# Health Information Compliance Alert

## Enforcement News: Beware: Data Theft Still Topping Large-Scale Breach Incidents

**Plus: Don't let employees go on shopping sprees on your patients' dime.**

June was a big month for large healthcare data breaches, yielding 19 breach reports on the **HHS Office for Civil Rights**' (OCR) "Wall of Shame."

Most of the reported breaches stemmed from theft (nine breaches), while eight involved unauthorized access and/or disclosure. Improper disposal and hacking/IT incident scored one breach incident each. The largest breaches involved theft.

Most (13) breach incidents involved healthcare providers, while three breaches involved business associates (BAs) and three more involved health plans.

The largest breach incident affected 50,000 individuals and involved improper disposal of a portable electronic device by **Lancaster County EMS** in South Carolina. Texas-based BA **Global Care Delivery Inc.** reported a breach affecting more than 18,000 individuals stemming from a laptop theft, and the health plan **Oregon's Health CO-OP** also reported a laptop theft-related breach affecting 14,000 individuals.

Rhode Island healthcare provider **CVS Health** reported a desktop computer theft that resulted in a data breach affecting more than 12,000 individuals, and another theft reported by Nevada healthcare provider **Implants, Dentures & Dental (Half Dental)** also involved 12,000 individuals' PHI.

**Link:** You can access the OCR's Wall of Shame at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

**Safeguard Lucrative Patient Information From Employee Theft**

Employees who steal patient data to commit fraud and identity theft are increasingly facing harsh criminal charges.

The **New York County District Attorney's Office** (NYDA) in Manhattan has indicted eight individuals, one of which was a hospital employee, for stealing patient information as part of an ID theft ring. The **Montefiore Medical Center** employee allegedly stole patients' personal information and shared that information with others to open accounts and purchase luxury goods at department stores and major retailers.

The NYDA has charged the eight defendants with identity theft, grand larceny, criminal possession of a forged instrument, and more. "In this case, a hospital employee privy to confidential patient records allegedly sold financial information for as little as $3 per record," Manhattan DA **Cyrus Vance, Jr.** said in a June 19 statement.

The hospital employee was an assistant clerk in one of the hospital wings, where she had access to patients' names, birth dates, Social Security numbers and other personal information. The NYDA estimates that the ID theft ring racked up more than $50,000 in fraudulent purchases and purportedly compromised the personal information of as many as 12,000 patients.

Montefiore has cooperated fully with law enforcement in the investigation and has notified all affected individuals of the breach. The hospital is also providing affected patients with one year of credit monitoring, identity recovery services, and other identity protection measures.

**Understand The Anatomy Of A Cyberattack**

How can you defend your organization from cyberattacks? How do cyberattacks occur? If you want the answers to these questions and more, a new report from the **Workgroup for Electronic Data interchange** (WEDI) has some valuable insights.

On June 22, WEDI announced its release of "Perspectives on Cybersecurity in Healthcare," a primer on cybersecurity and cyberattacks for healthcare entities. The primer illustrates some of the challenges that healthcare organizations face in defending against cyberattacks and discusses the vectors in which they occur.

In the first four months of 2015, more than 99 million healthcare records have been exposed through 93 separate cyberattacks, according to WEDI. And the problem is growing rapidly.

**Impact:** "The frequency, scope and sophistication of cyberattacks are growing at a worrisome rate in healthcare," WEDI president and CEO **Devin Jopp, Ed.D** said in the June 22 announcement. "The risk of cyberattacks is no longer limited to the IT desk  it is a key business issue that must be addressed by executive leadership teams in order to build that 'culture of prevention.'"

The primer tackles three areas of cybersecurity:

1. The Lifecycle of Cyberattacks and Defense;

2. The Anatomy of an Attack; and

3. Building a Culture of Prevention.

You can access the document at [www.wedi.org/knowledge-center/white-papers-articles/issue-briefs/resources/2015/06/19/perspectives-on-cybersecurity-in-healthcare](www.wedi.org/knowledge-center/white-papers-articles/issue-briefs/resources/2015/06/19/perspectives-on-cybersecurity-in-healthcare).

**Trend: Must You Report Big Breaches To Your State Government?**

Oregon and Washington are the two states to most recently pass legislation requiring notification to the states Attorney General of large data breaches affecting more than 500 individuals. And this is a trend that isn't slowing down anytime soon.

"More than a dozen states require state government agencies notification," attorney **Mary Beth Gettins** of **Gettins' Law** said in a June 24 blog posting. In addition to notifying state government entities, many state laws now have different or more stringent requirements than HIPAA.

For example, some states require a shorter notice period to individuals affected by a breach than what is required under HIPAA, and some states give affected individuals the right to sue providers and health plans for failing to safeguard their personal information, Gettins noted. Some state laws extend the definition of what constitutes "personally identifiable information"  for instance, Oregon's new definition includes biometrics (fingerprints, retina or iris scans, etc.).

**Takeaway:** You must pay attention to your state laws in addition to the federal HIPAA laws, Gettins stressed. But determining which states' laws apply can be tricky if you serve patients who reside in different states.

**Rule of thumb:** "Sometimes, multiple state laws will apply to a practice or health plan," Gettins said. What matters is in what state the individual resides, not where your practice or health plan is located.