HLB
HOOPER, LUNDY & BOOKMAN, PC
HEALTH CARE LAWYERS

Stolen Laptop Costs Provider $1.5 Million

By Paul Smith
September 20, 2012

In a sign of growing impatience with heel-dragging providers, the Department of Health and Human Services (HHS) has settled potential HIPAA violations arising from the theft of a laptop containing unencrypted health information for $1.5 million. The press release concerning the settlement is at http://www.hhs.gov/news/press/2012pres/09/20120917a.html.

According to the press release and a Resolution Agreement between HHS and the provider, the provider – a hospital and its related medical group - reported the theft of the laptop to HHS in April of 2010. The laptop contained patient prescriptions and clinical information. The Resolution Agreement states that HHS's investigation indicated that until late 2009, the provider had not conducted a full security risk analysis, and did not implement required privacy and security policies, procedures and controls until 2010. The provider did not admit any HIPAA violations.

In its press release, the HHS Office for Civil Rights (OCR) said:

> "OCR's investigation indicated that these failures continued over an extended period of time, demonstrating a long-term, organizational disregard for the requirements of the Security Rule.
>
> "'In an age when health information is stored and transported on portable devices such as laptops, tablets, and mobile phones, special attention must be paid to safeguarding the information held on these devices,' said OCR Director Leon Rodriguez. 'This enforcement action emphasizes that compliance with the HIPAA Privacy and Security Rules must be prioritized by management and implemented throughout an organization, from top to bottom.'"

In addition to the monetary settlement, the Resolution Agreement requires the provider to comply with a three-year Corrective Action Plan (CAP). The CAP requires the provider to—

- Prepare policies and procedures relating to portable media (including risk analysis, tracking, encryption and privacy), incident response, workstation use and security, and workforce sanctions.
- Submit policies and procedures to HHS for review and approval, adopt them as approved, and update them at least annually.

- Distribute its policies and procedures to its workforce, and obtain a signed acknowledgement from all members of the workforce who have access to electronic protected health information that they have read and understood the policies and procedures, and will abide by them.
- Train workforce members in the policies and procedures, and require them to certify that they have received the training.
- Investigate workforce violations of the policies and procedures.

In addition, the provider is required to appoint an independent monitor, approved by HHS, to review the provider's compliance with the CAP. The monitor must make unannounced site visits, interview workforce members, and investigate reports of noncompliance with the CAP. The monitor is to make twice-annual reports to HHS. HHS reserves the right to conduct its own reviews of the provider's compliance. The provider must also submit its own annual compliance report to HHS and the monitor.

The settlement indicates that – more than seven years after providers were supposed to be compliant with the HIPAA Security Rule - those who have not performed a risk analysis and implemented security policies and procedures can expect little sympathy if they suffer a security incident – even if they report it themselves. It also illustrates the risks of using laptops to store unencrypted health information. Although HIPAA does not mandate encryption of portable media, if this laptop had been properly encrypted, its loss would not have been reportable under federal breach reporting standards.

Hooper, Lundy & Bookman, PC assists clients with a range of HIPAA compliance activities, including policies and procedures, workforce training and managing data breaches. *For additional information, please contact: Paul Smith, Clark Stanton or Steve Phillips in San Francisco at 415-875-8500; Hope Levy-Biehl, Karl Schmitz or Amy Joseph in Los Angeles at 310-551-8111; or Bob Roth in Washington, D.C. at 202-580-7700*.

###