Codify
BY AAPC

Eli's Rehab Report

Patient Privacy: Ignoring Paper Records Could Prove to Be A Costly Mistake

Lesson: Provide proper HIPAA training to all employees and institute proper HIPAA policies and procedures.

The **HHS Office for Civil Rights** (OCR) is as serious about your safeguarding the privacy of paper records as it is about the security of protected health information (PHI) on your computers, networks and mobile devices. A recent HIPAA breach case demonstrates just how.

OCR lowered the boom on community-based healthcare system **Parkview Health System, Inc**. (serving northeast Indiana and northwest Ohio) following a complaint filed back in June 2010. OCR launched an investigation after receiving the complaint, which was from a retiring physician who alleged that Parkview violated the HIPAA Privacy Rule.

Background: In 2008, Parkview took custody of medical records belonging to approximately 5,000 to 8,000 patients while helping the retiring physician to transition her patients to new providers, according to OCR. Parkview considered purchasing some of the physician's practice as well.

On June 4, 2009, Parkview employees left 71 cardboard boxes of these medical records unattended in the retiring physician's driveway when they discovered that she was not at home, OCR states. The medical records were "accessible to unauthorized persons" and "within 20 feet of the public road," which was "a short distance away from a heavily trafficked public shopping venue."

What OCR Demands in the CAP

OCR announced on June 23 that in addition to the $800,000 fine, Parkview agreed to a corrective action plan (CAP). According to attorney **Linn Foster Freedman** in a June 27 Privacy Alert analysis for the law firm **Nixon Peabody LLP**, the CAP requires Parkview to:

- Develop, maintain, and revise, as necessary, any written policies and procedures, including addressing non-electronic PHI, and provide them to HHS for approval;
- Distribute the approved policies and procedures to all workforce members who have access to PHI and to new employees within 20 days of starting work;
- Review policies and procedures periodically and promptly update them when operations or regulations change; and
- Develop workforce training and submit it to HHS for approval, and then train all employees, document the training through a dated certification from each workforce member who received training, and train new employees within 20 days of starting work.

Parkview must also notify HHS in writing within 30 days if Parkview determines that a workforce member has violated the policies and procedures, noted associate attorney **Jefferson Lin** in a June 23 blog posting for the Seattle-based law firm **Ogden Murphy Wallace Attorneys**. And the settlement agreement requires Parkview to submit to HHS a final report demonstrating compliance with the CAP.

Don't Ignore Your Security Practices for Paper Records

Sure, this settlement appears to provide the straightforward wisdom: provide proper HIPAA training to all employees and institute proper HIPAA policies and procedures. Or perhaps the simplest lesson is: don't leave boxes of medical records

unattended in someone's driveway. But experts believe there's more that you can learn from this case.

Caution: "The settlement is particularly notable because it relates to paper records, which is a departure from OCR's recent focus on electronic PHI," pointed out health law attorney **Leah Roffman** in a June 26 blog posting for the law firm **Cooley LLP**. And OCR has highlighted that too many complaints stem from improperly discarded or transferred records.

"Organizations should pay careful attention to the transfer and disposal of both electronic and paper patient records," Lin stressed. And OCR has posted some helpful FAQs regarding HIPAA and the proper disposal of PHI and patient records: www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf. The document answers the following six questions:

What do the HIPAA Privacy and Security Rules require of covered entities (CEs) when they dispose of PHI? May a CE dispose of PHI in dumpsters accessible by the public? May a CE hire a business associate (BA) to dispose of PHI?

May a CE reuse or dispose of computers or other electronic media that store electronic PHI?

How should home health workers or other workforce members of a CE dispose of PHI that they use off of the CE's premises?

Does the HIPAA Privacy Rule require CEs to keep patients' medical records for any period of time?

Beware of Potentially Arbitrary Settlement Amounts

Another interesting aspect of this particular settlement is the seemingly large penalty inching dangerously close to the $1-million mark. Experts are puzzled at the large settlement amount particularly because the case involved no actual improper access to the PHI.

Watch out: "Although there is no mention that an unauthorized person actually had access to or took any records from the boxes in the driveway, Parkview agreed to pay $800,000 for the violation," Freedman noted. "There is no guidance on what the settlement amount is based upon or how it was calculated under the HIPAA regulations."

Bottom line: As more and more breach cases come to light, pay attention to not only the trends in the terms of CAPs, but also the monetary settlement amounts. And hopefully, OCR will become more transparent in how it calculates these penalties.