Lost thumb drive leads to $150K fine

'An ounce of prevention is worth a pound of cure,' says chief HIPAA enforcer.

CONCORD, MA | December 30, 2013

An unencrypted USB drive has ended up costing one dermatology practice, which has settled with the Department of Health and Human Services for failing to address HITECH's breach notification provisions.

Adult & Pediatric Dermatology (known as APDerm), which provides dermatology services in Massachusetts and New Hampshire, agreed on a settlement of $150,000 for privacy and security violations, and will be required to put a corrective action plan in place to fix deficiencies in its HIPAA compliance program, according to a notice posted Dec. 26 on the HHS website.

It's the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the HITECH Act, say officicials from HHS' Office for Civil Rights.

OCR launched its investigation of APDerm after being tipped off that an unencrypted thumb drive containing the protected health information of some 2,200 people was stolen from a vehicle of one its staff members. The drive was never recovered.

The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of PHI as part of its security management process, officials say.

Moreover, APDerm failed to fully comply with the HITECH Breach Notification Rule, which requires organizations to have written policies and procedures in place and to train workforce members.

In addition to the $150,000 resolution amount, AP Derm's settlement includes a corrective action plan requiring development of a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities. The practice will also be required to provide an implementation report to OCR.

"As we say in healthcare, an ounce of prevention is worth a pound of cure," said OCR Director Leon Rodriguez, in a press statement. "That is what a good risk management process is all about – identifying and mitigating the risk before a bad thing happens. Covered entities of all sizes need to give priority to securing electronic protected health information."

4-year long HIPAA breach uncovered

Breach discovered in random health system audit

January 2, 2014

In the world of HIPAA privacy and security breaches, 2013 was a big year, and the last days of December proved no exception.

The five-hospital Riverside Health System in southeast Virginia announced earlier this week that close to 1,000 of its patients are being notified of a privacy breach that continued for four years.

From September 2009 through October 2013, a former Riverside employee inappropriately accessed the Social Security numbers and electronic medical records of 919 patients. Reportedly, the employee was a licensed practical nurse, according to a Daily Press account. The breach wasn't discovered until Nov. 1 following a random company audit.

"Riverside would like to apologize for this incident," said Riverside Spokesperson Peter Glagola, in a Dec. 29 notice. "We are truly sorry this happened. We have a robust compliance program and ongoing monitoring in place, and that's how we were able to identify this breach. We are looking at ways to improve our monitoring program with more automatic flags to protect our patients."

The practical nurse who inappropriately accessed the records has had their employment terminated, according to Riverside officials.

HIPAA covered entities and, more recently, business associates can be slapped with up to $50,000 fines per HIPAA violation due to willful neglect that goes uncorrected. Entities could face $10,000 per violation due to willful neglect when the violation is properly addressed.

Just this past month, the Department of Health and Human Services settled with Adult & Pediatric Dermatology of Concord, Mass., for $150,000 over alleged violation of HIPAA privacy, security and breach notification rules.

According to an HHS press release, an unencrypted thumb drive containing the protected health information of 2,200 individuals was stolen from an employee's car. However, when HHS' Office for Civil Rights conducted an investigation, it was discovered the practice had failed to conduct adequate risk analyses and did not comply with breach notification requirements.

When *Healthcare IT News* spoke with OCR Director Leon Rodriguez back in August about where HIPAA-covered entities most often make their biggest misstep, he pointed to risk analysis inadequacies, for business associates and covered entities alike. It's the "failure to perform a comprehensive, thorough risk analysis and then to apply the results of that analysis," he said.

2013 also brought with it some of the biggest HIPAA privacy and security breaches to date. Advocate Health Care, for example, reported the second largest HIPAA breach, compromising the PHI of more than 4 million individuals after four unencrypted laptops were stolen from one of its facilities back in July.

FOR IMMEDIATE RELEASE
May 7, 2014

Contact: HHS Press Office
(202) 690-6343

Data breach results in $4.8 million HIPAA settlements

Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center." NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing ePHI.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.

In addition to the impermissible disclosure of ePHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.

"When entities participate in joint compliance arrangements, they share the burden of addressing the risks to protected health information," said Christina Heide, Acting Deputy Director of Health Information Privacy for OCR. "Our cases against NYP and CU should remind health care organizations of the need to make data security central to how they manage their information systems."

NYP has paid OCR a monetary settlement of $3,300,000 and CU $1,500,000, with both entities agreeing to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing progress reports.

News

FOR IMMEDIATE RELEASE
August 14, 2013

Contact: Office of Civil Rights
(202) 619-0403

HHS settles with health plan in photocopier breach case

Under a settlement with the U.S. Department of Health and Human Services (HHS), Affinity Health Plan, Inc. will settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules for $1,215,780. Affinity Health Plan is a not-for-profit managed care plan serving the New York metropolitan area.

Affinity filed a breach report with the HHS Office for Civil Rights (OCR) on April 15, 2010, as required by the Health Information Technology for Economic and Clinical Health, or HITECH Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information. Affinity indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

Affinity estimated that up to 344,579 individuals may have been affected by this breach. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

"This settlement illustrates an important reminder about equipment designed to retain electronic information: Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent," said OCR Director Leon Rodriguez. "HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information."

In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all ePHI.