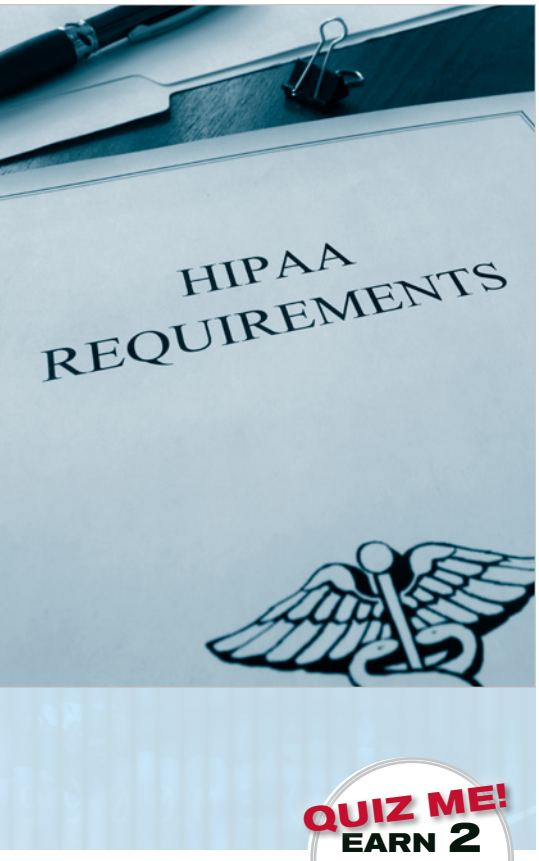
By **DEVON BERNARD**

# Help With HIPAA

Tips for ensuring compliance with the regulations that protect patients' private health information

**CE CREDITS** ***Editor's Note:*** Readers of *Compliance Corner* are now eligible to earn two CE credits. After reading this column, simply scan the QR code or use the link on page 39 to take the *Compliance Corner* quiz. Receive a score of at least 80 percent, and AOPA will transmit the information to the certifying boards.




QUIZ ME! EARN 2 BUSINESS CE CREDITS P.39

**What does the Health Insurance Portability and Accountability Act (HIPAA) mean for O&P professionals?**

In a nutshell, HIPAA and subsequent regulations require you to do five things: Put safeguards or protocols in place regarding patients' protected health information (PHI); reasonably or cautiously limit the exposure or uses of the PHI to the minimum necessary amount to complete your intended goal (billing, for example); create procedures that limit who may access or view PHI; implement a training program for all employees on how to protect PHI; and create a way to notify a patient if his or her PHI has been compromised or breached, and understand how to identify if PHI has been compromised or breached.

**OVER THE PAST FEW YEARS,** as the health-care arena has become more complex and health data more frequently shared, the five obligations outlined in HIPAA have become more important. HIPAA compliance is under increased scrutiny as enforcement activities have been ramped up due to the increased use and availability of PHI. The Office for Civil Rights (OCR), the entity charged with enforcing HIPAA, now conducts periodic audits on its own to gauge your compliance with the HIPAA Privacy, Security, and Breach Notification Rules—which are in addition to the audits and investigations OCR conducts as a result of a complaint or other issues. The consequences for not being compliant have become more substantial and frequent as well.

OCR uses a tiered approach for issuing civil monetary penalties, or fines, for HIPAA violations and/or noncompliance; these penalties range from $100 to $50,000 per violation, with a maximum penalty of $1.5 million per year for violations of an identical violation. The amount of the fine is based on your level of compliance or negligence and the number of patients involved.

The first tier is "did not know" or "reasonable diligence" violations. These are HIPAA violations that occur without your knowledge and could not have been foreseen due to the policies and procedures you have established. These violations may occur because you may not have had a complete understanding of the laws. In these cases, the minimum penalty is $100 per violation, not to surpass $25,000 in one year for the same violation.

