News

FOR IMMEDIATE RELEASE
April 22, 2014

Contact: HHS Press Office
202-690-6343

Stolen laptops lead to important HIPAA settlements

Two entities have paid the U.S. Department of Health and Human Services Office for Civil Rights (OCR) $1,975,220 collectively to resolve potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. These major enforcement actions underscore the significant risk to the security of patient information posed by unencrypted laptop computers and other mobile devices.

"Covered entities and business associates must understand that mobile device security is their obligation," said Susan McAndrew, OCR's deputy director of health information privacy. "Our message to these organizations is simple: encryption is your best defense against these incidents."

OCR opened a compliance review of Concentra Health Services (Concentra) upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information. Concentra has agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.

OCR received a breach notice in February 2012 from QCA Health Plan, Inc. of Arkansas reporting that an unencrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member's car. While QCA encrypted their devices following discovery of the breach, OCR's investigation revealed that QCA failed to comply with multiple requirements of the HIPAA Privacy and Security Rules, beginning from the compliance date of the Security Rule in April 2005 and ending in June 2012. QCA agreed to a $250,000 monetary settlement and is required to provide HHS with an updated risk analysis and corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI. QCA is also required to retrain its workforce and document its ongoing compliance efforts.

OCR has six educational programs for health care providers on compliance with various aspects of the HIPAA Privacy and Security Rules. Each of these programs is available with free Continuing Medical Education credits for physicians and Continuing Education credits for health care professionals, with one module focusing specifically on mobile device security: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training

The Resolution Agreements can be found on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html

To learn more about non-discrimination and health information privacy laws, your civil rights and privacy rights in health care and human service settings, and to find information on filing a complaint, visit us at www.HHS.gov/OCR

###

Note: All HHS press releases, fact sheets and other news materials are available at *http://www.hhs.gov/news*.

Like HHS on Facebook, follow HHS on Twitter @HHSgov, and sign up for HHS Email Updates.

Follow HHS Secretary Kathleen Sebelius on Twitter @Sebelius.