HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

April 2013

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Why are so many DLA Piper employees certified in compliance?

See page 16

This article, published in *Compliance Today*, appears here with permission from the Health Care Compliance Association. Call HCCA at 888-580-8373 with reprint requests.

by Shannon Hartsfield Salimone

First settlement for a smaller HIPAA breach

» HIPAA penalties are not reserved for large breaches.
» Addressing a breach quickly won't insulate an organization from penalties.
» A breach gives OCR the opportunity to uncover other problems.
» Even smaller covered entities will be held accountable.
» Companies should look for gaps in current compliance plans.

Shannon Hartsfield Salimone *(Shannon.salimone@hklaw.com) is a Partner in the Tallahassee office of Holland & Knight LLP, where she is the Regulatory and Litigation Leader of the firm's Health Care & Life Sciences Team and Co-chair of the Data Privacy and Security Team.*

Data breaches do not have to be extremely large to result in significant financial penalties. On January 2, 2013, the Department of Health and Human Services (HHS) kicked off the new year by announcing the very first HIPAA breach settlement involving fewer than 500 individuals. Hospice of North Idaho (HONI), an independent, non-profit agency, had a laptop stolen in June of 2010. The laptop, which was unencrypted, contained electronic information on 441 patients. HONI reported the breach to the HHS Office for Civil Rights (OCR) as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act.


Salimone

It appears that, once the theft occurred, HONI followed the notification requirements in the HITECH Act interim final rules regarding breach notification. In a press release[1] issued on December 27, 2012, HONI reported that, upon learning of the theft, it began a risk assessment and development of a corrective action plan immediately. It received no indication that any information was accessed. HONI contacted the patients who could have been affected and offered credit monitoring. Additionally, HONI offered families of deceased patients support through the assignment of a personal recovery advocate. The company hired industry experts in the areas of Information Technology and Human Resources, replacing the outsourced services employed during the time of the laptop theft. The hospice took several other measures, such as conducting a risk analysis and increasing security measures on its equipment, including encrypting all laptops and developing stronger password enforcement. In addition, the hospice adopted stronger security policies and procedures, and implemented a schedule of continuing privacy and security training.

In its press release, HONI asserts that it is currently in compliance with all federal regulations. HONI Vice President Kim Ransier stated, "We realize that we must adhere to these regulations while continuing to provide the highest quality care for our patients and not lose sight of our mission."

Covered entities are at risk

Although the hospice took a number of measures to address the breach, the settlement announcement makes it clear that even a rapid and detailed response to a security incident

will not necessarily insulate a covered entity from enforcement actions. As with other HITECH Act-related settlements, it appears that, while the breach report triggered the investigation, the violations that OCR subsequently identified, rather than the breach itself, resulted in the financial settlement. The breach report provided the opportunity for OCR to take a close look at the covered entity's HIPAA compliance efforts. OCR found deficiencies in the HIPAA compliance program, which could have resulted in civil money penalties. Instead, the parties elected to settle the matter. Specifically, OCR found that the hospice had not conducted a risk analysis to safeguard electronic protected health information. Additionally, the entity lacked policies and procedures to address mobile security devices.

…even a rapid and detailed response to a security incident will not necessarily insulate a covered entity from enforcement actions.

In the HHS statement announcing the settlement, OCR Director Leon Rodriguez stated, "This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information." He also observed that "Encryption is an easy method for making lost information unusable, unreadable and indecipherable."

Fortunately, compliance officers have myriad resources that can help prevent breaches and their resulting penalties. For example, on December 12, 2012, HHS launched a new online educational initiative called "Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information" (available at www.HealthIT.gov/mobiledevices).[2] Through this website, OCR and the HHS Office of the National Coordinator for Health Information Technology provide videos, frequently asked questions, articles, and other resources addressing security of patient information on mobile devices.

The HONI breach settlement is the first one involving less than 500 patients, but it will not be the last. It is critical that health care entities and their business associates conduct accurate and thorough risk analyses to try to anticipate threats to information security and protect against those hazards. Additionally, compliance officers should re-examine their HIPAA compliance plans to ensure that they contain robust policies regarding mobile devices. Sufficient effort on the front end will reduce the chances that a company will find itself as the subject of a future HHS settlement.

The breach report provided the opportunity for OCR to take a close look at the covered entity's HIPAA compliance efforts.

1. Dept of Health and Human Services, press release: "HHS announces first HIPAA breach settlement involving less than 500 patients." January 2, 2013. Available at http://www.hhs.gov/news/press/2013pres/01/20130102a.html
2. Dept of Health and Human Services, press release: "New tools to help providers protect patient data in mobile devices." December 12, 2012. Available at http://www.hhs.gov/news/press/2012pres/12/20121212a.html