By **DEVON BERNARD**

Breach Etiquette

Follow HIPAA's rules for making notifications once a breach has occurred

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 34 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.34

THE CHANGES TO THE Health Insurance Portability and Accountability Act (HIPAA) that took place in 2010 and late 2013 have made an impact on O&P—especially with regard to the occurrence of breaches of patients' protected health information (PHI) and individually identifiable health information and the requirements of notifying the appropriate entities of those breaches. Under HIPAA, practitioners have the burden of proving compliance with the Breach Notification Rule and proving that all of the required notifications have been made. This month's *Compliance Corner* reviews who must be notified of breaches and when those notifications must be made.

A "breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI. Impermissible use or disclosure of PHI will be presumed to be a breach unless it is demonstrated or documented through a risk analysis that there is a low probability that the PHI has been compromised.

Identifying when a breach occurred and how many individuals have been affected is key to determining which type of notification a health-care professional is required to make. Below are explanations of the four types of notices and the timeframes during which the notifications must be made.

Notices to Individuals

You are required to notify each individual patient when a breach of his or her PHI has occurred and has been discovered, regardless of the number of individuals affected by the breach. A breach is considered "discovered" on the date you learn of the breach, and not on the date the breach actually occurred. The approved, and primary, method of notification is a written notice via first-class mail. However, it also is acceptable to use email if a patient has given you permission to contact him or her via email. Regardless of the method, the notification must be made within 60 days of the discovery of the breach.

What type of information must you include in the written notice? First, include a brief description of the breach, describing the types of information that may have been involved in the breach. For example, did the breach include the individual's name and Social Security number, or did the breach only include his or her name and birthdate? Be sure to clarify when the breach may have occurred.

Second, explain what you are doing in response. Describe what you are doing to investigate the breach, and what you are doing to limit the harm to the patient. You may want provide details regarding what you will do to prevent future breaches.

Next, describe what the affected patient may do to limit the potential harm from the breach. This may include suggesting that the individual contact his or her banks and credit card companies,

or monitor his or her credit score.

Finally, include contact information for the individual within your company the patient may contact with questions. The contact person should be your compliance officer or a staff member with knowledge about breaches and HIPAA. If the breach was the result of or included one of your business associates, offer contact information for that business associate.

What if your contact information for affected parties is out of date? In situations where you have inaccurate or out-of-date information, the method you must use to attempt to contact the affected individuals depends on the number of individuals for which you have incomplete, inaccurate, or out-of-date information.

If the breach included 10 or more people for whom you do not have sufficient contact information, you must post a notice on your website for at least 90 days indicating that a breach has occurred and asking patients to contact you to learn if their information was involved (the notice does not need to list the individuals affected). You also may provide a notice to the media—a local newspaper or TV station in the area in which you believe the individual resides—and should include a toll-free contact number.

If you have out-of-date contact information for fewer than 10 individuals, then you may contact the affected individuals via telephone or any other means of contact at your disposal, such as email or text messages.

Notices to Media

While you are not required to notify the media for each individual breach that occurs at one of your facilities or offices, you must notify the local media if you experience a breach that includes or has the possibility to include more than 500 individuals. "Local media" includes TV, radio, and newspaper offices in the area where the affected individuals live.

The most effective way to accomplish this notification is to create and distribute a press release to the appropriate media channels. The press release should include all of the information you would have provided in the individual written notices discussed above.

As with the individual written notices, the notification to the media must be made without any delays and in no case later than 60 days following the discovery of a breach involving more than 500 individuals.

Notices to HHS

How and when you must notify the secretary of the Department of Health & Human Services (HHS) depends on the number of individuals affected or possibly affected by the breach; as with the requirement of notifying the media, the magic number is 500.

If a breach affects less than 500 individuals, you must notify the secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. This means that any breaches involving less than 500 individuals that occurred and were discovered in 2015 must be reported to the secretary by March 1, 2016. You are not required to wait until the end of the year to report the breach or breaches to the secretary; you may report them as they occur.

The notification must be completed electronically via the breach portal on the HHS Office of Civil Rights website: *https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf*. Have the following information ready when accessing the portal: when the breach occurred, when it was discovered, what was breached, what you did to correct the breach, and what steps you took in notifying the patients.

If the breach affects more than 500 individuals, you must notify the secretary immediately and without any unreasonable delay, but in no case later than 60 calendar days from the discovery of the breach. Use the same breach portal discussed above.

Notices to Business Associates

If you are acting as or considered a business associate (BA) to another covered entity, then you also may be required to notify individuals of a breach, if the covered entity has delegated this responsibility to you under your business associates agreement. If this is the case, you would follow all the breach notification protocols discussed above.

If the individual notification duties were not delegated to you as a BA, you

would, at a minimum, be required to notify the covered entity that a breach has occurred and that you discovered the breach. You must provide this notice to the covered entity without any delays and no later than 60 days from the day you discovered the breach. Your notification should include the identification of each individual affected by the breach, and any other information the covered entity may need as part of its notification to the individuals affected by the breach; this may include what type of information was breached, what is being done to correct the breach, etc.

Documenting Disclosures

It's important to know what to do if you need to document and demonstrate that a breach did not occur and that a proper notification was not required.

First, your risk assessment should demonstrate a low probability that PHI has been compromised by impermissible use or disclosure. A valid and basic risk analysis should include the following steps:

- Examine the unauthorized person who used the PHI or to whom the disclosure was made. Is the person/entity required to follow HIPAA?
- Determine if the PHI was actually acquired/viewed. Was the information encrypted?
- Evaluate the type and amount of information that was accessed, used, or disclosed and the nature and the extent of the PHI. Is it sensitive information—for example, Social Security numbers? What type of information was disclosed and used—for example, clinical information?
- Establish the extent to which the risk to the PHI has been mitigated. Were there corrective steps taken to stop future or further disclosures?

Second, in addition to a low probability that PHI has been compromised, there are three exceptions to the definition of breach that would not require you to make a notification.

The first exception applies to the acquisition, access, or use of PHI by any employee, if such acquisition, access,

or use was made in good faith and within the scope of authority granted to the employee, and does not result in further use or disclosure in a manner not permitted by the privacy rule. An example of this would occur if your biller pulls the wrong file of a patient by mistake. There is no breach because the access of the file was done during routine work under his or her authority and did not result in any further uses or disclosures.

The second exception applies to the inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another person at the same covered entity or business associate, or at an organized health-care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the privacy rule. For example, this exception would apply if you send a detailed prescription to the wrong referring physician, you realize what occurred, and you correct the action—and the PHI is not disclosed or used any further. There is no breach because all parties were authorized to view the PHI, and are bound by HIPAA not to disclose or use the PHI.

The final exception applies if you have a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

Record Keeping

Since you have the burden of proving you are compliant with the Breach Notification Rule and that all of the required notifications have been made, or that a breach did not occur and a notification was not required, consider creating and maintaining a record, or log, of all breaches or suspected breaches that may have occurred during any calendar year. Your log may include the results of your risk analyses, the dates that any breaches occurred or the date you discovered the breaches, a description of the breaches, the number of individuals affected, a description of who was notified of the breaches, and all actions taken to correct the breaches. This type of log will be helpful when you make your yearly report to the secretary of Medicare.

Keep in mind that you must meet certain administrative requirements to be considered compliant with the Breach Notification Rules. For example, you must have in place written policies and procedures regarding breach notifications, you must train employees on these policies and procedures, and you must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

Adhering to the Breach Notification Rule can take a lot of time and documentation, but protecting your patients' privacy is well worth the extra work.

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:

BOC www.bocusa.org