HEALTHCARE
BUSINESS MONTHLY
Coding | Billing | Auditing | Compliance | Practice Management

AAPC®
Advancing the Business of Healthcare

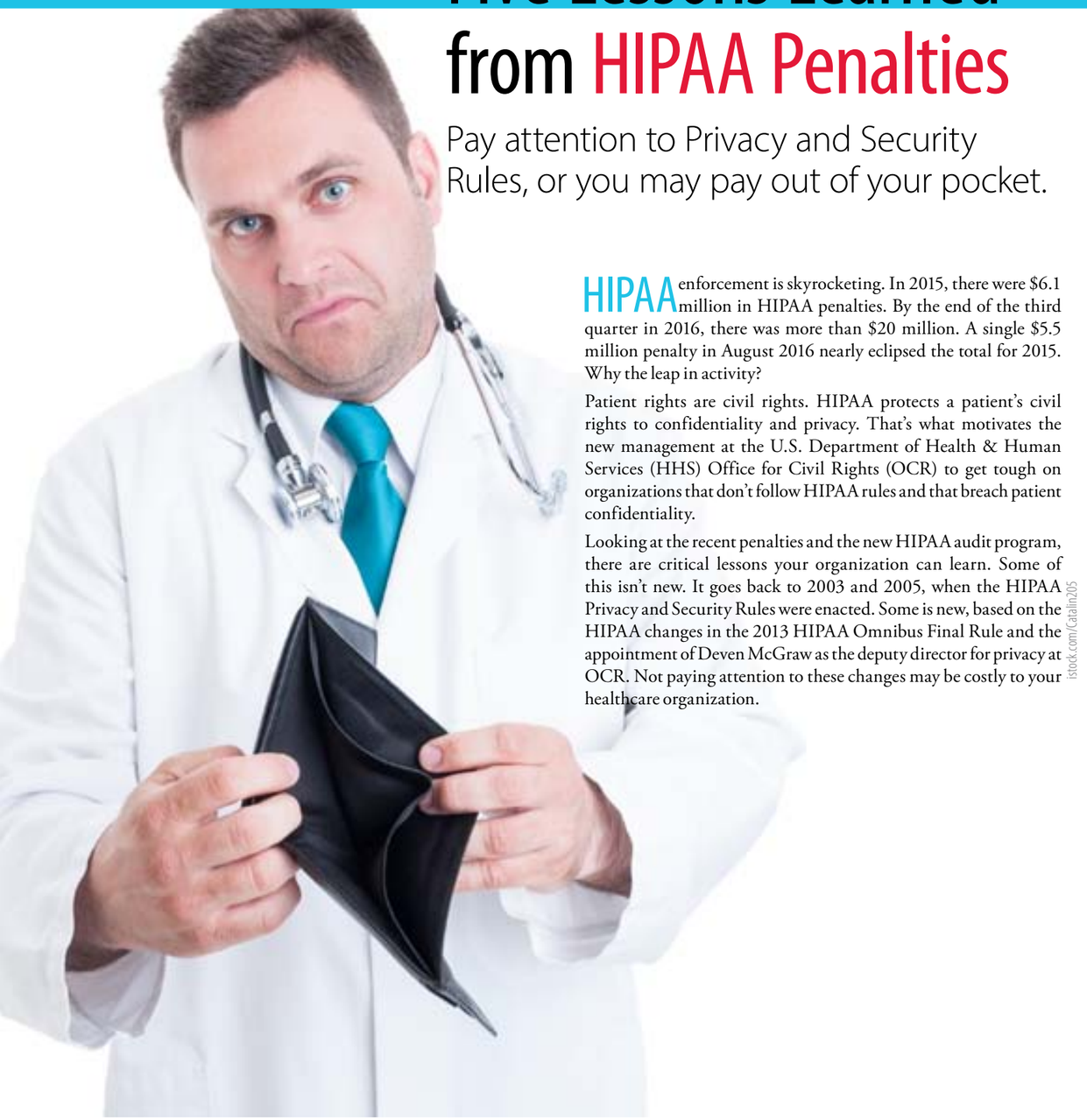
January 2017 www.aapc.com

2016 SALARY SURVEY: Pay Climbs for Credentials

By Mike Semel

Five Lessons Learned from HIPAA Penalties

Pay attention to Privacy and Security Rules, or you may pay out of your pocket.



istock.com/Catalin205

HIPAA enforcement is skyrocketing. In 2015, there were $6.1 million in HIPAA penalties. By the end of the third quarter in 2016, there was more than $20 million. A single $5.5 million penalty in August 2016 nearly eclipsed the total for 2015. Why the leap in activity?

Patient rights are civil rights. HIPAA protects a patient's civil rights to confidentiality and privacy. That's what motivates the new management at the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) to get tough on organizations that don't follow HIPAA rules and that breach patient confidentiality.

Looking at the recent penalties and the new HIPAA audit program, there are critical lessons your organization can learn. Some of this isn't new. It goes back to 2003 and 2005, when the HIPAA Privacy and Security Rules were enacted. Some is new, based on the HIPAA changes in the 2013 HIPAA Omnibus Final Rule and the appointment of Deven McGraw as the deputy director for privacy at OCR. Not paying attention to these changes may be costly to your healthcare organization.

The government has created model notices that are available for free: Use them.

LESSON 1:
Patient Paperwork Is Important

The new HIPAA audit program has started. OCR announced that the first organizations being audited for the Privacy Rule must submit their Notice of Privacy Practices for review, must have it posted in their offices and available for patients, and have it posted prominently on their website. The wording in the Notice of Privacy Practices must comply with changes in the 2013 HIPAA Omnibus Final Rule.

