HIPAA Fines, Mobile Devices and Risk Assessments:

Follow the Steps or Pay the Price

By Lance O. Leider, Esq.
(Edited and introduction by Anne Hughes, ACP, FCP)

From its passage into law, the Health Insurance Portability and Accountability Act (HIPAA) has changed the landscape of, not only the healthcare industry, but the legal field as well. There is not a single aspect of our lives that has not been affected by the technology explosion and HIPAA has tried to keep pace by imposing stiff penalties on those who are noncompliant with the handling of protected health information (PHI). Attorneys and paralegals alike need to be aware of the privacy and security rules of HIPAA and we all need to realize that breaches in privacy can be avoided. If such breaches of PHI do occur, the penalties are very real.

Next are two examples of the need for HIPAA compliance to avoid privacy breaches, consequences for noncompliance and suggested solutions to avoid the same thing happening to your firm.

Two separate entities have agreed to pay the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) $1,975,220 in fines collectively. The settlements resolve potential violations of the HIPAA privacy and security rules involving stolen, unencrypted laptops. These two actions shine a light on the significant risk unencrypted laptops and other mobile devices pose to the security of patient information.[1]

HIPAA has changed the landscape of the healthcare industry and the legal field as well.

Concentra Received Risk Assessments, but Did Not Act on Findings.

According to the OCR, an investigation of Concentra Health Services, a subsidiary of Humana, was conducted after a laptop was stolen from a Missouri physician therapy center. This investigation revealed that Concentra had previously received multiple risk analyses that stated the company lacked encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information. Concentra's efforts to remedy the risk were incomplete and inconsistent, leaving patients' health information vulnerable. Concentra agreed to pay $1,725,220 to settle potential security violations and adopt a corrective action plan.

QCA Investigation. The QCA Health Plan, Inc., investigation began in February 2012, after an unencrypted laptop containing the medical records of 148 individuals was stolen from an employee's car. The investigation revealed that QCA failed to comply with multiple requirements of the HIPAA privacy and security rules. According to *Modern Healthcare*, the company is required to pay $250,000, as well as provide HHS with an updated risk analysis and corresponding risk-management plan.[2]

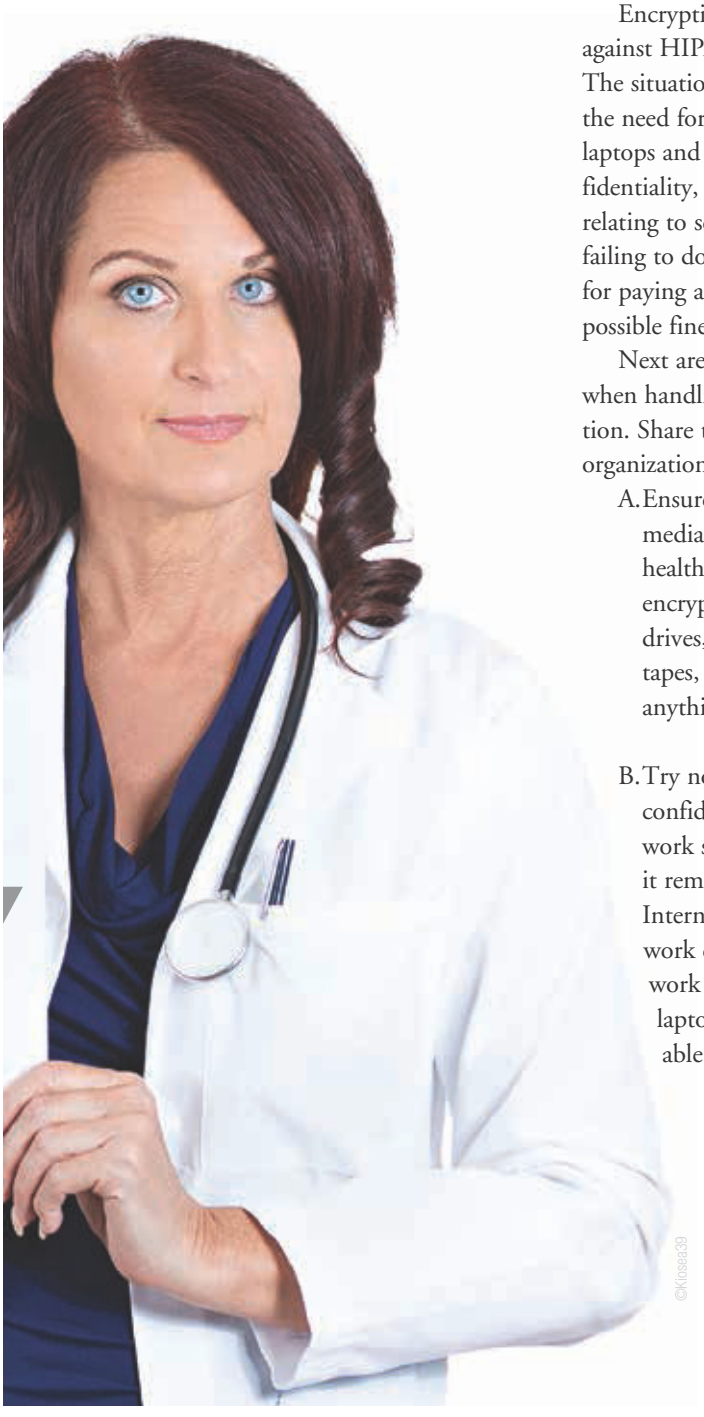
Case Study: Data Breach at Colorado Hospital Highlights IT Security Risks. A small rural hos-

pital in Glenwood Springs, Colorado, has identified a virus on its computer network that had captured and stored screen shots of protected health information in a hidden file system. The hidden folder was created on Sept. 23, 2013, but was not discovered until Jan. 23, 2014. The breach identified at least 5,400 individual patients whose information was compromised.

