Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Can PHI Really End Up On Google? Yes, This Happened

Plus: Big security flaw puts Unix systems at risk.

Yet another data breach serves as a warning to mind your business associates (BAs) and third-party vendors.

Case in point: Huntsville, AL-based **Diatherix Laboratories** recently notified more than 7,000 of its U.S. clients that their protected health information (PHI) was unsecured for nearly three years, according to a Sept. 24 blog posting by Dallas-based **Entrust**. Although the breach first occurred back in September 2011, Diatherix didn't discover it until July 2014.

Specifically, the PHI included patients' lab test results, which became publicly accessible through Google when Diatherix's billing contractor, **Diamond Computing Company**, accidentally allowed the PHI to become accessible on the Internet. In addition to test results, patients' exposed records also included patient addresses, Social Security numbers, diagnoses, and more, Entrust reported.

Beware: Unix-Based Systems Have Serious Security Flaw

If your computer uses a **Unix**-based operating system (OS) like Linux or Mac OS X, your data could be at grave risk.

On Sept. 24 and 25, several announcements came out regarding a recently discovered serious security flaw in all Unix-based system implementations, reports **Jim Sheldon-Dean**, founder and director of compliance for **Lewis Creek Systems LLC** in Charlotte, VT. The security flaw is known as the "Bash/Shellshock Vulnerability."

"Exploitation of this vulnerability may allow a remote attacker to execute arbitrary code on an affected system," Sheldon-Dean warns. The **United States Computer Emergency Readiness Team** (US-CERT) is aware of the Bash vulnerability. For more information, go to www.us-cert.gov/ncas/current-activity/2014/09/24/Bourne-Again-Shell-Bash-Remote-Code-Execution-Vulnerability.

How New State Data-Breach Laws Could Cause HIPAA Compliance Confusion

A new state law in Florida that became effective on July 1 has continued the trend of stricter data breach state laws. And Florida is the newest state to enact a breach statute that conflicts in key ways with the federal HIPAA law.

The new Florida law, the Florida Information Protection Act (FIPA) replaces the state's breach notification requirements and expands Florida's reach and enforcement, said Maryland-based partner attorney **Emily Wein** in a recent analysis for **Ober Kaler Attorneys at Law**. FIPA is yet another law that reinforces a trend of states enacting their own data breach and notification laws that expand beyond the scope of the federal requirements under HIPAA.

Under FIPA, in the event of a breach, covered entities (CEs) must provide affected individuals with a notice that meets the statute's requirements within 30 days after the breach determination or reason to believe a breach occurred, Wein explained. But this requirement conflicts with federal HIPAA requirements under HIPAA, providers have 60 days to provide notice.

Trap: "The question raised is whether HIPAA [CEs] in Florida continue to have the 60-day timeframe or 30-day timeframe," Wein pointed out. "Answering that question requires a determination of whether HIPAA's longer notice period would be preempted by FIPA's more stringent 30-day timeframe."

FIPA differs from HIPAA in a few other important ways. For example, FIPA requires CEs and their third parties to institute reasonable security measures but falls short of providing detail on what that means. HIPAA, on the other hand, has more specific security requirements, which Florida providers must still follow.

Also, FIPA requires some compliance by a CE's third-party agent, but the statute does not actually make that third party individually liable under FIPA like business associates are under HIPAA, Wein stated. And FIPA's penalties for not providing proper notice are assessed per breach, not per affected individual, but the statute doesn't say whether state regulators will also take into account the specific facts of each situation in assessing total penalties like HIPAA does.

To read the new Florida statute (Fl. Stat. § 501.171), go to www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html. Or go to www.leg.state.fl.us/statutes/index.cfm and type "501.171" into the search box.

Try Decision-Point Maps To Help Justify Not Meeting MU Deadlines

The **Centers for Medicare & Medicaid Services** (CMS) and the **Office of the National Coordinator** (ONC) recently granted certain flexibility to hospitals and eligible professionals (EPs) in meeting Stage 2 Meaningful Use (MU) measures in 2014. But EPs and hospitals must thoroughly explain the reasons behind their failure.

Problem: Although this flexibility is a boon for many struggling providers, CMS' and ONC's guidance has left many providers scratching their heads, wondering who is allowed to claim the exception. (See "Meaningful Use: Get Your 2014 CEHRT Now," HIC v14n9, page 66.)

"Any EPs or hospitals that attest for a different stage than what they were scheduled for must be prepared to defend this decision in an audit, understanding that each case will be evaluated individually," warned **Ogden Murphy Wallace Attorneys** (OMW) associate attorney **Elana Zana** in a Sept. 30 announcement. "This defense should therefore be very well documented."

Solution: In partnership with **ECG Management Consultants,** OMW developed maps of decision points and examples of acceptable and unacceptable justifications for not meeting your scheduled MU stage in 2014. One decision-point map focuses on provider options if this is your first or second year and the second map outlines options if this is your third or fourth year whether you're dealing with the 2014 Stage 1 or Stage 2 objectives and measures.

Link: To access the decision-point maps, go to http://omwhealthlaw.com/meaningfuluseattestationin2014/.

Why Certain HIPAA Breach-Related Lawsuits Are Failing

More state courts are requiring actual proof that patients' information was used for identity theft following a data breach before awarding punitive damages. This time, an Alabama court chimes in.

In February, Alabama-based **Flowers Hospital** determined that one of its employees stole patient records containing patient names, addresses, Social Security numbers, and health insurance information, according to an Oct. 3 blog posting by the law firm **Nixon Peabody LLP**. The employee was charged with trafficking in stolen identities, and then five affected patients filed a class action lawsuit against Flowers.

Flowers filed a motion to dismiss the complaint, arguing that the patients "didn't have standing to sue based merely on an increased likelihood of identity theft in the future," Nixon Peabody related. In response, the judge ordered the patients to file a Second Amended Complaint to show evidence that a third party used their Social Security numbers to file false tax returns as they alleged.

Bottom line: "Clearly, if the plaintiffs can show that their identities were actually stolen and used to file false tax returns as a direct result of the breach at Flowers Hospital, the Motion to Dismiss will be jeopardized," Nixon Peabody concluded.