until almost a month after the breach occurred."

And although the breach originated with Accretive, "OCR held North Memorial responsible for the breach, concluding that North Memorial had failed to obtain 'reasonable assurances' that the vendor would safeguard the PHI to which it was given access,'" Cohen and Montague stated. Because the breach occurred prior to the 2013 regulations that implemented the Health Information Technology for Economic and Clinical Health Act's (HITECH) grant of authority to OCR to directly regulate BAs, OCR didn't pursue enforcement action against Accretive.

Takeaway: This settlement and CAP is particularly instructive for healthcare providers regarding BAAs, because many covered entities (CEs) take "a prophylactic approach" when managing their BAAs by sending such agreements to all of their vendors regardless of whether the vendors will have access to PHI, Cohen and Montague noted. "The North Memorial resolution agreement, however, suggests that OCR expects [CEs] to have a more deliberate process to assess who is and who is not a business associate."

Link: For more on the North Memorial settlement and CAP, go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/north-memorial-health-care/index.html.

Hacking Takes Top Prize For HIPAA Breaches In March

Healthcare providers, health plans, and business associates (BAs) reported 24 total breach incidents in March 2016, with one huge breach that affected millions of patients.

Of the 24 total, healthcare providers reported most of the breaches in March (21), while only two health plans and one BA reported breaches to the **HHS Office for Civil Rights** (OCR). Nine breaches involved hacking/IT incidents, followed closely by eight involving unauthorized access/disclosures. Theft (five) and loss (two) accounted for the remaining breaches.

By far the largest breach came from Florida-based healthcare provider **21st Century Oncology**, which reported a hacking/IT incident involving a network server that impacted more than 2.2 million individuals' protected health information (PHI). The incident underscores the shear damage that hackers can inflict on healthcare entities, as well as

the wide access to patient data hackers can gain when they access key network servers.

You can view all the reported large HIPAA breaches (affecting more than 500 individuals) at OCR's "Wall of Shame" at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.