HIPAA Settlement May Herald New HHS Offensive

By Eric D. Fader, Day Pitney LLP

The U.S. Department of Health and Human Services announced on Dec. 26 that a Massachusetts-based dermatology practice will pay $150,000 to settle claims that it violated the privacy, security and breach notification rules of the Health Information Portability and Accountability Act of 1996.[1] Adult & Pediatric Dermatology PC (APDerm) thus became the first HIPAA-covered entity to be fined for failure to have policies and procedures in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act. This event may signal an expansion of HHS's campaign against those health care providers who, in HHS's view, may not be taking their HIPAA responsibilities seriously enough.

APDerm, based in Concord, Mass., has 12 physicians at four practice locations in Massachusetts and two in New Hampshire. HHS's Office for Civil Rights ("OCR") began investigating the practice after receiving a report that an unencrypted thumb drive containing the electronic protected health information ("ePHI") of about 2,200 patients had been stolen from the locked vehicle of one of its staff members. The thumb drive was never recovered.

There was no evidence of actual harm to any individual and it was not even clear that anyone's ePHI had actually been accessed. Further, APDerm had notified its patients and the media of the theft within 30 days after it occurred, as the breach notification rule requires. Nonetheless, upon its investigation, OCR determined that APDerm had not "conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process," and "did not fully comply with requirements of the breach notification rule to have in place written policies and procedures and train workforce members."

As part of the settlement, APDerm will be obligated to follow a corrective action plan that will require it to conduct a comprehensive risk analysis of the practice's security risks and the vulnerabilities to the ePHI it maintains; following the risk analysis, develop a risk management plan which must be reviewed and approved by OCR; implement and distribute any necessary revisions to APDerm's policies and procedures and then retrain all appropriate personnel; report to OCR any instances of noncompliance by APDerm's personnel with the privacy, security, and breach notification rules; submit an implementation report explaining how APDerm will comply with the above obligations; and retain all documents and records related to compliance with the corrective action plan for three years.

It appears, therefore, that the cost to APDerm in personnel and consultants' time and disruption to its practice, will be a significant increment to the amount of the monetary settlement. Although some of the requirements of the corrective action plan were things that APDerm should have done previously, or should have been doing on an ongoing basis, being required to implement numerous administrative changes under the time deadlines imposed by HHS certainly compounds the inconvenience to the practice.

The settlement with APDerm is the latest in a series of firsts and other similar events in HIPAA and HITECH Act enforcement over the past two years. In June 2012, the Alaska Department of Health and Social Services ("DHSS") paid a $1.7 million settlement to HHS in an incident with strong similarities to APDerm's occurrence. An unencrypted hard drive was stolen from the vehicle of a DHSS employee and, during the subsequent investigation, OCR determined that DHSS did not have adequate policies and

procedures in place to safeguard ePHI; had not completed a risk analysis or implemented sufficient risk management measures; and had not completed security training for its personnel. DHSS also did not have in place access controls to safeguard its hardware and portable devices. DHSS's settlement was OCR's first HIPAA enforcement action against a state agency.

In September 2012, Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (together, "MEEI") agreed to pay $1.5 million to HHS to settle alleged violations of the HIPAA security rule. After the theft of an unencrypted laptop containing the ePHI of MEEI patients and research subjects, OCR's investigation determined that MEEI, among other things, had failed to perform a proper risk analysis regarding the confidentiality of ePHI maintained on portable devices, and had not adopted and implemented policies and procedures regarding access to such ePHI and security incident identification, reporting and response.

In January 2013, in the first settlement involving a breach of unsecured ePHI that affected fewer than 500 patients, the Hospice of North Idaho agreed to pay the HHS $50,000 to settle potential violations of the HIPAA security rule after the theft of an unencrypted laptop. Again, OCR's investigation determined that a proper risk analysis had not been conducted, and that the required policies and procedures to address mobile device security were not in place.

In May 2013, Idaho State University ("ISU") agreed to pay a $400,000 settlement to HHS after the breach of unsecured ePHI of about 17,500 patients at an outpatient clinic. Firewall protections on ISU's servers had been accidentally disabled, leaving the patients' ePHI unsecured for at least 10 months. OCR's investigation determined that ISU's risk analyses and assessments of its clinics did not adequately identify potential risks and vulnerabilities and that ISU did not have proper security measures, policies and procedures in place.

In July 2013, the managed care company WellPoint Inc. agreed to pay a $1.7 million settlement to HHS after security weaknesses in an online application database left the ePHI of more than 600,000 individuals vulnerable to unauthorized access over the Internet. OCR's investigation revealed that WellPoint did not adequately implement policies and procedures for authorizing access to the database and did not have proper technical safeguards in place.

Finally, in August 2013, Affinity Health Plan Inc. agreed to a $1.2 million settlement with HHS after it was found to have returned leased photocopiers to their lessors without deleting unsecured ePHI that had been stored on the photocopiers' hard drives.

Although there have also been other types of HIPAA settlements in recent years, the above string of incidents illustrates HHS's focus on safeguarding unencrypted ePHI in various forms. All HIPAA-covered entities and business associates should now be on notice that HHS is targeting not only flagrant scofflaws, but also health care providers that may be in compliance with "most" of their responsibilities under HIPAA, HITECH and the regulations promulgated thereunder. A review of the facts of recent settlements suggests that HHS is also attempting to make examples of HIPAA and HITECH Act offenders in as wide a variety of scenarios as possible.

Of course, a medical practice that purchases a binder of HIPAA policies and procedures from an online vendor and puts it on the shelf, believing itself compliant and protected, could have a rude awakening if it does not properly train (and periodically retrain) its employees and then suffers a data breach. Forms, logs and agreements must be reviewed regularly and updated to reflect the practice's actual procedures whenever those are modified, and risk assessments must be performed and documented on a regular basis.

Each risk assessment should review all systems and devices in which the practice, its personnel, and its business associates maintain, or by which any of them transfer, ePHI. Any vulnerabilities discovered must be documented and corrected and personnel retrained as necessary. There must also be an incident response plan in place that sets forth necessary steps and procedures in the event of a data breach. Finally, all of the practice's relationships with its service providers should be analyzed to determine whether each service provider is a "business associate" under HIPAA, and business associate agreements with state-of-the-art language must be entered into with each.

Perhaps most importantly, properly encrypting all devices — particularly portable devices — that are used to store or transmit ePHI can convert an incident of unauthorized access, or the loss or theft of a device, from a reportable privacy and security breach into a benign event that need not be reported for HIPAA purposes. HHS refers health care providers to the National Institute of Standards and Technology's Guide to Storage Encryption Technologies for End User Devices for encryption processes to render ePHI unusable, unreadable or indecipherable.

***

Eric Fader is of counsel in Day Pitney's New York office where he has represented health care providers in connection with business planning and corporate governance issues, transactional matters and federal and state regulatory requirements for more than 25 years.

This article was first published in Law360 on January 29, 2014.
