HCPro
a division of BLR

Strategies for Health Care Compliance

P4 **CAC implementation tips**
Two Cleveland Clinic administrators share their tips for implementing a computer-assisted coding system.

P5 **OCR ends 2013 with a bang**
OCR closed out 2013 by slapping a dermatology practice with a hefty fine and corrective action plan.

P6 **Safeguard your EHR**
A recent OIG report recommends using audit controls in your EHR to protect your organization against fraud.

P8 **Privacy and security of patient portals**
Get strategies for providing access to medical records through patient portals without sacrificing privacy and security.

P11 **2014 OPPS final rule**
CMS finalized changes to packaged services and clinic visit E/M coding.

Volume 18
Issue No. 4
APRIL 2014

No breach of PHI too small

The Omnibus Rule impact on unauthorized disclosures

Although the majority of the provisions of the HIPAA Omnibus Rule have become effective, many Breach Notification Rule revisions cause confusion for organizations.

"We know language has changed, but we're struggling to understand what that new language means and whether it really operationally has a significant impact on the number of incidents that are treated as breaches," says **Adam Greene, JD, MPH,** a partner at Davis Wright Tremaine, LLP, in Washington, D.C.

Organizations are now tasked with informing patients of smaller breaches that were likely internalized or only reported to HHS in the past. Pursuant to the HITECH Act, breaches affecting 500 or more individuals must be reported to HHS and are subsequently posted on its so-called "wall of shame." These are often large breaches that are the result of laptop computer theft or a security incident. But what about those smaller-scale, everyday breaches that are often the result of human error?

Facilities that have already taken a stringent approach with respect to breach notification may not see much difference in their operations under the new rule, according to Greene. Those that previously did not regard breaches involving an impermissible use or disclosure of PHI without evidence of harm as reportable may experience more difficulty adjusting to the changes.

"I think it's going to depend on how you interpreted the old rule," he says.

The Omnibus Rule definition of breach

The Omnibus Rule eliminated the "harm threshold," which required covered entities (CE) to report a breach only if it put affected individuals at significant risk. Now, a reportable breach is any use or disclosure of PHI that is not permitted by the HIPAA Privacy Rule.

Determining the true meaning of the word "compromised" with respect to PHI is a major issue for

Dermatology practice hit with fine

OCR ends 2013 with a bang and a familiar story

For OCR, 2013 ended with a bang, not a whimper.

As the year came to a close, OCR on December 26 announced it had reached a $150,000 settlement agreement and corrective action plan (CAP) over potential HIPAA violations with a dermatology practice with offices in Massachusetts and New Hampshire.

It was the first case brought against a covered entity (CE) for not having policies and procedures in place to address the breach notification provisions of the HITECH Act, OCR said in a press release. But otherwise, the details of the case with Adult & Pediatric Dermatology, PC, of Concord, Mass. (APDerm) sounded all too familiar. OCR began an investigation after receiving a report October 7, 2011, from the dermatology practice that an unencrypted thumb drive containing the ePHI of approximately 2,200 individuals was stolen from a staff member's vehicle. The thumb drive, which contained ePHI related to the performance of Mohs surgery—an advanced treatment procedure for skin cancer—was never recovered. As required by the HIPAA Breach of Notification Rule, APDerm notified its patients of the theft of the thumb drive within 30 days, as well as alerting the media and HHS.

OCR, which reports breaches affecting 500 or more individuals on its website *(http://tinyurl.com/2c3hhey),* has often warned about the risk of unencrypted mobile devices and the threat they pose to ePHI if lost or stolen.

"I'm getting tired of saying the same old, same old. I just want to say, come on people, get with it," says **Lesley Berkeyheiser,** cofounder of the consulting company N-Tegrity Solutions Group. She works out of the company's east coast office in Glen Mills, Penn. "I think the lesson for healthcare organizations is to please get the basics."

Another resolution agreement carries a cost

As well as seeking settlements with larger organizations to settle potential HIPAA violations that have resulted in payments or up to $4.3 million, OCR has recently brought settlements against less sizable organizations. The APDerm case reinforces the message that OCR is not letting small organizations, such as independent practitioners, off the hook when it comes to safeguarding patients' PHI, Berkeyheiser says. This is OCR's 17th resolution agreement since 2008.

The practice agreed to pay the relatively modest $150,000 to settle the case—an indication that while OCR wants to send the message that it expects all CEs to comply with HIPAA rules, it is not looking to put healthcare organizations out of business, says Berkeyheiser.

And the cost is relative. "No matter the size of the covered entity, a breach of PHI can have very expensive consequences," says **Bruce D, Armon, Esq.,** a healthcare attorney and partner at Saul Ewing, LLP, in Philadelphia.

As well as the hit to the pocketbook, there is also the cost to an organization's reputation, Berkeyheiser notes.

A failure to comply

OCR will require APDerm to implement a CAP to correct deficiencies in its HIPAA compliance program. OCR said its investigation revealed that the dermatology practice had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have written policies and procedures in place and train workforce members.

The CAP requires that APDerm develop a risk analysis and risk management plan to address and mitigate any security risks and vulnerabilities, as well as to provide an implementation report to OCR.

The agreement was signed December 24, 2013—a dubious Christmas present for any healthcare organization. You can view the resolution agreement at *www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/apderm-resolution-agreement.pdf.*

This latest case underscores how important it is for organizations to implement written policies and procedures to ensure HIPAA compliance, Armon says.