Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: No 'Present Injury,' No Grounds For Lawsuit, State Court Says

Plus: Encryption policy does nothing if you don't actually follow it.

If you're a healthcare provider in Michigan, you can rest easy knowing that a state appeals court has ruled that unless a plaintiff can prove a "present, actual injury" in a data breach case, awarding damages will be highly unlikely.

On Dec. 18, the **Michigan Court of Appeals** shot down a lower court's ruling that sided with the patients, reported Bloomberg's Bureau of National Affairs. The appellate court reversed and remanded the lower court's opinion, ruling that the lower court should have granted summary judgment to Detroit-based **Henry Ford Health System** (HFHS) in a class action lawsuit.

Background: HFHS contracted with **Perry Johnson and Associates Inc**. (PJA) for transcription services, according to Bloomberg. PJA's subcontractor made an error that caused patient records to become available on the Internet.

The online-accessible information included patient names, medical record numbers, and physician notes on patient visits. The named plaintiff in the class action lawsuit claimed her information posted online included diagnoses of alopecia and a sexually transmitted disease.

The lawsuit alleged negligence, breach of contract, and invasion of privacy, Bloomberg reported. The lower court denied HFHS's and PJA's summary judgment motions. HFHS and PJA appealed the decision.

Because the plaintiff's only claim of losses stemmed from costs she incurred for identity theft protection services, the appeals court disagreed with the lower court's ruling. The appeals court decided that the plaintiff failed to prove that the credit monitoring costs "relate to a present, actual injury." Further, the plaintiff provided no evidence that anyone actually viewed her PHI on the Internet or used her information for an improper purpose.

Identity theft protection services that the named plaintiff initiated "are not cognizable damages in the absence of present injury," the appeals court said. Many other courts have also decided that plaintiffs in data breach lawsuits cannot recover credit monitoring services as damages following a data breach where there is no evidence of actual identity theft.

Encrypt Your Mobile Devices Or Face A Hefty Judgment

Yet another unencrypted laptop has sparked a data breach and this time, the oversight and other compliance demands outweighed the monetary penalty.

In a Dec. 19 consent judgment, the **Boston Children's Hospital** (BCH) agreed to pay out $40,000 as a result of an alleged data breach that affected more than 2,000 patients, according to an announcement by the **Massachusetts Attorney General's** (AG's) office.

An unencrypted BCH-issued laptop was stolen from a physician while he was at a May 2012 conference in Buenos Aires, the AG reported. The laptop contained the PHI of 2,159 patients, including names, birth dates, diagnoses, procedures, and surgery dates. More than 1,700 of those patients were children under the age of 18.

Despite BCH's written policies to the contrary, the laptop had no encryption software installed on it prior to the incident. As a result, BCH faced a lawsuit filed under HIPAA and the Massachusetts Consumer Protection Act.

Suffolk Superior Court entered a consent judgment, alleging that BCH failed to protect the PHI of these 2,159 patients,

the AG said. The consent judgment ordered BCH to pay a $30,000 civil penalty and $10,000 to a fund for educational programs regarding protecting personal information and PHI.

BCH also must take steps to prevent future security violations and comply with state and federal data security laws and regulations, including tracking, encrypting and physically securing all portable devices, as well as train its workforce on proper handling of PHI. And BCH will continue a review and audit of its security measures, according to the AG.

Another Boston hospital faced an even bigger payout of $100,000, also for failing to protect patients' PHI when an unencrypted laptop was stolen from a physician's unlocked office. On Nov. 21, the Massachusetts AG's office announced that a court has ordered **Beth Israel Deaconess Medical Center** (BIDMC) to pay a $70,000 civil penalty, $15,000 in attorneys' fees, and $15,000 to the AG's educational fund.

The stolen laptop was the physician's personal device, but the hospital knew about and authorized its use for hospital-related business. The laptop contained the PHI and personal information of nearly 4,000 patients and employees.

BIDMC's policy required employees to encrypt and physically secure laptops containing PHI and personal information, but staff were not following these policies, the AG charged. Also, BIDMC did not notify the affected individuals about the data breach until nearly four months after the fact.

In addition to the monetary penalties, BIDMC is facing similar oversight and compliance requirements as BCH.

Hospital Claims HIPAA Violation To Fight Back Against Whistleblowers

If your organization is facing a whistleblower action for violating the False Claims Act, can you accuse the whistleblower employees of violating HIPAA in the course of making their case against you? This hospital thinks so.

