Knox McLaughlin Gornall & Sennett, P.C.
Erie • Pittsburgh • Jamestown, NY
814-459-2800 • www.kmgslaw.com

Stolen Laptop Containing Patient Information Costs Providers $1.5 Million

Posted on October 01, 2012

On September 17, 2012, the Department of Health and Human Services (HHS) announced that the Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (MEEI) agreed to pay an amount of $1.5 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). As this article describes, this settlement is one of many recent actions that demonstrate the government's increased commitment to enforcing the HIPAA regulations.

As many in the health care industry are aware, HIPAA regulations (specifically, the Privacy Rule and Security Rule) require health care providers and health care organizations to comply with complex standards in order to ensure the confidentiality and security of patients' protected health information. Protected health information (PHI) is generally any individually identifiable health information transmitted or maintained by a health care provider or organization. The Privacy Rule sets limits on who can access and receive PHI. The Security Rule protects PHI in electronic form by requiring entities covered by HIPAA to implement and maintain physical, technical, and administrative safeguards. For years, the Office of Civil Rights (OCR), the government agency responsible for enforcing HIPAA, did not aggressively enforce these rules.

On February 19, 2009, however, President Obama signed into law the stimulus package known as the American Recovery and Reinvestment Act (ARRA). Among other things, ARRA contains the Health Information Technology for Economic and Clinical Health Act (HITECH Act) which provides the once dormant HIPAA regulations with newfound power. The HITECH Act increases penalties forHIPAA violations, imposes data breach notification requirements for unauthorized uses and disclosures of unsecured PHI, and extends the legal requirements set forth in HIPAA to third parties performing functions that involve the use or disclosure of PHI (known under HIPAA as "Business Associates")(1). The HITECH Act also provides State Attorneys General with the authority to bring civil actions to enforce HIPAA violations on behalf of state residents (an authority previously reserved for the OCR).

Much of the increased recent enforcement activity stems from the HITECH Act's requirement that theHHS perform periodic audits to ensure health care providers, organizations, and business associates comply with HIPAA and the HITECH Act. In November 2011, OCR piloted a program (OCR HIPAAAudit Program) to perform 115 audits of health care providers and organizations to review selected privacy, security, and breach notification policies.

In July 2012, OCR released the OCR HIPAA Audit Program Protocol utilized by OCR investigators. The protocol covers over 160 areas of performance evaluation, including 81 areas related to the Privacy Rule, 78 areas related to the Security Rule, and 10 areas related to data breach notification. The protocol also demonstrates that OCR has broadened its audit activities to include a review of the use of encryption technology and requirements related to data breach reporting, including risk assessment processes and the content and timeliness of notifications. Health care providers, health care organizations, and business associates should recognize that, in light of the new enforcement environment, a failure to comply withHIPAA regulations increases the risk of liability. While far from comprehensive(2), the following recent examples of HIPAAenforcement actions serve as a warning to health care providers, health care organizations, and business associates:

- **For Providers and Entities using Portable Devices:** After contacting OCR to report the theft of a personal laptop containing the unencrypted PHI of MEEI patients and research subjects, including patient prescriptions and clinical information, MEEI agreed to pay a settlement amount of $1.5 million and agreed to adhere to a corrective action plan (CAP) and periodic independent audits to ensure compliance with the CAP.
- **For Government Agencies working with PHI:** After contacting OCR to report the theft of a USBdrive from the vehicle of an employee, the Alaska Department of Health and Human Services (ADHHS) agreed to pay a settlement amount of $1.7 million and agreed to a CAP that requires the ADHHS to review, revise, and maintain its policies and procedures to ensure compliance with the Security Rule. ADHHS is also required to report back to OCR regularly on its ongoing compliance efforts.
- **For Smaller Group Practices:** After an OCR investigation revealed that Phoenix Cardiac Surgery,P.C. lacked appropriate safeguards to protect PHI and was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible, the physician group agreed to pay a settlement amount of $100,000 and enter into a CAP that includes a comprehensive review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules.
- **For Insurers and Health Plans:** After 57 hard drives containing the unencrypted PHI of more than 1 million people were stolen from a facility leased by Blue Cross and Blue Shield of Tennessee (BCBST), and government authorities found that the insurer failed to have appropriate safeguards in place, BCBST agreed to pay a settlement amount of $1.5 million and enter into aCAP that requires the insurer to review and revise its privacy and security policies and procedures, to conduct regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA, and to perform reviews to ensure BCBST complies with the CAP.
- **For Private Businesses:** After an OCR investigation confirmed media allegations that CVS was disposing of pill bottles containing patient information in unsecured and publicly accessible trash containers outside selected stores and further revealed that CVS failed to implement adequate employee training and security safeguards, CVS agreed to pay a settlement amount of $2.25 million, to engage a qualified independent third party to conduct assessments of CVS compliance, and to allow OCR to actively monitor its compliance over a three-year period.
- **For Business Associates:** In what appears to be the first lawsuit filed by a State Attorney General under the HITECH Act, Minnesota's Attorney General filed a lawsuit against Accretive Health, Inc., a debt collection agency that assists health care entities with revenue cycle management, for theft of a laptop from an Accretive employee's rental car. The laptop contained the unencrypted PHI of over 20,000 patients of two Minnesota hospital systems. The Minnesota Attorney General and Accretive entered into a settlement agreement in which Accretive agreed to "wind down" its remaining work for Minnesota clients and pay the Minnesota Attorney General nearly $2.5 million.

(1) Health care entities should note that in addition to the data breach requirements set forth byHIPAA and the HITECH Act, Pennsylvania maintains its own data breach disclosure law (Breach of Personal Information Notification Act) for a breach of computerized data that materially compromises the security or confidentiality of personal information. See 73 P.S. §§ 2301, et seq.

(2) The health care compliance newsletter, Health Information Privacy/Security Alert, reports that as of September 1, 2012, OCR had published 452 breach reports that affected over 20 million people.

The attorneys at Knox Law are committed to assisting clients ensure compliance with the HIPAA and HITECH Act regulations. If you have questions or concerns about matters related to compliance with HIPAA and HITECH Act regulations, such as implementing adequate policies and procedures to appropriately safeguard patient information, training staff on HIPAA regulations, conducting a HIPAA compliance analysis, or contracting with Business Associates, please contact us at 814-459-2800.

Legal Advice Disclaimer: *The content of this website is provided for general information purposes only. It should not be used as a substitute for consulting an attorney for legal advice regarding the reader's own affairs. Knox McLaughlin Gornall & Sennett, P.C. is not responsible for the content provided on any third-party website which may be accessed via links provided by this site.*

Copyright © Knox McLaughlin Gornall & Sennett, P.C.
Not to be reproduced without permission.