January 14, 2013

## New Year, Same Old Security Issues

By Amy M. Joseph

On January 2, the Department of Health and Human Services (HHS) released a statement announcing the first HIPAA breach settlement involving less than 500 patients.[1] According to the press release, the Hospice of North Idaho (HONI) reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients was stolen in June of 2010. Over the course of the investigation, the Office for Civil Rights ("OCR") learned that HONI was not in compliance with requirements of the HIPAA Security Rule. HONI had not conducted a risk analysis to safeguard ePHI and also did not have policies and procedures in place to address mobile device security. HONI settled the potential HIPAA violations for $50,000.[2]

In the press release, OCR Director Leon Rodriguez states:

> 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. . . . Encryption is an easy method for making lost information unusable, unreadable and undecipherable.

This settlement follows a $1.5 million settlement in September 2012 involving a stolen laptop with unencrypted information, as described further at http://health-law.com/wp-content/uploads/2012/09/HIPAA_eAlert-Stolen_Laptop_9-12.pdf

Unfortunately, these two settlements are not the only recent examples in the press involving the theft of unsecured electronic devices containing ePHI. On November 20, 2012, Omnicell, a vendor that provides automated medication dispensing services, notified providers in multiple states that an unsecured electronic device containing ePHI was stolen from an Omnicell employee's car.[3] According to the Sentara Healthcare website, Omnicell mailed letters on December 31, 2012 to affected patients. And on December 26, 2012, Gibson General Hospital is reported to have mailed letters to approximately 29,000 patients regarding the theft of an unencrypted hospital laptop containing ePHI. The laptop was stolen from an employee's home during a burglary in late November, and has not yet been recovered.[4]

These recent incidents serve as a reminder of the importance of having policies and procedures in place to address mobile device security, as well as the importance of providing adequate training to a provider's workforce on the topic. The incidents also illustrate the risk of using

laptops to store unencrypted health information, as each of these scenarios could have been easily avoided if the electronic devices had been encrypted.  HHS provides guidance on remote use on its website, including guidance on security measures for laptops and other portable media that can be viewed at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html


*For additional information, please contact attorneys Hope Levy-Biehl, Karl Schmitz or Amy Joseph in Los Angeles at 310.551.8111; Paul Smith or Stephen Phillips  in San Francisco at 415.875.8500; Jennifer Hansen in San Diego at 619.744.7300; or Robert Roth or Kelly Lavin, (Director of Government Relations & Public Policy-a non-attorney professional)   in Washington D.C. at 202.580.7700.*

---

[1] *See* http://www.hhs.gov/news/press/2013pres/01/20130102a.html.

[2] HONI did not admit to liability as part of the settlement agreement.  *See* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf.

[3] *See* http://www.sentara.com/News/NewsArchives/2012ARchive/Pages/Privacy-Notice-for-Sentara-Healthcare-Patients.aspx; http://www.freep.com/article/20121221/NEWS05/121221077/University-of-Michigan-Health-System-Omnicell-patient-information-stolen.

[4] *See* http://www.tristate-media.com/drr/news/local_news/article_0fc959e4-5127-11e2-85a8-0019bb2963f4.html.