According to *Healthcare IT News*, among the stolen data was patient names, addresses, dates of birth, telephone numbers, Social Security numbers, credit card information, and admission and discharge dates.

Hospital officials have been unable to determine how the virus was loaded onto the hospital network, according to *Healthcare IT News*. Consequently, officials believe that there is "very high" probability that the data had been accessed by an outside entity.[3]

HIPAA-covered entities are responsible for making sure all personal information is protected. Not all law firms are HIPAA-covered entities, but some are. Is yours? A law firm may become required to adhere to HIPAA provisions or just list a HIPAA-covered entity if it has a business associate agreement with a healthcare provider.


©Klosea39

Suggested Solutions:

1. Encrypt Laptops and Other Equipment or Pay the Price.

Encryption is one of your best defenses against HIPAA non-compliance incidents. The situations described above highlight the need for all entities to encrypt their laptops and other devices. With client confidentiality, privilege and other concerns relating to sensitive information, law firms failing to do so may put that entity at risk for paying a large fine to the OCR and possible fines for state law violations.

Next are some practical tips to use when handling protected health information. Share them with others in your organization:

A. Ensure that all types of electronic media by which you transfer patient health information of any kind are encrypted. This includes thumb drives, CD ROMs, DVDs, backup tapes, mini hard drives and anything else.

B. Try not to remove any PHI or confidential information from your work site. If you need to work on it remotely, use a secure, encrypted Internet connection to access your work database. Avoid saving the work or data onto your personal laptop hard drive or other removable media.

C. Never leave your laptop or other media in a car you are having worked on by a mechanic, having an oil change, having the car washed, or while you run into a store. Thieves stake out such locations and are waiting for careless individuals to do this.

D. Never leave your work devices (laptop, thumb drive or other electronic media) in your car. What can be worse than having your car stolen? Having your car stolen with your work laptop in it with patient information and other confidential attorney-client privileged information on it.

2. Take Steps to Secure Your Network.

Breaches of the kind outlined are not solely confined to hospitals, large providers or large law firms. In fact, it may be that a hospital or law firm is targeted because of its smaller size or location in a rural area with easier access to its systems.

Viruses like the one in the Colorado hospital could be loaded onto systems as a result of an outside attack (think: "hackers") or through inside means like a corrupted flash drive or by deliberately opening an infected e-mail.

It is imperative that a HIPAA-covered entity or business associate of a HIPAA-covered entity has an effective cyber security plan. Some common sense steps include making sure that anti-virus software is up-to-date and that computers are secure from access by unauthorized personnel such as cleaning crews, other clients and their families, or opposing counsel and staff. Also, meet with an IT professional regularly to discuss additional security measures that can be put in place such as restricting access and accessibility to certain files or the ability to download programs and applications to essential staff only.

Hacked data represents a growing share of HIPAA breaches. It is imperative that covered entities ensure their compliance

continued on page 26

continued from page 25

with HIPAA to avoid any sanctions by the Office for Civil Rights (OCR). To date, the OCR has collected in excess of $18 million in fines and penalties for failures to secure patient information.

3. Get a Risk Assessment.

A HIPAA Risk Assessment is a thorough review and analysis of areas where you may have risk of violating the HIPAA laws. Federal regulations require that covered entities have this assessment done. Thus, law firms with business associate agreements with HIPAA-covered entities also need to undergo a HIPAA Risk Assessment. An OCR auditor could show up at your firm to check for HIPAA compliance and if that happens, they will ask for your Risk Assessment. Do you have one? Do you know who your HIPAA compliance officer is?

---

1 U.S. Department of Health and Human Services Press Office. "Stolen Laptops Lead to Important HIPAA Settlements." U.S. Department of Health and Human Services. (April 22, 2014). From: *http://www.hhs.gov/news/press/2014pres/04/20140422b.html.*

2 Conn, Joseph. "Unencrypted-Laptop Thefts at Center of Recent HIPAA Settlements." *Modern Healthcare*. (April 23, 2014). From: http://www.modernhealthcare.com/article/20140423/NEWS/304239945/unencrypted-laptop-thefts-at-center-of-recent-hipaa-settlements.

3 McCann, Erin. "Small-Town Hospital Gets Hacked." Healthcare IT News. (March 17, 2014). From: *http://www.healthcareitnews.com/news/small-town-hospital-gets-hacke*d.

Lance O. Leider is an attorney with The Health Law Firm, which has a national practice. Its main office is in the Orlando, Florida, area. www.TheHealthLawFirm.com The Health Law Firm, 1101 Douglas Avenue, Altamonte Springs, Florida 32714, Phone: (407) 331-6620.

LLeider@thehealthlawfirm.com