JONES WALKER

e*bulletin

HEALTH CARE

January 2013 Vol. 15 healthcare@joneswalker.com

DHHS SETTLES FIRST HIPAA BREACH INVOLVING FEWER THAN 500 INDIVIDUALS

According to a U.S. Department of Health and Human Services ("DHHS") news release, dated January 2, 2013, Hospice of North Idaho ("HONI") has agreed to pay DHHS, Office of Civil Rights ("OCR") $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule. Significantly, this is the first settlement with DHHS involving a breach of unprotected electronic protected health information ("ePHI") affecting fewer than 500 individuals.

The June 2010 incident leading to the settlement involved the theft of a laptop, which, according to the news release, was unencrypted and contained the ePHI of 441 individuals. The news release indicated that HONI routinely used unencrypted laptops as part of its hospice field work. The Resolution Agreement between DHHS and HONI, discussed in greater detail below, stated that HONI reported the theft of the laptop to OCR on February 16, 2011[1], and on July 22, 2011, OCR notified HONI of OCR's investigation regarding HONI's compliance with HIPAA's Privacy, Security, and Breach Notification Rules.

Over the course of the investigation, according to the news release, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI and did not have in place policies and procedures to address mobile device security as required by the HIPAA Security Rule. More specifically, according to the Resolution Agreement, OCR's investigation found that during certain time periods, HONI had not conducted an accurate and thorough analysis of the risk to the confidentiality of ePHI on an on-going basis as part of its security management process. In particular, OCR found that HONI did not evaluate the likelihood and impact of potential risks to the confidentiality of ePHI maintained in and transmitted using portable devices, implement appropriate security measures to address such potential risks, document the chosen security measures and the rationale for adopting those measures, and maintain on an on-going basis reasonable and appropriate security measures. In addition, OCR found that during certain time periods, HONI did not adequately adopt or implement security measures sufficient to ensure the confidentiality of ePHI that it created, maintained, and transmitted using portable devices to a reasonable and appropriate level. The Resolution Agreement notes that the Agreement is not an admission of any liability by HONI.

In addition to paying $50,000, HONI entered into a Corrective Action Plan ("CAP"). The CAP requires, among other things, that for a two-year period, HONI must, upon receiving information that a workforce member may have failed to comply with HONI's Privacy and Security policies and procedures, promptly investigate the matter. If HONI, after its review and investigation, determines that a member of its workforce has failed to comply with its Privacy and Security policies and procedures, HONI must notify DHHS in writing within 30 days. The notification must not only include a complete description of the event, including the relevant facts, the persons involved, and the provision(s) of HONI's

[1] Federal HIPAA Privacy and Security regulations at 45 C.F.R. §164.408 provide that a covered entity must, following the discovery of a breach of unsecured PHI, notify the Secretary of DHHS. For breaches of unsecured PHI involving 500 or more individuals, a covered entity must, among other things (and with certain exceptions), provide to the Secretary the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach (as set forth in 45 C.F.R. §164.404). For breaches of unsecured PHI involving less than 500 individuals, a covered entity must, among other things, maintain a log or other documentation of such breaches and, no later than 60 days after the end of each calendar year, provide the notification for breaches occurring during the preceding calendar year.

JONES WALKER

e*bulletin

HEALTH CARE

January 2013 Vol. 15 healthcare@joneswalker.com

Privacy and Security policies and procedures implicated, but it must also include a description of the actions taken and any further steps HONI plans to take to address the matter, to mitigate any harm, and to prevent it from recurring, including the application of appropriate sanctions against workforce members who failed to comply with its Privacy and Security policies and procedures.

The news release stated that since the June 2010 theft, HONI has "taken extensive additional steps to improve their HIPAA Privacy and Security compliance program." HONI itself issued a press release, dated December 27, 2012, in which it noted that, upon report of the theft, it "immediately began a risk assessment and development of a corrective action plan," which included "taking precautionary steps in the event the information was used maliciously," such as identifying and contacting patients who could have been affected by the incident and offering them credit monitoring. In addition, HONI "hired industry experts in the areas of Information Technology and Human Resources, replacing the outsourced services employed during the time of the laptop theft."

In addition, according to HONI's press release, HONI "conducted a thorough risk analysis as a part of its security process, increased security measures on all equipment containing patient information and adopted stronger security policies and procedures to insure the safety of patient health information. Other measures taken were the encryption of all laptops, stronger password enforcement, and HIPAA privacy and security training on a scheduled basis." Further, the press release noted, among other things, that HONI is conducting ongoing education and staff training on a regular basis.

In discussing this incident, DHHS' news release quoted OCR Director Leon Rodriguez, who stated that "[t]his 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." In addition, the news release referred to a new educational initiative titled, "Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information," which was released by OCR and the HHS Office of the National Coordinator for Health Information Technology ("ONC") (available here). The educational initiative provides health care providers and organizations with tips on ways to protect health information when using mobile devices such as laptops, tablets, and smartphones. For example, one webpage discusses how to protect and secure health information when using a mobile device, and includes tips such as using a password or other user authentication, installing and enabling encryption, installing and activating remote wiping and/or remote disabling, and disabling and not installing sharing applications.

As the HONI settlement demonstrates, it is imperative that providers timely and diligently conduct thorough risk assessments that identify threats and vulnerabilities and compare current measures and processes to what is required and recommended to adequately safeguard health information. Jones Walker can not only assist with conducting such risk assessments, but can also assist in analyzing the results of the assessments and in developing action plans to improve the effectiveness of the providers' processes and controls, to help mitigate any identified risks and vulnerabilities, and to facilitate providers' compliance with federal privacy and security laws and regulations. As we have noted in prior E*Bulletins, effective action plans may include revisions to current policies and procedures, as well as training work force personnel utilizing such tools as analyzing real-life instances of HIPAA breaches, and preparing interactive in-services and customized training sessions.

JONES WALKER

e*bulletin

HEALTH CARE

January 2013 Vol. 15 healthcare@joneswalker.com

For more information about this article and/or ways in which Jones Walker can assist with any HIPAA issues, including, but without limitation, risk assessments and training, please contact Lynn M. Barrett at lbarrett@joneswalker.com.

—Lynn M. Barrett, Esq.

Jones Walker offers a broad range of legal services to health care industry clients, including regulatory compliance, litigation, investigations, operations, and transactional matters. These legal principles may change and vary widely in their application to specific factual circumstances. You should consult with counsel about your individual circumstances. For further information regarding these issues, contact:

Myla R. Reizen
Miami Center, Suite 2600
201 S Biscayne Boulevard
Miami, FL 33131-4341
305.679.5716 *tel*
305.679.5710 *fax*
mreizen@joneswalker.com

Health Care Attorneys

Lynn M. Barrett
Allison C. Bell
George F. Bloss, III
David P. Borghardt
Amy C. Cowley
Mark A. Cunningham
Nadia de la Houssaye
Kathryn W. Drey
Stephanie C. Edgar
S. Trent Favre
Pauline F. Hardin
Kathleen A. Harrison
Kathryn H. Hester
Robert B. House
Mary Margaret Kuhlmann
Joseph J. Lowenthal, Jr.
J. Leray McNamara
James C. Percy
David G. Radlauer
Rudolph R. Ramelli
Myla R. Reizen
Krystal Pfluger Scott
Donald W. Washington
Amy M. Winters

To subscribe to other E*Bulletins, visit http://www.joneswalker.com/ecommunications.html.