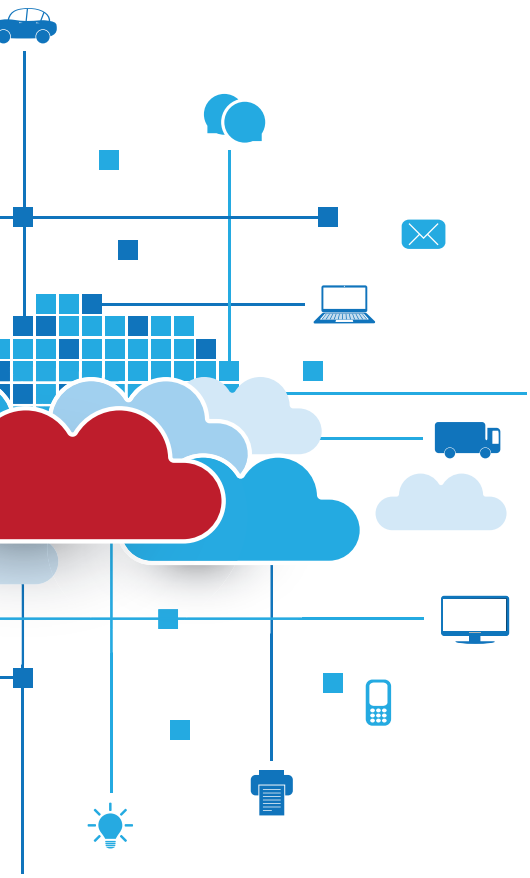
By **DEVON BERNARD**

Getting Down to Business

Know the rules for identifying business associates and understanding a patient's right to access information

QUIZ ME! EARN 2 BUSINESS CE CREDITS P.39

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.



It may be tempting to put issues related to the Health Insurance Portability and Accountability ACT (HIPAA) on the backburner or to create a policy and forget about it. But doing so could be costly as fines for HIPAA violations are on the rise.

This month's *Compliance Corner* takes a look at two components of the HIPAA regulations: business associates/business associate agreements and a patient's right to access information.

Business Associates and Agreements

A business associate (BA) is a person or entity, including a subcontractor, which provides services on behalf of or to covered entities, and requires the use and disclosure of protected health information (PHI) or electronic protected health information (ePHI). The BA also creates, receives, maintains, or transmits PHI on behalf of a covered entity. PHI, also called individually identifiable health information, is information created by a health-care provider that is used to identify an individual for the purpose of treatment and billing.

PHI may include information such as the new Medicare Beneficiary Identifier (MBI) numbers, Social Security numbers, names, birth dates, addresses, and similar data. But this information by itself is not always considered PHI; to be considered PHI, the information must be used and related to the provision/billing of health care or the patient's condition. For example, if a patient's email address is listed by his or her employer or in some other directory, the email would not be considered PHI; but if the information is listed with payment information, then it could be considered PHI.

It is easy to identify third-party billers, clearinghouses, or accrediting/credentialing organizations as business associates; and it is easy to identify non-business associates, such as hospitals, referring physicians, or an Internet provider. However, some of the other entities you work with may not be as clear cut—entities such as manufacturers and cloud computing service providers.

If you are using a cloud computing service provider for the purpose of storing or maintaining your files, including ePHI, then the provider would be considered a BA. This is true even if the cloud service provider is storing encrypted ePHI and is never viewing the information. The service provider is considered a BA because it is storing and maintaining the ePHI on behalf of you, the covered entity.

With manufacturers, suppliers, and distributors, identifying whether they should be considered BAs is more difficult and depends on what functions they provide, as well as what functions they provide to *you*. In most instances, under the HIPAA Privacy Rule, device manufacturers would be considered health-care providers because they are providing services, support, guidance, or supplies related

to the care of a patient—and as such they would not be considered a BA.

In other instances, however, manufacturers, suppliers, and distributors could be considered BAs—for example, if they are providing you and the patient a cost-savings estimate or analysis of a particular product/service over another, and they require access to certain PHI/ePHI. In addition, if a manufacturer or distributor simply sells its products to you and you deliver the items, it could be considered a BA if you are providing it with PHI/ePHI.

When dealing with BAs, you are required to have a business associate agreement (BAA) in place. The BAA is a contract between you (the covered entity) and the BA that provides assurances that the BA is properly handling and safeguarding PHI and/or ePHI. The BAA also lays the groundwork for the types of services the BA will perform for you and the amount of PHI/ePHI the BA requires to carry out these activities, as well as when the BA will have access to this information.

To help determine if someone is a potential BA and if a BAA is required, consider the following:

- **Is the PHI/ePHI being disclosed to someone in the capacity of his or her job as a member of your workforce?** If yes, then a BAA would not be required. If no, then a BAA may be required.
- **Is the PHI/ePHI being disclosed to a health-care provider for treatment purposes?** If yes, then a BAA would not be required. If no, then a BAA may be required.
- **Is the PHI being disclosed to a health plan/insurer for payment purposes?** If yes, then a BAA would not be required. If no, then a BAA may be required.
- **Is the PHI being disclosed to another covered entity?** If yes, then a BAA is not required. If no, then a BAA may be required.
- **Does the entity or individual receive, maintain, or transmit PHI/ePHI for the purpose of any of the following activities: claims processing, administration, data analysis, utilization review, quality assurance, patient safety activities, billing, benefits management, practice management, etc.?** If yes, then a BAA is required. If no, then a BAA may not be required.
- **Does the entity or individual provide you with any of the following services, and the services require the disclosure of PHI/ePHI: legal, accounting, consulting, data aggregation, management, administrative, accreditation, or financial?** If yes, then a BAA would be required. If no, then a BAA may not be required.

