Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Why The NFL Isn't Immune To HIPAA Breaches Either

Plus: Employee snooping can spur an expensive (and embarrassing) lawsuit.

Password protection without encryption isn't enough to avoid a costly HIPAA breach, even for the **National Football League** (NFL).

A laptop containing the records of thousands of NFL players was stolen from a **Washington Redskins** trainer's car, the Los Angeles Times reported on June 2. The incident occurred on April 15, 2016.

According to a Redskins statement, the laptop was password-protected but was not encrypted. The Redskins claimed that there was "no reason to believe the laptop password was compromised" and "the NFL's electronic medical records system was not impacted."

A backpack containing the laptop was stolen from the trainer's car, and the laptop contained the copies of medical exam results for NFL scouting combine attendees from 2004 through 2016. The **NFL Players Association** (NFLPA) consulted with the **U.S. Department of Health and Human Services** (HHS) on the theft.

The NFLPA said it's still determining what to do regarding the breach, beyond notifying the affected individuals, but the Redskins said it has started encrypting all laptops issued to athletic trainers and other team personnel, according to the Times.

Beware: A Nosy Employee Can Land Your Organization In Court

If you suspect employee snooping on medical records especially when they're spying on fellow employees' records you'd better nip that problem in the bud right away.

A former employee has filed a lawsuit in a Denver federal district court against **Aspen Valley Hospital** in Colorado, alleging that a human resources (HR) manager exposed his protected health information (PHI) and that the hospital repeatedly violated HIPAA, The Aspen Times reported. The employee's identity is concealed in the lawsuit to protect his privacy.

The employee alleges that the HR manager outed him as HIV-positive. The lawsuit also contends that he was fired in retaliation for complaining to the **HHS Office for Civil Rights** (OCR) and since then has been unable to obtain employment in the area partly due to the hospital's "continuing retaliation."

The HR manager, who was also the privacy officer for the hospital's health plan, allegedly told another employee about the plaintiff's condition over drinks and dinner in September 2012. Despite outstanding job performance reviews and promotions since 2003, this was the point when the plaintiff's employment status began to unravel, according to the lawsuit.

Hacking/IT Incidents Top Breaches Reported In June

Safeguarding your electronic protected health information (ePHI) may seem super high-tech at times, but keep in mind that one of your biggest weaknesses is still good old-fashioned paper files and films.

That's the case with the latest reported breaches in June 2016. Of the 15 total large-scale breaches reported to the **HHS Office for Civil Rights** (OCR) that affected more than 500 individuals, six stemmed from paper/films. Five involved a network server, and one each involved email, electronic medical record (EMR), and "other portable electronic device." One incident involved both an EMR and a network server.

Most breaches were reported by healthcare providers (12 breaches), with two involving health plans and only one reported by a business associate (BA). Most (seven) involved a hacking/IT incident, with five involving an unauthorized access/disclosure, two involving improper disposal, and one involving loss.

The largest breach reported in June affected 27,393 individuals and stemmed from an unauthorized access/disclosure of paper/films. **Wal-Mart Stores, Inc.** in Arkansas, listed as a healthcare provider, reported the breach on June 8. To view the OCR's "Wall of Shame," which lists all reported breaches involving more than 500 individuals, go to https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.