Health Information Compliance Alert

Industry Notes:

Unencrypted Laptop Leads to ePHI Breach

The **Hospice of North Idaho** (HONI) will pay $50,000 to the **U.S. Department of Health and Human Services'** (HHS) for a "breach of unprotected electronic protected health information (ePHI) affecting fewer than 500 individuals," according to a Jan. 2, HHS press release.

"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," said OCR Director **Leon Rodriguez** in the release.

The action comes following an investigation by the **HHS Office for Civil Rights** (OCR) after HONI reported the theft of an unencrypted laptop, in June 2011, containing the electronic protected health information of 441 patients. The organization regularly uses laptops containing ePHI for field work.

"Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule," the press release added.

To see the release, go to: www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf.

CMS Helps Ensure Your Mobile Devices Are HIPAA-Compliant

Many practices have adapted to using mobile electronic devices to help maintain patient records, such as tablets, laptops, and smartphones -- but with new technology comes new concerns about ensuring that protected health information (PHI) stays private. The Department of Health and Human Services (HHS) aims to help you secure that information with the release of a new initiative called "Mobile Devices: Know the Risks. Take the Steps. Protect and Secure Health Information."

"The use of mobile health technology holds great promise in improving health and health care, but the loss of health information can have a devastating impact on the trust that patients have in their providers. It's important that these tools are used correctly," said **Joy Pritts, HHS' Office of the National Coordinator for Health Information Technology** (ONC) chief privacy officer in a Dec. 12 statement. "Health care providers, administrators and their staffs must create a culture of privacy and security across their organizations to ensure the privacy and security of their patients' protected health information."

According to the new publication, you can take steps such as encryption, passwords, firewalls, and other methods to confirm that your PHI remains private. In addition, the agency suggests you keep your mobile devices with you at all times and delete any information you won't need any longer.

To read all of HHS's resources on this topic, visit www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.