

January 15, 2013

Health Law Alert

First HIPAA Breach Settlement Involving Less than 500 Patients

Earlier this month, the Office for Civil Rights of the U.S. Department of Health & Human Services (“OCR”) announced that Hospice of Northern Idaho (“HONI”) agreed to pay a \$50,000 fine and enter into a two-year corrective action plan to settle potential HIPAA violations. Notably, this is the first HIPAA settlement involving a breach of unsecured electronic protected health information (“ePHI”) affecting less than 500 patients.

OCR, which is the federal agency that enforces HIPAA, began its investigation after HONI, as required by the HITECH Act, reported to OCR that an unencrypted laptop computer containing ePHI of 441 patients was stolen. During its investigation, OCR discovered that HONI did not:

- Conduct an accurate and thorough risk analysis to safeguard ePHI on an on-going basis as part of its security management process;
- Evaluate the likelihood and impact of potential confidentiality risks of ePHI maintained in, and transmitted using, mobile devices;
- Implement appropriate security measures to address those potential risks;
- Document the security measures and the rationale for adopting them;
- Maintain reasonable and appropriate security measures; or
- Have policies and procedures to address the security of mobile devices.

In the press release announcing the settlement, OCR’s Director warned that “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.”

To address the large number of HIPAA breaches involving laptops and other mobile devices, OCR recently launched an educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information*, which gives healthcare providers, and others associated with the healthcare industry, practical tips to protect their patients’ ePHI when using mobile devices. Those tips can be found at www.HealthIT.gov/mobiledevices.

The misplacement or theft of mobile devices containing ePHI has become, unfortunately, somewhat prevalent. Despite this prevalence, and often, as was the case with HONI, the lack of intentional misconduct on the part of the healthcare organization whose mobile device is misplaced or stolen and the lack of evidence that anyone actually improperly accessed the ePHI, OCR’s settlement with HOPI is another sign that OCR, which has begun conducting

unannounced compliance audits of healthcare organizations of all sizes, is vigorously enforcing HIPAA and the HITECH Act.

Please feel free to contact us if you have any questions or want to discuss.

This Health Law Alert is intended for general informational purposes only, and should not be construed as legal advice. We would be happy to provide you with advice about specific situations if desired. © 2013 Law Offices of Robert A. Polisky. All rights reserved.