$4.8 Million HIPAA Security Settlement Is the Largest HIPAA Payout Yet

written by CPH Insurance | June 15, 2016

The HIPAA malpractice settlements of 2014 are the largest we've seen in the industry thus far. No doubt some of these violations resemble to the comical "slipping on a banana peel" – but every example comes with a valuable lesson about HIPAA: the cost for violating the Accountability Act is ever on the rise.

Settlements in just the first two quarters of 2014 topped out the charts on HIPAA-related lawsuits. Let's take a look at the top violations of 2014.

#2: Medical Records Dumping Fail

Cost: $800,000

Violation: Privacy Rule

Parkview Health System helped a retiring physician make the hard-earned transition from life as a leader to a life of leisure. Parkview took custody of ~5,000 patient records while they considered purchasing the physician's practice. In the strenuous moving process, employees left 71 cardboard boxes unattended in the driveway of the physician's home.

As a result of this painful and almost slapstick slip-up, Parkview came under investigation by the OCR, was assigned $800,000 in resolutions and a full policy, procedure, training and implementation report requirement.

Read more about the medical transportation case at HHS.gov

In cases of blunder or real errors, malpractice insurance keeps businesses afloat. Read more for coverage information for Non Profit Medical Professionals like Parkview.

#1: Enemy Number One – Data Security & ePHI violations

Cost: $4,800,000

Violations: Security Rule, Privacy Rule

New York and Presbyterian Hospital (NYP) and Columbia University (CU) confessed to the threat of a security breach in September of 2010. Nearly 7,000 individuals were exposed in ePHI (electronic Protected Health Information) security failures. The case of joint partnership between the ivy league

university and the local hospital resulted in a shared data network and shared firewall that created a major breach when a personally-owned computer server became accessible over search engines.

That is to say, individual's data became accessible on the internet. Publicly.

The fact is, **security cases like this are becoming more and more prevalent**. Take matters into your own (practice's) hands by discovering the failures in your security system before your patient's information becomes exposed.

For more information on the NYP & CU case, click here.

Discover the coverage options for practices and individuals worried about malpractice risks

The increasing risks and costs of violating HIPAA are not anomalous to these cases – the expense comes with a strong endorsement from the HHS.

"HHS also put the industry on notice that any entity self-reporting a security breach should not expect much leniency." – Law360.com,

Things you need to know:

ePHI – electronic Portable Health Information. Any time you put patient's information on a computer or mobile device, you need to abide by ePHI security standards.

Risk analysis – HIPAA is starting to require companies to test their networks for attacks. Stay compliant by staying prepared.

Keep up to date with Privacy and Security protections – Stay informed. Utilize training materials for HIPAA compliance. Always stay safe, and stay covered. HIPAA is ever-changing, and it's tough to stay secure in this modern, digital world.