Healthcare IT News

Groups hit with record $4.8M HIPAA fine

'The gloves are off' after patient data winds up on Google

To those shirking their HIPAA privacy and security duties: get ready to pay up. That's the message the Department of Health and Human Services is sending after it set records Wednesday for imposing the largest HIPAA monetary fine to date on two entities found to be seriously lacking in the security arena.

New York-Presbyterian Hospital and Columbia University Medical Center together have agreed to hand over a whopping $4.8 million to settle alleged HIPAA violations after the electronic protected health information of 6,800 patients wound up on Google back in 2010.

Following an investigation by the Office for Civil Rights, the HHS division responsible for HIPAA enforcement, it was discovered that the HIPAA breach transpired when a CU physician, who developed applications for NYP and CU, attempted to deactivate a personally-owned computer server on the network containing ePHI. Due to lack of technical safeguards, server deactivation resulted in ePHI being accessible on the Internet.

The data was so widely accessible online that the entities learned of the breach after receiving a complaint by an individual who saw the ePHI of their deceased partner, a former NYP patient, online.

"The message here is get your house in order," Rachel Seeger, OCR's senior health information privacy outreach specialist, told *Healthcare IT News*, prior to the official announcement. "The gloves are off."

"You can only imagine what's happening at your child's pediatrician office."

NYP will pay the lion's share of the settlement at $3.3 million, while CU has agreed to pay $1.5 million.

In addition to underscoring the severe security deficiencies and practices at NYP and Columbia University Medical Center, the settlement also exposes another disconcerting reality, said Seeger, and that's: "Who you expect to be the leader" is not. "You can only imagine what's happening at your child's pediatrician office."

Despite the more than $25.1 million in fines OCR has levied on healthcare entities that have demonstrated willful neglect over protecting patients' health information, the

cases involving disabled or nonexistent firewalls, unencrypted devices, emails sent with patient data to the wrong recipient, or accidentally posting PHI online are in no short supply.

And because of this, "OCR will only continue with these enforcement activities," added Seeger.

Just last month, OCR levied nearly $2 million in fines … after two unencrypted laptops containing patient health information were stolen. Both entities also failed to implement proper risk analyses.

Just last month, OCR levied nearly $2 million in fines against Concentra Health Services and Arkansas-based QCA Health Plan after two unencrypted laptops containing patient health information were stolen. Both entities also failed to implement proper risk analyses, according to OCR officials.

In addition to the regular HIPAA investigations and subsequent settlements, OCR will also officially be launching its HIPAA audit program in fall 2014 for covered entities. The audit program kicks off for business associates starting in 2015, said Seeger.

Not only do organizations face considerable federal and state penalties for violating privacy laws, there's also all the associated costs that run up the bill.

These costs include extending free credit monitoring to patients, outsourcing hotline support, hiring an external investigation or forensic experts. Then, don't forget the in-house investigations, legal costs and the hit to your reputation. All in all, these costs average to $2 million for each healthcare entity over a two-year period, according to a 2014 Ponemon Institute breach report.

It's not all bad news, however. Some healthcare groups appear to be making modest improvements. The same Ponemon report highlighted a slight downtick in the number of breaches healthcare organizations reported in 2013, compared with 2012. In 2012, some 45 percent of healthcare organizations reported having a five or more data breaches. This past year, the number fell to 38 percent.

From Healthcare IT News – May 8, 2014 -
http://www.healthcareitnews.com/news/group-slapped-record-hipaa-fine