HARRISBIOMEDICAL™
COMPLIANCE SERVICES
1035 ANDOVER PARK WEST, SUITE 120, TUKWILA, WA 98188

Stolen Laptops Lead to HIPAA Citations/Penalties

Two companies have paid the Office for Civil Rights (OCR) $1,975,220 to resolve potential violations of the HIPAA Privacy and Security Rules

Company (Lesson ?) #1

On April 22nd, 2014, the U.S. Department of Health and Human Services reported that an OCR compliance review revealed that a Missouri Physical Therapy Center's measures securing patients' protected health information (PHI) were "incomplete and inconsistent… leaving its PHI vulnerable throughout the organization." The investigation, triggered by a breach report, found that the company's lack of encryption on its laptops, desktop computers, medical equipment, tablets, and other devices containing electronic protected information (ePHI) was a "critical risk".

OCR's investigation also determined, among other things, that the company had failed to establish and implement insufficient security management processes necessary to safeguard patient information. The upshot was a negotiated penalty of $1,725,200 plus preparation and implementation of a corrective action plan to verify the company's remediation of OCR's findings.

Company (Lesson ?) #2

Responding to a breach notice (See Breach Notification Rule) from an Arkansas Health Plan of the theft of an unencrypted laptop computer containing ePHI of 148 individuals, OCR found the company had also failed to comply with "multiple requirements of the HIPAA Privacy and Security Rules". Although the company had encrypted its devices after discovering the breach, OCR cited the company for numerous compliance deficiencies beginning from the initial compliance date of the Security Rule in 2005 through 2012.

The company was required to provide the United States Department of Health and Human Services an updated Risk Analysis, a corresponding Risk Management Plan, including specific security measures to reduce the risks and vulnerabilities of its ePHI, retrain it workforce and document ongoing compliance efforts. It also wrote a check to HHS in the amount of $250,000.

Comment: If nothing else, these two examples (among hundreds throughout the country) underscore the importance of protecting your patients protected health information in both the hard copy (PHI) and/or electronically (ePHI). A couple of recommendations:

1. Encrypt all devices on which patient protected information (PHI) is used or stored, including desk top computers and all mobile devices such as laptops, I-pads, I-phones, discs, tapes, USB/flash drives. Devices get stolen and password protection is never enough. (If it's encrypted, it's HIPAA compliant),
2. Make sure you have current written policies and procedures including all requirements of the HIPAA Privacy, Security, Breach Notification, and Omnibus Rules. (You'd be surprised how many dental offices thought they'd done all the HIPAA stuff back in 2003 with the Privacy Rule). If you haven't already, update your existing programs to current standards.
3. Conduct scheduled risk analyses, in keeping with all the HIPAA rules, to ensure your

security measures are working to protect your patients' information and reduce the risks and vulnerabilities to your patients' PHI and ePHI.

4. Train your staff. Keeping staff current with the many facets of protecting your patients' PHI
and ePHI is a major first step to staying in compliance.

NOTE: OCR has six educational programs available for health care providers on compliance with various aspects of the HIPAA Privacy and Security Rules. The program focusing specifically on mobile device security is *"Your Mobile Device and Health Information Privacy and Security"* can be found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/training