Once you have determined if an entity is a BA and whether a BAA is required, the next step is to create a BAA. There is no one standard form or document; the format of the BAA depends on the type of work the BA is doing and the amount of information needed to complete the job(s).

However, at a minimum, a BAA should accomplish the following 10 goals:

- Establish what uses and disclosures are permitted by the BA.
- Establish that no other uses or disclosures of PHI/ePHI are allowed unless granted by the BAA or as required by law.
- Require that the BA implement appropriate safeguards to prevent unauthorized use or disclosure of PHI/ePHI.
- Require the BA to report any uses or disclosures of PHI/ePHI not provided for by its contract, including the reporting of breaches of unsecured PHI/ePHI.
- Require the BA to assist you with granting individuals access to their PHI/ePHI, amending their PHI/ePHI, and/or accounting of disclosures of their PHI/ePHI.
- To the extent the BA is to carry out a covered entity's obligation under the Privacy Rule, require that the BA comply with the requirements of the Privacy Rule.
- Require the BA to make available its internal practices, books, and records relating to the use and disclosure of PHI/ePHI, and to make them available to Medicare or its contractors.
- Require that at the termination of the BAA, the BA return or destroy all PHI/ePHI.
- Require the BA to ensure that any subcontractors it may engage on its behalf that will have access to PHI/ePHI agree to the same restrictions and conditions that apply to the BA with respect to the PHI/ePHI.
- Be sure the BA provides you with the authority to terminate the BAA if the BA violates a material term of the BAA.

These 10 elements are just the basic items to be addressed within your BAAs. You should create agreements that are specific to your needs and the actions performed by your BAs.

If you are still uncertain if an individual or entity is acting as a BA, consult with your attorneys or consider having the BA sign a BAA. However, individuals or entities may be less inclined to sign a BAA if they are not required to do so, especially when it may place an undue burden on them. Also, be sure to review your BAAs carefully and make sure they are not imposing any unnecessary burdens or liabilities on you.

Patient's Right to Access Information

Patients have a right to access—to simply view or receive copies of—a wide range of information about themselves and their care, even if the information is maintained by you or by a BA or subcontractor on your behalf in a designated record set (i.e., medical records, billing records, payment and claims records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals) for as long as the records exist. Patients also may request that this information be forwarded to a third party.

However, patients may not request access to PHI/ePHI or other information if it is not part of a designated record set because the information is not used to make decisions about the patient's care. This type of information may include quality assessments or quality control records, patient safety records, or management records that are used for business decisions rather than to make decisions about individuals and/or their care. For example, an individual does not have the right to access information related to your purchasing costs but may have the right to access the billing records or payment records.

There also is a mandatory exemption to the right to access information for psychotherapy notes and any information that may be related to any pending legal cases.

How patients request access is up to you as a covered entity. You may require that patients request access in writing, or you may use an in-house form or online portal.

Regardless of the method, the patient must be informed of your procedures to request access—for example, via your Notice of Privacy Practices. In addition, your method for requesting access must not create barriers or burdens to patients or unreasonably delay the patient in accessing the requested information. This would include requiring patients to come into your office in person to complete forms or to fill them out in triplicate.

In granting access to the patient, you are required to provide access to the PHI/ePHI and information requested, in whole or in part, no later than 30 calendar days from receiving the individual's request. But it should be done as soon as possible. If, for some reason, you are unable to provide access and complete the request within 30 days, you may extend the time, one time only, by an additional 30 days. When extending the timeframe, you must notify the patient in writing of the reasons for the delay and the date by which you will provide access and complete the request.

A patient's access to all or a portion of the information requested can be denied if the information is not part of a designated record set maintained by you or your BAs, or if the information is exempted from the right of access because it constitutes psychotherapy notes or is part of a legal proceeding. However, you may not withhold or deny an individual access to his or her PHI/ePHI on the grounds that he or she owes you money for other services or care provided. If you are denying access, in whole or in part, you must provide the reason in writing to the patient no later than 30 days after the request.

As part of the patient's request to access select information, the patient also may request that the information

be provided in a desired format, such as via hard copy or electronic copy. You are obligated to provide the information in the form and format requested, if it is easy and readily available.

If the patient is requesting copies—and not simply requesting to view the information—you may charge the patient a reasonable fee for the service of producing a copy on his or her behalf. If the patient makes copies on his or her own, or uses his or her mobile device to take pictures while viewing the chart and records, you may not charge the patient.

The reasonable, cost-based fee to provide the patient or his or her representative with a copy of PHI/ePHI, or to provide a copy to a designated third party, may be based on either *actual costs* or *average costs*, but the fee should not be so high as to create barriers or persuade the patient against exercising his or her right to access the information.

If you use *actual costs* as the basis for your fee, you may only include the cost of certain labor, supplies, and postage per request. The labor portion of your charge may only include the labor associated with creating and delivering the requested information in the form and format requested or

agreed upon by the patient or his or her representative. The labor for copying should not include the costs or time associated with reviewing the request for access, or searching for and retrieving the information requested. The charge for supplies would include things like paper if the request is for a hard copy, or a disk or USB drive if that is the format the patient has requested. Postage may be charged when the patient requests that the copy be mailed.

If you use *average costs*, you are not calculating your labor costs for each request; instead, you may use a flat cost based on the average amount of labor used in previous requests, and then factor in your supply costs and postage costs, if applicable. If you maintain all PHI electronically and the patient is requesting an electronic copy, you also have the option of simply charging a flat fee, which may not exceed $6.50 per request.

A Good Start

The information provided here is not a complete list of your responsibilities regarding BAs/BAAs and a patient's rights to access information. However, it does provide you with a good framework to understand your obligations and determine whether you are on the right path to compliance. O&P

***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