Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Heads Up: Another Court Shoots Down Lawsuit Based On 'Actual Harm'

Plus: OCR's 'Wall of Shame' gets a makeover and new web address.

The **U.S. District Court for the District of New Jersey** has joined a slew of other courts that have dismissed a data breach-related lawsuit because the plaintiff failed to prove "actual harm."

On March 31, the district court dismissed a complaint filed by four plaintiffs against **Horizon Healthcare Services** d/b/a **Blue Cross Blue Shield of New Jersey** that alleged claims under the Fair Credit Reporting Act and several state law causes of action, reported Providence, RI-based attorney **Steven Richard** in an April 7 blog posting for **Nixon Peabody LLP.**

The lawsuit arose from the theft of two password-protected laptops from Horizon's headquarters. The laptops contained the personal information of more than 839,000 of the insurer's members.

Three of the named plaintiffs in the class action lawsuit claimed that they received "less than they bargained for" because Horizon allocated part of their premiums for data protection, Richard said. But the district court ruled that this contention alone could support the plaintiffs' lawsuit. Further, the plaintiffs claimed an "imminent risk of future harm," but they failed to allege any post-breach misuse of the data in question, and so the court dismissed this claim as well.

The fourth named plaintiff justified his legal standing to sue by alleging that the thief filed a fraudulent tax return under his and his wife's names and attempted to fraudulently use his credit card, Richard noted. But the court again dismissed this claim, because the plaintiff could not sufficiently link injuries from the fraudulent tax return and credit card use to the Horizon laptop theft.

"Specifically, the court found that this plaintiff's allegations demonstrated only the mere possibility, rather than the plausibility, that his alleged injuries were connected to the laptop theft," Richard stated.

Where Did OCR's 'Wall Of Shame' Go?

If you've noticed a "page not found" error message on the **HHS Office for Civil Rights** (OCR) "Wall of Shame" listing the breaches affecting more than 500 individuals, you're not alone.

In early March, HHS changed the Internet link for the Wall of Shame to https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. "The information is now available in a much easier to use format using modern web technologies on secure pages that are part of the new HHS OCR portal that will someday be used for submission of information requested in the random audit, due to restart 'real soon now,'" says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems LLC** in Charlotte, VT.

Benefit: "The new format is much easier to read and search, with easy export of the data in multiple formats," Sheldon-Dean notes. "See what happens to others make sure it doesn't happen to you."

Also, the NIST Computer Security Incident Handling Guide, Special Publication 800-61 revision 2, has been relocated to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Focus On 3 Crucial Areas To Reduce Health IT-Related Sentinel Events

Using health IT and electronic health records (EHRs) should improve patient care and safety, right? Not necessarily,

according to **The Joint Commission** □ and you need to take certain steps to safely implement health IT.

On March 31, the Joint Commission issued a Sentinel Event Alert specifically focusing on the safe use of health IT. "EHRs introduce new kinds of risks to an already complex healthcare environment where both technical and social factors must be considered," the Joint Commission said.

Joint Commission sentinel event reports between Jan. 1, 2010 and June 30, 2013 identified 120 sentinel events related to health IT, appearing in the following eight categories:

1. Human-computer interface (33 percent) □ ergonomics and usability issues resulting in data-related errors;

2. Workflow and communication (24 percent) □ issues relating to health IT support of communication and teamwork;

3. Clinical content (23 percent) □ design or data issues relating to clinical content or decision support;

4. Internal organizational policies, procedures, and culture (6 percent);

5. People (6 percent) □ training and failure to follow established processes;

6. Hardware and software (6 percent) □ software design issues and other hardware/software problems;

7. External factors (1 percent) □ vendor and other external issues; and

8. System measurement and monitoring (1 percent).

The Joint Commission also set forth actions that focus on these three crucial areas:

1. Safety Culture □ Create and maintain an organization-wide culture of safety, high reliability and effective change management.

