Health Information Compliance Alert

Enforcement News: Warning: Laptops Used In The Field Are At High Risk

Plus: You'll pay big for improperly dumping patient files.

Just because a laptop is password-protected doesn't mean that you can avert a HIPAA breach. You must encrypt any and all mobile devices especially if you use them in the field.

Case in point: Medical device company **DJO Global** recently notified some of its patients about a breach relating to a stolen laptop, reported attorney **Linn Foster Freedman** in a Jan. 30 blog posting for the law firm **Nixon Peabody LLP**. A thief stole the laptop from a DJO consultant's locked car outside a coffee shop in Roseville, Minn., smashing the car window and taking the consultant's backpack containing the laptop.

Although the laptop was password-protected, it was not encrypted and contained protected health information (PHI), according to a DJO statement. The laptop contained some patient names, phone numbers, diagnosis codes, DJO products received, surgery dates, health insurer names, clinic names, doctor names, and more.

No credit card information was on the laptop, but a few patients' Social Security numbers were stored, DJO said. The company claims that immediately after the theft, DJO worked with a data privacy firm to delete all personal information stored on the laptop. The laptop contained logical access control and tracking/remote management software.

"This is another important warning to medical device manufacturers and contractors to implement encryption technology on any laptops that are used in the field," Freedman warned.

State Laws Will Get You For Improper PHI Disposal, Too

If you hire a company to dispose of your patient records for you, you'd better know for certain that the company will do it the right way otherwise, you'll be liable for the breach.

On Jan. 5, the **Indiana Attorney General** (AG) entered into a consent judgment with dentist **Joseph Beck** in a Marion County court to address allegations of improper disposal of patient records. The consent judgment stems from an AG complaint for violating HIPAA and the Indiana Disclosure of Security Breach Act, according to a Jan. 12 analysis by **Stacy Cook**, an attorney with **Barnes & Thornburg LLP.**

According to the AG's complaint, Beck hired a private company to dispose of his patient records, and less than one week later 63 boxes of patient records were discovered in a dumpster at a church in Indianapolis. The patient records contained patient names, health information, Social Security numbers, insurance information, birth dates, and state identification numbers.

Under the terms of the consent judgment, Beck must pay a $12,000 fine.

The AG announced that this was the first time Indiana has sued for a HIPAA violation. "This recent settlement serves as a reminder that Indiana, like most states, has its own security breach laws that apply to personal information, which includes, but is not limited to, protected health information," Cook noted.

Stay Up-To-Date On New State Privacy/Security Laws

More and more states are jumping on the data breach law bandwagon, hoping to regulate not only non-healthcare businesses' data privacy and security practices, but also healthcare entities' HIPAA compliance. And with so many HIPAA

breach lawsuits using state law claims, you need to stay abreast of these new state laws as they emerge.

1. New Jersey: On Jan. 9, New Jersey enacted a state law effective Aug. 1, 2015 that requires health insurance companies to encrypt personal data they transmit electronically on a public network or retain on end-user computers, such as desktops, workstations, laptops, storage media, and smart phones.

Healthcare data breaches in New Jersey prompted the law, notes Jim Sheldon-Dean, founder and director of compliance for Lewis Creek Systems LLC in Charlotte, VT. You can read a brief text of the bill at www.njleg.state.nj.us/2014/Bills/S1000/562_R1.PDF.

2. New York: On Jan. 15, New York Attorney General Eric

Schneiderman announced that he would propose legislation that would require business to use baseline data security standards and broaden the state's breach notification law, according to a recent posting by attorney **Linn Foster Freedman** for the law firm **Nixon Peabody LLP.**

Under the proposed legislation, companies would receive safe harbor if they appropriately categorize their data according to risk, implement a data security plan, and attain certification.

3. California: State legislators in California passed a bill called the "Confidential Health Information Act," which would incorporate HIPAA standards into state law and clarify the standards for protecting medical information confidentiality in insurance transactions, Freedman reported.

One of the unique provisions in the law allows individuals covered by another person's health plan to submit requests to the insurer to keep certain sensitive information private, such as mental health care, sexually transmitted infection tests, and family planning services. A fact sheet on the law is available at www.cfhc.org/sites/default/files/SB_138_Fact_Sheet.pdf.

4. Indiana: On Jan. 12, senators in Indiana introduced a bill that proposes changes to the state's data breach law. The proposed changes would include expanding the statute to apply to non-computerized data, clarifying definitions about who is required to notify individuals, and requiring data users to post certain information concerning data privacy practices on their websites, Freedman noted.

The bill would also require data users to implement security measures, increase the penalty amounts that the Attorney General can assess in an enforcement action up to $150,000, and clarify the notification requirements in the disclosure letter to individuals. The latest version of the bill is available at https://iga.in.gov/legislative/2015/bills/senate/413#document-529c8193.

You May Soon Report On 12 Psychosocial Vital Signs In Your EHRs

Including social and behavioral information about your patients in electronic health records (EHRs) is on the horizon.

The **Institute of Medicine** (IOM) recently released a new report that identified 17 social and behavior domains, or data sets, that it believes should be included in EHRs because of their impact on health, reported **Geralyn Magan** in a Dec. 17 analysis for Washington, D.C.-based **Leading Age**. The IOM also identified 12 measures for these domains.

The domains and measures dubbed "psychosocial vital signs" should be included in certified EHRs and as Meaningful Use objectives, the IOM recommended. For each of the 12 measures, the IOM developed one or more specific questions for physicians to ask patients, as well as the screening frequency and follow-up activities.

The 12 measures include:

1. Race/Ethnicity
2. Tobacco Use
3. Alcohol Use
4. Residential Address

5. Educational Attainment
6. Financial Resource Strain
7. Stress
8. Depression
9. Physical Activity
10. Social Isolation
11. Intimate Partner Violence
12. Neighborhood Median Household Income.

Link: You can access the IOM's report at www.iom.edu/~/media/Files/Report Files/2014/EHR-phase-2/EHRreportbrief.pdf.