The second tier is "reasonable cause," or a violation where you were unable to comply with the HIPAA standards, but made attempts to become compliant. This means you attempted to comply, but for some reason were unable to do so; you were not intentionally ignoring the laws. In these cases, the minimum penalty is $1,000 per violation, not to surpass $100,000 in one year for the same violation.

Tiers three and tier four are linked because they both hinge on the term "willful neglect." This means that you intentionally or willfully ignored your obligations under HIPAA. Tier three will be applied if you take actions to correct your shortcomings and violations. This tier carries a minimum penalty of $10,000 per violation, not to surpass $250,000 in one year for the same violation. If no attempt is made to correct the violation, tier four will apply, and the penalty will be a minimum of $50,000 per violation, not to surpass $1.5 million in one year for the same violation.

The maximum amount for a violation in any tier is set at $50,000 per violation, with an annual maximum of $1.5 million. In addition to monetary penalties, you also may be subject to criminal penalties, including jail time. The jail time may range between one and 10 years.

To help avoid these costly penalties and ensure compliance with HIPAA standards for privacy, security, and breaches, here are some examples of the top reasons companies and individuals have been found to have violated HIPAA. These examples come from OCR's "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." It is a complete list of all breaches (the access/use/disclosure of unsecured PHI, in a manner not permitted by HIPAA, which poses a significant risk of harm to the affected individual) affecting 500 or more individuals, and it currently includes 1,847 separate incidents.

## Lost or Stolen Devices

Of the 1,847 incidents included in the "Breach Portal," 924 were listed as lost or stolen; 604 of the lost or stolen items were described as a laptop or other portable device. This means that 32 percent of the reported breaches of health information result from a lost or stolen device.

The U.S. Department of Health & Human Services (HHS) has created a list of 11 tips for protecting and securing PHI when using a portable device:

1. Use passwords or other forms of authentication to gain access to the device and the files located on the device. It is suggested that the password be at least six characters long and include a combination of upper- and lowercase letters, numbers, and symbols, and that you change passwords on a routine basis.
2. Install and enable some form of encryption software or apps or similar features on your devices.
3. Have the ability to activate remote disabling and/or wiping. (This is especially handy if your device is lost or stolen.) Remote wiping is a security feature that enables you to remotely erase the data on a mobile device; remote disabling is a security feature that enables you to remotely lock or completely erase data stored on a mobile device. Many current portable devices already include these features, but you must be sure the features are activated and being used.
4. Consider disabling and/or not installing file sharing applications, as these can be a way for people to access your files without your knowledge.
5. Install and activate a firewall. Once again, most devices and operating systems already have a firewall, but you must be sure it has been activated.
6. Use some type of security software.
7. Ensure your security software is up to date.
8. Before downloading any new applications, research them and understand how they work. For example, some apps may need to copy your files in order to work; these apps would jeopardize the health data stored on your phone.
9. Maintain physical control of your mobile device, as devices such as phones and tablets can be easily misplaced. Some methods of control include securing the device when it is not in use (via a locker or secure room, or by locking the screen) and making sure no one else uses the device.
10. Take precautions when using wifi networks. Use secured networks if you intend to transmit any health data, and use secured browsers. It also is suggested that you turn off wifi features when you are not using them.
11. Delete all stored health information. This is critical when you are replacing or upgrading your current devices. Consider using some type of "overwriting" software, and do not rely on the "delete" button, or emptying your trash, to achieve deletions.

For more information regarding securing electronic health information, including conducting risk analyses, visit *www.healthit.gov*.

## Hacking

Nearly 300 of the 1,847 listed instances of breaches on the OCR website (282) were self-reported as being related to hacking/IT issues. To combat hacking issues, you can employ some of the same guidance given for protecting mobile devices. This includes using strong passwords (six or more characters, upper- and lowercase, etc.) and changing passwords on a regular basis. Also, be sure you are using firewalls, and that firewalls are maintained, updated, and adequate for your needs. Next, be sure your security software is routinely updated and is capable of searching out the newest versions of malware and viruses.

> Be sure you are using firewalls, and that firewalls are maintained, updated, and adequate for your needs.

