



## \$2.5 Million Settlement Reached as HIPAA Crackdown Continues on Unsecured Portable Devices

### IN SHORT

**The Situation:** The U.S. Department of Health and Human Services has announced a \$2.5 million settlement relating to a health care provider's alleged HIPAA violations in connection with an employee's stolen laptop.

**The Implication:** The settlement indicates that the federal government will continue aggressive enforcement actions against providers failing to comply with HIPAA when using digital media and portable devices.

**Looking Ahead:** Digital health vendors and their health care providers should review their current policies regarding portable devices and run regular risk analyses to ensure compliance.

A recent settlement of \$2.5 million for alleged violations of the Health Insurance Portability and Accountability Act ("HIPAA") continues a trend of government enforcement targeting health care providers and vendors that fail to comply with HIPAA when using digital media and devices. The settlement should be seen as a warning for digital health companies in particular to review their policies and procedures regarding HIPAA security compliance for mobile applications, devices, and platforms.

#### Background

On April 24, 2017, the U.S. Department of Health and Human Services, Office of Civil Rights ("OCR") [announced](#) a \$2.5 million settlement for alleged HIPAA violations in connection with a laptop stolen from a parked vehicle outside an employee's home. The settlement was reached with CardioNet, Inc., a provider of remote mobile monitoring services, following CardioNet's disclosure of multiple breaches in 2012 of unsecured electronic protected health information ("ePHI") affecting more than 1,300 and 2,200 people, respectively, both of which [appear](#) to involve stolen laptops.

#### OCR's Findings

While initiating an investigation in response to CardioNet's disclosure of the breaches, OCR discovered more systemic violations of HIPAA's security rules. The settlement agreement [alleges](#) that CardioNet had failed to: (i) implement processes to prevent, detect, contain, and correct security violations; (ii) implement policies and procedures governing the receipt and removal of hardware and electronic media containing ePHI into and out of its facilities, the encryption of such media, and the movement of these items within its facilities until years after initially reporting the breaches; and (iii) safeguard against impermissible disclosures of PHI by its employees or take sufficient steps to immediately correct the disclosure. OCR's announcement accompanying the settlement clarified that CardioNet's HIPAA security policies and procedures were only in draft form and had not been implemented, including policies for safeguarding ePHI and mobile devices.



The settlement should be seen as a warning for digital health companies.



#### Terms of CardioNet's Corrective Action Plan

As part of the settlement agreement, CardioNet agreed to a corrective action plan that requires CardioNet to:

- Conduct a risk analysis of the security risks and vulnerabilities that incorporates its current facilities and electronic equipment, data systems, and applications. CardioNet is required to review and update the analysis annually and more frequently, if appropriate.
- Develop and implement an organization-wide risk management plan to address and mitigate any security risks and vulnerabilities found in the risk analysis.
- Review and revise its HIPAA security rule policies and procedures, with a specific focus on device and media controls.
- Review and revise its HIPAA security rule training program, including ensuring it includes a focus on security, encryption, and handling of mobile devices and out-of-office transmissions.

Should CardioNet fail to comply with the corrective action plan, the settlement agreement allows OCR potentially to proceed with the imposition of civil monetary penalties for violations discovered through OCR's investigation of the breaches and for any other violations of HIPAA it may find.

**Impact of Settlement on Digital Health Providers and Vendors**

While CardioNet is identified as a covered entity, this settlement should be a warning to business associates as well, including in particular vendors operating in the growing digital health market. Just last year, OCR [targeted](#) a business associate for the first time, reaching a \$650,000 settlement based on similar facts where a lost mobile device with unsecured ePHI led OCR to discover the company lacked policies on the removal of mobile devices containing PHI from its facility or for handling security incidents.

In OCR's announcement of the CardioNet settlement, it specifically noted that "[m]obile devices in the health care sector remain particularly vulnerable to theft and loss." It warned that a failure to implement mobile device security puts individuals' sensitive health information at risk, potentially leaving individuals unprotected. Therefore, these settlements represent an ongoing trend of the type of HIPAA violations that are getting OCR's attention.

Digital health vendors and their client health care providers should ensure that they are conducting periodic risk analyses and implementing policies and training programs that address their specific digital health privacy and security risks, particularly with respect to their mobile devices and platforms.

**The CardioNet Settlement**



**\$2.5 Million**  
– and –  
**Corrective Action Plan**

- ✓ Analysis of security risks and vulnerabilities
- ✓ Implementation of risk management plan
- ✓ Review/revision of HIPAA security procedures focusing on device controls
- ✓ Review/revision of HIPAA security rule training

**THREE KEY TAKEAWAYS**

1. Beyond the incidents involving the stolen laptops, an investigation uncovered CardioNet's systemic violations of HIPAA security regulations.
2. In addition to the \$2.5 million payment, the company is required to engage in a specific Corrective Action Plan.
3. Digital health vendors and their health care providers should take note that these types of violations will continue to attract the attention of enforcement agencies.

**CONTACTS**

-  Alexis S. Gilroy  
Washington
-  J. Todd Kennard  
Columbus
-  Kevin D. Lyles  
Columbus
-  David E. Kopans  
Columbus

**YOU MIGHT BE INTERESTED IN:** [Go To All Recommendations >>](#)

Data Breach Risks for 401(k) and Retirement	New Mexico On the Brink of Passing Data Breach	ePrivacy— European Commission Tries to Catch	Digital Health Law Update, Vol. II, Issue 5
---	--	--	---

Notification  
Law

Up with the  
Evolution  
of Modern  
Communication  
Technologies

---

SUBSCRIBE

SUBSCRIBE TO RSS



---

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide<sup>SM</sup>.

**Disclaimer:** Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at [www.jonesday.com](http://www.jonesday.com). The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2017 Jones Day. All rights reserved. 51 Louisiana Avenue, N.W., Washington D.C. 20001-2113