CARLTON FIELDS

HIPAA - Lessons From the Fresenius Settlement

HEALTH CARE | HEALTH CARE | CYBERSECURITY AND PRIVACY | MARCH 30, 2018

Patricia S. Calhoun

In an industry overrun with news of almost daily privacy breaches, what makes the Fresenius settlement especially newsworthy is the size of the fine compared to the size of the breach and the types of breaches involved.

On February 1, it was announced that Fresenius Medical Care North America (Fresenius) had agreed to pay $3.5 million and enter into a comprehensive corrective action plan for potential violations of the Health Insurance Portability and Accountability Act (HIPAA). Fresenius, a large network of dialysis facilities, cardiac and vascular labs, and urgent care centers, reported five relatively small uncomplicated breaches at five different facilities involving the protected information of a total of 521 patients.

- The Duval Facility in Florida suffered a break-in and two desktop computers were stolen, one of which contained the electronic protected health information (ePHI) of 200 patients.
- At the Magnolia Grove Facility in Alabama, an unencrypted USB drive was stolen from a workforce member's car. The USB drive contained the ePHI of 245 patients
- At the Ak-Chin Facility in Arizona, the compliance line received an anonymous call that a hard drive was missing from a desktop computer that had been taken out of service. The hard drive contained the ePHI of 35 persons. The incident was reported to a local manager but not to the Fresenius corporate department.
- At the Augusta Facility in Georgia, an unencrypted laptop was stolen from a workforce member's car. The laptop had the ePHI of 10 persons.
- The Blue Island Facility in Illinois also suffered a break-in and three desktop computers and one encrypted laptop was stolen. One of the desktops contained the ePHI of 31 persons.

So, how did the fact that five different facilities got robbed end up costing Fresenius $3.5 million?

Certainly, the fact that all five incidents occurred during one calendar year within a large organization was a factor. The Director of the Department of Health and Human Services Office for Civil Rights (OCR), Roger Severino, stated in a February 1 press release that the "number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprise-wide risk analysis for a covered entity."

In addition, the press release makes it clear that the OCR took a hard look at Fresenius's policies. Director Severino stated that "covered entities must take a thorough look at their internal policies and procedures to ensure they are protecting their patients' health information in accordance with the law." The OCR investigation found that the AK-Chin facility failed to implement policies to address security incidents, that the Magnolia Grove facility failed to implement policies that govern the receipt and removal of hardware and electronic media in and out of the facility, and that the Duval and Blue Island facilities failed to implement policies to safeguard their facilities and equipment from unauthorized access, tampering, and theft.

The corrective action plan (CAP) provides further evidence that the OCR is focused on policies. In the CAP, in addition to conducting a risk analysis, developing an encryption report, and updating its training program, Fresenius agreed to the following:

- To develop a written risk management plan;
- To develop a written process to regularly evaluate any environmental or operational changes that affect the security of ePHI;
- To review and revise policies and procedures related to the receipt, removal, and movement of electronic devices and media;
- To review and revise policies and procedures to limit physical access to all electronic information systems and the facilities

while ensuring that properly authorized access is allowed; and

- To develop a facility security plan that documents efforts to safeguard the facilities from unauthorized physical access, tampering and theft.

And finally, the OCR focused on encryption; three of the stolen devices were unencrypted devices. In the CAP the OCR requires that Fresenius produce an encryption report that identifies the total number of devices and equipment, the number of devices that are encrypted, and a description of the plan to encrypt the devices or an explanation for why encrypting the device is not reasonable and appropriate.

HIPAA lessons learned:

1. **Enterprise-wide risk assessment.** If your facility is part of a larger whole, it is time to ensure that there is an overall HIPAA policy and that you perform an enterprise-wide HIPAA risk assessment.
2. **Policies.** Review your policies to ensure they are up-to-date and all-inclusive. Check to see if there is one dealing with movement of protected health information (PHI) and electronic devices in and out of the facility; a policy that addresses environmental and operational changes that affect PHI, a policy regarding physical safety and the threat of theft, a policy regarding encryption, and one addressing security incidents. (Interestingly, the AK-Chin facility was cited for failing to implement policies to address security incidents, despite the fact that a security incident was not involved in the breach.)
3. **Encryption.** Review the implementation of encryption at your facility. Although the CAP language gives Fresenius an opportunity to explain why all devices are not encrypted, it seems likely that only an extreme situation will be an acceptable reason not to encrypt. It appears clear that the OCR expects that all mobile devices housing PHI be encrypted.

HIPAA privacy and security officers should take note and review and update their plans accordingly.