In addition, ensure information is encrypted—and encrypted to a standard acceptable under HIPAA. Note that while encryption is not necessarily a HIPAA requirement (your data/health information is not required to be encrypted as long as you have other safeguards in place), the HIPAA regulations are clear that one of the only ways information is considered absolutely secured (unusable, unreadable, etc.) is via encryption. So, if the health information you are using is encrypted, that provides one more layer of protection, especially when dealing with breaches. For maximum security, ensure data is being encrypted during all phases of usage: transmission, rest, and storage.

Another tool to safeguard against hacking is to have proper training and protocols in place. The training does not need to be technical or intense, but it's important to educate your staff about potential threats and malicious software so they are able to identify it and report it. Also, make sure that everyone knows what links and attachments are secure and valid, and what to do if a staff member opens a link or attachment that should not have been opened.

Finally, to prevent hacking or to limit the effects of hacking, talk to your information technology (IT) department to ensure the steps outlined above are being taken. If you don't have an IT department, you may want to speak with an IT consultant, preferably one with knowledge about HIPAA, and run an assessment of your vulnerabilities and risk.

## Improper Disposal

Improper disposal accounted for 65 of the 1,847 breaches listed on the OCR website. When disposing of records, ensure that the information is made unreadable/indecipherable and unable to be reconstructed. For paper files or records, consider measures such as shredding or burning, or a means that ensures total destruction. Besides encryption, destruction is the only other way, under HIPAA, to ensure that health information is considered secured.

For electronic records and files, proper disposal includes using software to overwrite the files or destroying the hard drive. This is especially important when you are disposing of old laptops, computers, or thumb drives, but you should check other equipment as well. Fax machines and copiers may store information on their hard drives, so be sure these are erased on a regular basis—especially if you are leasing the equipment.

## Unauthorized Access/Disclosure

Unauthorized access and/or disclosures accounted for 462 of the 1,847 breaches listed on the OCR website, accounting for roughly 25 percent of the breaches—the second biggest reason for breaches.

Disclosures are the means in which you communicate PHI to an outside entity, and these are allowed under HIPAA in many circumstances—for example, PHI may be emailed to a physician for treatment or to your billing company for billing, as long as it is communicated under secure measures. However, some disclosures are not allowed; under HIPAA, only certain people are allowed to access the data.

PHOTO: Getty/Welcomia

Some examples of unauthorized access/disclosures include the following:

- Not obtaining proper authorization to use patient videos or testimonials for your website or marketing materials.
- Insider peeking or people within your company looking at patients' charts, when they have no need to view the charts as part of their daily duties.
- Sending/releasing the wrong patient's information.
- Not having or using business associate agreements (BAAs), when required.

It's important to ensure that no one accesses a patient's medical records without proper authorization or approval as directed by your policy and procedures manual or under an employee's job description and duties. If you use electronic health records, consider instituting tracking systems and/or clearance level passwords to prevent unauthorized access. Also, review all current BAAs to make sure they are up to date and valid, and review your interactions with other individuals and companies to determine if you need BAAs.

## Protecting Your Facility

These are just some examples of HIPAA compliance issues that could impact an O&P facility. To review other issues related to HIPAA compliance, visit the OCR website and search under "HIPAA Compliance and Enforcement." There you may review resolution agreements and other case examples. If you review a case example, resolution agreement, or another issue addressed above and identify a similar issue within your organization and realize you may be vulnerable, be sure to address the issue and, if necessary, update your training and procedures.

Remember that you can best ensure patients' privacy needs are met—and reduce the amounts you may be fined should a breach occur—if you implement a strong and reliable training program, maintain proof that everyone has received proper training, and show that you are doing your "due diligence." CP

***Devon Bernard*** *is AOPA's assistant director of coding and reimbursement services, education, and programming. Reach him at* dbernard@aopanet.org.

Take advantage of the opportunity to earn two CE credits today! Take the quiz by scanning the QR code or visit ***bit.ly/OPalmanacQuiz.***

**Earn CE credits accepted by certifying boards:**