2. Process Improvement □ Develop a proactive, methodical approach to health IT process improvement that includes assessing patient safety risks.

3. Leadership □ Within a culture of safety and process improvement, enlist multidisciplinary representation and support in providing leadership and oversight to health IT planning, implementation and evaluation.

Resource: To read the March 31 Sentinel Event Alert, go to www.jointcommission.org/assets/1/18/SEA_54.pdf.

Stay Up-To-Date On Your State's Data Breach Law

Montana has recently joined the many other states that are expanding and changing their data breach statutes. Specifically, Montana has significantly changed and expanded its definition of personally identifiable information (PII).

Effective Oct. 1, Montana's PII definition will expand to include individual taxpayer numbers and "medical record information," which Montana law defines as personal information that relates to an individual's physical or mental condition, medical history, treatment or claim information, according to an April 7 analysis by Rochester, NY-based associate attorney **Kate A.F. Martinez** for **Nixon Peabody LLP.** Montana's data breach law will also now require any entity that issues a breach notification to also simultaneously submit a copy of the notice to the state attorney general, Martinez noted.

"This is just one spate of amendments to data breach notification laws across the country," Martinez pointed out. "Wyoming's revised law will go into effect on July 1, 2015, and it expands the state's definition of PII to include a birth or marriage certificate, medication information, health insurance information, biometric data, and an individual taxpayer number."

Bottom line: Montana's recent statutory changes should "remind everyone to carefully consider where the impact of a breach will be felt and how each individual state defines PII and requires notification in the event of a breach," Martinez

stressed.

Watch Out For Criminal Charges Resulting From HIPAA Violations

Although criminal charges stemming from HIPAA noncompliance are rare, federal authorities are still following through on these charges in certain types of cases.

A federal court recently indicted former **ProMedica** employee **Jamie Knapp** on charges that she illegally and intentionally accessed patient data at **Bay Park Hospital** in Oregon, OH, NBC24 reported on April 6. A respiratory therapist, Knapp allegedly accessed a patient's health information on a protected hospital computer between May 10, 2013 and March 25, 2014.

The hospital computer contained the electronic health records (EHRs) of 596 patients, but the initial investigation showed no patient information like Social Security numbers or financial information had been compromised. Although the Oregon, OH police chose not to file charges against Knapp back in June 2014, a HIPAA investigation led federal authorities to recently decide to bring charges against Knapp.

Protect Against Employees' Unauthorized Access To Prevent Breaches

In another instance of a healthcare provider's employee inappropriately accessing medical records, **Hattiesburg Clinic** in Hattiesburg, MS recently notified patients of a potential security breach. In January, the clinic discovered that an optometry provider who had left the clinic's employment had accessed medical records, WDAM reported on April 2.

The former employee **Scott Paladichuk, OD,** allegedly accessed patient records to mail letters so he could inform patients of his new employer. "All information obtained by the provider has been retrieved and Hattiesburg Clinic has not received any indication that the information accessed was for reasons other than sending the letters," the clinic said in a recent statement.

Nevertheless, the clinic notified patients of the unauthorized access and formally notified the **U.S. Department of Health and Human Services** (HHS).

Why FDA Is Backing Off From Regulating Certain Devices

Good news: You no longer need to worry about the **U.S. Food and Drug Administration** (FDA) "over-regulating" certain low-risk medical software products.

On Feb. 9, the FDA issued finalized guidance on its policy for medical device data systems (MDDS), medical image storage devices and medical image communication devices. The guidance finalizes the draft document issued in June 2014.

The final guidance describes the FDA's intention not to enforce regulatory controls applicable to such devices, due to the low risk they pose to patients and their importance in advancing digital health, according to a Feb. 12 analysis by the law firm **Ropes & Gray LLP.** The guidance "reflects FDA's continued efforts to apply a risk-based framework that avoids over-regulation of certain low-risk medical software products."

The Feb. 9 FDA release is available at www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm401996.pdf.