What is commonly seen during client assessments are:

- Notice of Privacy Practices that have not been changed since 2003, when HIPAA began;
- Notice of Privacy Practices that are given to new patients, but are not displayed in waiting areas; and
- No current Notice of Privacy Practices on an organization's website.

Practices also sometimes use a generic form on the internet, and only add their name. Some practices have a set of downloadable New Patient forms on their websites with a release that says the patient has been offered a Notice of Privacy Practices. This will not do! Your complete notice must be on the website, and new patients should receive a copy during their first visit. The government has created model notices that are available for free: Use them.

Action Point: Check to be sure your Notice of Privacy Practices meets the 2013 standards, is displayed and available in all your waiting areas, and is prominently displayed on your website.

LESSON 2:
Vendor Management Is Critical

Recent fines of $1.55 million, $2.7 million, and $400,000 were assessed to organizations that shared protected health information (PHI) with vendors without having a current Business Associate Agreement in place. Those fines make it worthwhile for you to identify each of your business associates, and to create or update contracts that include the required wording that changed in 2013.

Make sure your vendors understand that the 2013 HIPAA Omnibus Final Rule makes them liable for data breaches, and requires each business associate to implement a full HIPAA compliance program.

In June 2016, the first-ever penalty against a business associate was $650,000 for losing 412 nursing home resident records. In September 2016, a $400,000 fine was assessed against a business associate that lost a client's backup tapes.

If your healthcare organization is selected for a HIPAA audit, your business associates may be audited, too. If they fail, it might result in consequences for you.

Action Point: Have proper contracts for each of your business associates, indicating their commitment to HIPAA compliance. If a vendor won't sign a Business Associate Agreement, or think they don't have to do anything beyond signing the agreements, find another vendor.

LESSON 3:
Security Is Not Optional

No one likes the inconveniences required to secure data, any more than we like going through checkpoints at airports, government buildings, and sporting events. But it's now a part of our lives, and we have to get used to it.

The HIPAA Security Rule is a framework of information technology (IT) security requirements designed to protect health data against loss, theft, unauthorized access, or lack of availability. In today's world of increasing cyber threats, including ransomware, you can no longer get away with using an unsecured network that fails to incorporate strict requirements for auditing, data backups, and end-user security.

The first requirements in the HIPAA Security Rule are a security risk analysis and risk management. These are the two items the OCR is requesting in their Security Rule audits.

No one likes the inconveniences required to secure data, any more than we like going through checkpoints at airports, government buildings, and sporting events.

A $2.75 million penalty was assessed against an organization that allowed users to log in to their network using generic user names, in violation of the HIPAA requirement for unique user identification. A $2.7 million penalty was assessed for storing patient data with a consumer-class cloud service that would not sign a HIPAA Business Associate Agreement. Other penalties occurred for lost devices and lost backup tapes.

Most of these penalties noted that the organizations had not done a security risk analysis to identify the threats and vulnerabilities that could affect the security of their data. Some penalties were against organizations that did risk analyses, but failed to remediate the identified problems.

Action Point: Conduct a security risk analysis and fix identified problems. Check for weak points your in-house staff and IT vendors may have missed. Whether you have an IT staff or outsource your IT services, hiring an independent certified professional to conduct your risk analysis and compliance assessment is a good idea.

LESSON 4:
Encrypt Your Devices and Email

The aforementioned penalties for data loss could have been prevented if the data had been encrypted. HIPAA (and state data breach laws) exempt encrypted data loss from data breach reporting (as long as the encryption keys were not taken with the data).

New, business-class Windows 10 computers and new servers include encryption at no extra charge. Windows 7 computers can be encrypted for approximately $100, each. Cell phones and tablets can be easily encrypted. Portable media, such as thumb drives and universal serial bus (USB) hard drives, can be purchased with encryption.

Email should always go through a secure system. When sending PHI internally within your organization, you do not have to encrypt messages; however, all PHI sent outside of your internal email system must be encrypted. Email encryption is usually an add-on that must be configured by an IT professional, and requires users to be trained and audited to ensure they always encrypt messages containing PHI.

Action Point: Have an IT professional configure encryption on all of your computers, servers, mobile devices, and portable media. Set up email encryption; and make sure your users are trained and know they must encrypt all messages containing PHI that are sent outside of your organization. Encryption is the least-expensive way to prevent a reportable breach.

LESSON 5:
Don't Ignore Paper Records

Some of the aforementioned 2016 penalties were for confidentiality and privacy breaches caused by the mishandling of paper records. Some records were sent to the wrong recipients. Others were sent to mailing services that had not signed Business Associate Agreements.

Action Point: Review your processes for handling paper records, mailing bills and other correspondence, and storing records to comply with retention requirements.

These are all fairly small changes that can prevent very large penalties. We are all patients, so these changes will protect your civil rights, too. **HBM**

Mike Semel is president and chief compliance officer for Semel Consulting. He has owned IT businesses for over 30 years, and has served as the chief information officer for a hospital and a K-12 school district. Semel is recognized as a HIPAA thought leader throughout the healthcare and IT industries, and has spoken at numerous conferences including AAPC, NASA Occupational Health, and the New York State Cybersecurity conference. He has written HIPAA certification classes and consults with healthcare organizations and business associates to help build strong cybersecurity and compliance programs. Semel can be reached at 888-997-3635, ext. 101 or mike@semelconsulting.com.

Resource

Model Notices of Privacy Practices may be found on the HHS website: www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/