Health Information Compliance Alert

Enforcement News: Don't Let Your Paper Files Trigger A HIPAA Breach

Plus: Nevada is getting serious about health data-related identity theft.

Breach reporting was in full force during the month of October, and most of those breaches arose from paper/films, with laptops and other portable devices coming in at a close second place.

Of the 20 total breaches reported in October, 14 involved healthcare providers, four involved health plans, and two involved business associates (BAs), according to the **HHS Office for Civil Rights** (OCR) "Wall of Shame" (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf). Ten of the incidents involved unauthorized access/disclosure of protected health information (PHI), six involved thefts, and four were hacking/IT incidents.

The various locations of breached information included paper/films (six), laptops or other portable electronic devices (five), email (four), electronic medical records (two), a network server (one), and a desktop computer (one). And for one reported breach, the OCR simply listed the location of breached information as "other."

The two largest breaches in October both occurred in Texas. **Children's Medical Clinics of East Texas** reported an unauthorized access/disclosure involving a desktop computer that affected 16,000 individuals, and the **Emergence Health Network** reported a hacking/IT incident involving a network server that affected 11,100 individuals.

Watch Out: States Are Cracking Down On Using PHI For Identity Theft

If an employee steals a patient's protected health information (PHI) to commit identity theft, that person could face more than a decade in prison and up to a half-million dollars in fines particularly if the employee commits the crime in a state like Nevada.

On Oct. 27, a former laboratory technician at a pediatric cardiology practice in Las Vegas pleaded not guilty to charges of illegal use and disclosure of patient health information and aggravated identity theft. A federal grand jury had indicted **Sherice Joan Williams** on these charges, according to a recent announcement by the **Nevada U.S. Attorney's Office**.

Between about Dec. 1, 2014 and Jan. 27, 2015, Williams allegedly accessed the PHI of a patient knowingly and without authorization, and then applied for personal credit cards using that patient's information. The **FBI** worked with the local police department to investigate the case.

Consequences: If convicted, Williams could face up to 10 years in prison for the illegal use/disclosure of patient health information charge, along with a minimum of two consecutive years for the aggravated identity theft charge. Williams could also face fines of up to $250,000 for each count.

Know Your HIPAA Breach Stats: Check Out These New Charts

One of the best ways to avoid stepping on a mine in a minefield is to know where those mines are located, and the same goes for HIPAA breaches. If you know where your vulnerabilities lurk, you're better prepared to avoid a disaster.

And the law firm **Davis Wright Tremaine LLP** (DWT) has just released a series of charts that plot out the vulnerabilities

and threats to protected health information (PHI) and trends in the healthcare sector. Studying the larger reported HIPAA breaches from the **HHS Office for Civil Rights** (OCR), DWT developed charts synthesizing recent breach data in these key areas:

- Number of breach incidents reported;
- Number of individuals affected;
- Causes or types of media (paper, laptop, email, portable electronic devices, etc.) that affect a disproportionate number of individuals;
- Breaches involving business associates (BAs); and
- Type of entity involved, including type of covered entity (CE) and type of BA.

Although the number of reported breaches affecting more than 500 individuals has increased dramatically in the past year or two, "the root causes of the reported breaches shifted very little," DWT stated. For example, the most common breach cause in May 2014 was theft, which accounted for 48 percent of breaches, and theft accounted for 49 percent of reported breaches in September 2015. Likewise, unauthorized access/disclosure accounted for 17 percent of reported breaches in May 2014, while that figure increased only slightly to 20 percent by September 2015.

Link: To view the charts, go to www.privsecblog.com/healthcare-breach-reports/.

Switching Employers? You Can't Take PHI With You

In the HIPAA realm, even the CEO of a healthcare company isn't safe from violation charges when handling protected health information (PHI) □ especially when that CEO tries to take clients' PHI to a new company after stepping down.

On Oct. 18, the Rochester, N.Y.-based advocacy group **Center for Disability Rights** (CDR) issued a news release alleging that the former CEO of **Angels in Your Home** took the PHI of clients and used it to recruit clients to a new agency, **All-American Home Care**. CDR is offering to arrange legal help to anyone who is or was affiliated with Angels in Your Home as a client or healthcare aide.

On Oct. 20, Angels in Your Home filed a lawsuit against the former CEO and All-American Home Care, as well as other defendants, the Rochester Democrat & Chronicle recently reported. Also, CDR has contacted the **New York State Attorney General's Office** and the state's health department, both of which said they would look into the potential HIPAA violation/breach case.

Although no programs affiliated with CDR were involved in the alleged privacy violation, CDR learned about the incident from its clients who received services from Angels in Your Home and who All-American had contacted.