Mount Sinai Hospital employees **Joseph Gaston** and **Xiomary Ortiz** filed a whistleblower action against the New York City-based hospital, alleging Medicaid fraud, according to a Dec. 22 analysis by Indianapolis-based attorney **Norman Tabler, Jr.** of the law firm **Faegre Baker Daniels LLP.**

Gaston and Ortiz claimed that Mount Sinai used "doctor swapping" practices in which one doctor provided services but the hospital billed the services under another doctor's name, Tabler said. They also accused the hospital of upcoding, billing for services never provided, and billing multiple times for a single service item.

Mount Sinai not only denied the whistleblowers' allegations, but it also filed a motion against Gaston and Ortiz claiming that they violated patients' privacy protections under HIPAA by exploiting confidential patient information in order to make the whistleblower case against the hospital.

In other words, Mount Sinai's position is not that Gaston and Ortiz "exploited inside information about the hospital; it's that they violated the privacy of patients by accessing their confidential medical records to make their whistleblower case," Tabler explained.

Implement These Measures To Avoid An Attack On Your Windows Systems

Following the recent hacker attack on **Sony**, the **U.S. Computer Emergency Readiness Team** (US-CERT) issued an alert on "targeted destructive malware" for Windows systems. The alert informs you of what you can do to help prevent an attack like the one on Sony.

Specifically, the Dec. 25 alert describes a Server Message Block (SMB) Worm Tool, which cyber threat actors are using to conduct cyber exploitation activities. Hackers used the SMB Worm Tool against Sony. The SMB Worm Tool is equipped with a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool.

"Due to the highly destructive functionality of this malware, an organization infected could experience operational impacts including loss of intellectual property and disruption of critical systems," US-CERT stated. For healthcare organizations, this malware could also cause exposure of protected health information (PHI).

The alert also contains steps that your organization can take to prevent infection and protect computer networks.

"Healthcare institutions would be well advised to review the bulletin and implement measures accordingly," warns **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems LLC** in Charlotte, VT. "Make sure your technical security folks know about this!"

Link: You can access the US-CERT alert (TA14-353A) at https://www.us-cert.gov/ncas/alerts/TA14-353A.

Get Ready For Big Changes To Health IT

The **Office of the National Coordinator for Health Information Technology** (ONC) released its Federal Health IT Strategic Plan 2015-2020 and it includes a robust blueprint for how the way you collect, use and share health information will drastically change in the next five years.

The ONC's strategic plan sets the stage and provides further context for the Nationwide Interoperability Roadmap, which should be released sometime in early 2015, said partner attorney **Laurie Cohen** in a Dec. 17 blog posting for the law firm **Nixon Peabody LLP.**

The strategic five-year plan for health IT outlines five goals in three major categories that the government aims to achieve by 2020:

1. Collect

- Goal 1: Expand adoption of health IT

2. Share

- Goal 2: Advance secure and interoperable health information

3. Use

- Goal 3: Strengthen health care delivery
- Goal 4: Advance the health and well-being of individuals and communities
- Goal 5: Advance research, scientific knowledge, and innovation

"With this updated Plan, the federal government signals that, while we will continue to work towards more widespread adoption of health IT, efforts will begin to include new sources of information and ways to disseminate knowledge quickly, securely, and efficiently," said National Coordinator for Health Information Technology **Karen DeSalvo, MD, MPH, MSc.**

"The first two goals of this Plan prioritize increasing the electronic collection and sharing of health information while protecting individual privacy," DeSalvo stated. "The final three goals focus on federal efforts to create an environment where interoperable information is used by healthcare providers, public health entities, researchers, and individuals to improve health, health care, and reduce costs."

Resource: To access the ONC's Federal Health IT Strategic Plan 2015-2020, go to www.healthit.gov/sites/default/files/federal-healthIT-strategic-plan-2014.pdf. The ONC is holding a comment period on the strategic plan until Feb. 6, 2015.

Keep A Close Watch On Your Contractors To Catch Data Breaches

If you don't know what your business associates are really doing when you're not looking, you could have a leak of protected health information (PHI) for weeks or even months before you even realize it.

Dignity Health Mercy Oncology Center's transcription contractor accidentally made public a link to some physician notes stored on a private server during a routine update, Redding Searchlight reported on Dec. 22. Dignity reported that

about 620 patients' PHI was accessible online for several weeks.

On Dec. 13, a physician reviewing patient records discovered the link accessible via **Google**. The records included the patients' names, birth dates, diagnoses, medications, therapies, and treatment plans. The records did not contain any financial information or Social Security numbers.

Mercy removed the link immediately and is working with Google to scrub any other links or archived versions of the web page, Redding reported. Mercy also no longer works with the transcription company. The healthcare provider claims that there are no signs of any unauthorized access to the PHI.