Published on *The National Law Review* https://natlawreview.com

CardioNet Settlement Shows Need for Healthcare Providers to Secure Mobile Devices

Article By:

Kim C. Stanger

C. Matt Sorensen

In the first Health Insurance Portability and Accountability Act ("HIPAA") settlement involving a wireless health services provider, CardioNet on April 24 agreed to pay $2.5 million for allegedly losing a laptop containing individual health information.

The size of this and other recent settlements demonstrates the increasingly active stance being taken by the Department of Health and Human Services Office for Civil Rights ("OCR") on the need for organizations to implement strong, HIPAA-compliant security policies – including those involving mobile devices used for work. The settlement was based on the impermissible disclosure of unsecured electronic protected health information ("ePHI").

Pennsylvania-based CardioNet provides remote mobile monitoring and rapid response to patients at risk for cardiac arrhythmias. In 2012, the company reported to OCR that a workforce member's unencrypted laptop had been stolen from a parked vehicle outside the employee's home. The laptop contained the ePHI of 1,391 individuals.

Encryption Can Help

OCR's investigation revealed that, at the time of the theft, CardioNet lacked sufficient risk analysis and risk management. In addition, the company's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented.

Breaches such as this can be prevented by the use of encryption. If an encrypted device containing ePHI is lost or stolen, the incident does not need to be reported to OCR and patients do not need to be notified. Most importantly, patients' ePHI will not be exposed if devices are lost or stolen. While encryption is not cheap, it is much less expensive than an OCR fine.

In addition to the fine, CardioNet agreed to adopt a corrective action plan requiring it to conduct a risk analysis, develop and implement a risk-management plan, revise its employee training program, and implement secure device and media controls.

A “Watershed Year”

In the past year, healthcare entities have seen a dramatic increase in HIPAA enforcement – and the related costs. CardioNet marks the seventh multi-million-dollar settlement with OCR in the last year – including a $5.5 million settlement with Memorial Healthcare System in February, a $2.14 million settlement with St. Joseph Health in October, a $5.5 million settlement with Advocate Healthcare in August, and $2.7 million settlements with Oregon Health & Science University and the University of Mississippi Medical Center in July.

And it is unlikely that this trend will change. A recent study issued by Navigant Global Technology Solutions indicates that 2017 is shaping up to be another “watershed year” for cybersecurity threats and attacks. Last year, healthcare accounted for by far the largest percentage of reported breaches – 42.7 percent.

This report suggests that organizations of all sizes partner with outside consultants and experts to ensure that all requirements are met and routinely audited. These actions include:

- Establish a cybersecurity program;
- Adopt a cybersecurity policy;
- Identify and install a chief information security officer;
- Establish a policy and process to assess vendor cybersecurity; and
- Conduct an annual risk assessment to include penetration testing.

National Law Review, Volume VII, Number 118