Health Information Compliance Alert

Enforcement News: Brace Yourself For Increased HIPAA Audits

Plus: OCR now handing out fines for not having breach policies.

The **HHS Office of Inspector General** (OIG) is slamming the **HHS Office for Civil Rights** (OCR) for OCR's apparently lax approach toward audits of HIPAA Security Rule compliance and you'll be the one to pay the price.

The OIG recently released a not-so-favorable report on the OCR's work in implementing the audit requirements under the HITECH Act. The OIG also found that OCR's own system implementations used in managing their audit process were not performed securely, noted **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, VT, in a recent analysis.

Look out: The OIG is charging OCR with implementing better controls on the HITECH auditing process and HHS systems, as well as implementation of periodic Security Rule audits, Sheldon-Dean stated. The report's impact could lead to increased efforts to audit HIPAA Security Rule compliance, "putting additional pressure on HIPAA entities to do the work necessary for HIPAA Security Rule compliance now."

Bright side? "The findings are likely to lead to an increase in surprise audits, but also more consistency in terms of OCR investigations and enforcements," wrote attorney **Linn Foster Freedman** of the law firm **Nixon Peabody LLP** in a Dec. 9, 2013 HIPAA law alert.

"Inconsistencies in OCR investigations and enforcements in different regions and with different investigators will hopefully lessen and become more predictable," Freedman noted. "This consistency will be helpful for day-to-day HIPAA compliance."

The OIG report is entitled, "The Office for Civil Rights Did Not Meet All Federal Requirements in Its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule." You can view the entire OIG report at http://oig.hhs.gov/oas/reports/region4/41105025.pdf.

Don't Have A Breach Notification Policy? OCR Will Fine You

The very first settlement involving a provider's lack of breach notification policies and procedures marks a new chapter in HIPAA enforcement. So if you don't already have these policies and procedures in place, you could face hefty fines.

On Dec. 27, 2013, the **HHS Office for Civil Rights** (OCR) announced that **Adult & Pediatric Dermatology, P.C.** of Concord, MA will pay out $150,000 and enter into a corrective action plan as part of a settlement agreement. OCR charged the practice with HIPAA violations, including the potential breach of 2,200 patients' protected health information (PHI).

The PHI was saved on an unencrypted thumb drive, which was stolen from a vehicle and never recovered, Sheldon-Dean explained. Further, the practice "had not conducted a HIPAA Risk Analysis and did not have in place written policies, procedures, and training for breach handling."

For more information from HHS on the breach incident and the settlement agreement, go to www.hhs.gov/news/press/2013pres/12/20131226a.html.

Resource: If you need instruction on HIPAA breach rules, attend the upcoming live audioconference "Compliance with HIPAA Security and Breach Rules What Every Medical Office Must Know," presented by **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC**. The 60-minute interactive audioconference will air on Tuesday, March 24, 2014 at 1:00pm Eastern. For more information, call 866-458-2965 or visit www.audioeducator.com/healthcare-compliance-and-hippa/hipaa-security-03-24-14.html.

How You Not Your Facility Can Be Liable For Unlawful Disclosures

In a potentially game-changing case, the **New York State Court of Appeals** decided that a health care clinic is not responsible for the HIPAA Privacy Rule violation of its employee. You as an individual could be held personally liable for such a violation if you're "acting outside the scope of employment."

Background: A nurse employed at a health care clinic recognized a patient who was being treated for a sexually transmitted disease, according to a Jan. 13 **Nixon Peabody LLC** Health Alert by attorney **Laurie Cohen**. The nurse sent text messages about the patient's medical information to her family members, including a family member who was dating the patient. This family member forwarded on the text messages to the patient.

After the patient complained to the clinic, the facility fired the nurse, Cohen explained. The patient then sued the clinic in federal court. Initially, the federal district court dismissed the patient's complaint, but on appeal, the **Second Circuit Court of Appeals** dismissed all but one cause of action.

When the case went to the New York State Court of Appeals, the court had to decide whether, under New York law, "there was a common right of action for breach of fiduciary duty of confidentiality for the unauthorized disclosure of medical information when an employee responsible for the breach acts outside the scope of employment," Cohen said.

The court decided that a medical corporation should not be held to a "heightened duty" for an employee's misconduct when the conduct was a "clear departure from the scope of employment, having been committed for wholly personal motives."

Caveat: But the court did caution "that a medical corporation could be held liable for its own conduct, including negligent hiring and supervision," Cohen noted. "It also stressed the importance of having policies and procedures and the appropriate training programs in place to address medical information confidentiality."

Link: You can read the entire court decision at www.nycourts.gov/ctapps/Decisions/2014/Jan14/224opn14-Decision.pdf.

Why Your EHR's Audit Functions Could Soon Change

If you're not using your electronic health record's (EHR's) audit functions, or over-using the copy-paste feature, the **Centers for Medicare & Medicaid Services** (CMS) could soon crack down on you. That's if the **HHS Office of Inspector General** (OIG) gets its way.

The OIG recently released a disappointing report, entitled "Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology." The report outlines findings mostly from an online questionnaire of 864 hospitals, with questions focusing on their use of Certified EHR Technology.

Although nearly all the surveyed hospitals had EHR technology with proper audit functions in place, many may not be using those functions to their full extent, the OIG found. Also, only about one-quarter of the hospitals had policies regarding the use of the copy-paste feature in their EHRs. The copy-paste feature, "if used improperly, could pose a fraud vulnerability," the OIG cautioned.

In some cases, the OIG also found that hospitals were often disabling EHR audit functions, according to an analysis by

the law firm **Nixon Peabody, LLC**. Based on the findings, the OIG made the following recommendations to CMS:

1. The Office of the National Coordinator (ONC) should propose a change to its EHR certification criteria to require that EHR technology keep audit logs operational whenever the technology is available to update or view records;

2. The ONC and CMS should develop a comprehensive plan to address fraud vulnerabilities in EHRs; and

3. CMS should develop guidance, in conjunction with hospitals, addressing the use of EHR's copy-paste feature.

Link: To view the full OIG report, go to http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf.