



Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

JULY 2018



**Local expertise,
regional teams,
and multinational
compliance**

an interview with
Jonathan Turner

by Jason Throckmorton, BS CHC

Tracking business associate agreements: Where are yours?

- » Obtain assurance from business associates that PHI will be safeguarded.
- » Assurances must be in writing.
- » OCR audits may request a list of business associates.
- » Agreements can be stand-alone or part of a contract.
- » Your legal counsel should approve any changes to the agreement.

Jason Throckmorton (throckmj@somc.org) is Information Security Auditor at Southern Ohio Medical Center in Portsmouth, OH.

Managing business associates and keeping track of the business associate agreements that come with them is part of the Health Insurance Portability and Accountability Act (HIPAA) compliance process. Tracking those business associate agreements (BAA) can be a tiresome journey if you do not have sole control over their issuance. However, with some organizational measures, you can turn this into a manageable task.



Throckmorton

By law, the HIPAA Privacy Rule applies only to covered entities—health plans, healthcare clearinghouses, and certain healthcare providers. However, most healthcare providers and health plans do not carry out all of their healthcare activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information (PHI) to these “business associates” if the providers or plans obtain satisfactory assurances that the business associate will use the information only

for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity’s duties under the Privacy Rule.¹

The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.²

This is where you need to start keeping track of the BAAs. As a covered entity, if you ever fall under an Office for Civil Rights (OCR) audit, you may possibly be asked to submit a list of your organization’s business associates. If you are not privileged to be the “keeper” of the BAAs, then you may not have, or be able to come up with, an accurate list. This is where tracking can become difficult.

Who or what is a business associate?

According to the Department of Health and Human Services, a business associate is “a person or entity that performs certain functions or activities that involve the use or

disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity.”³ Basically then, a business associate is any vendor that you contract with to do work for you that you could do yourself. Therefore, covered entities could have several dozen or even hundreds of business associates, and with each one comes a BAA. Here are just a few examples of business associates:

- ▶ Claims processing provider
- ▶ Outside legal counsel
- ▶ Data storage host
- ▶ Document destruction vendor

Business associate agreements can be stand-alone documents, included within a contract, or added to a contract as an appendix.

The agreement can be generated by the covered entity or the business associate. Typically, if the covered entity generates the agreement, then it is a stand-alone document. If the business associate generates the agreement, it is usually a part of the contract. Now this is where it can get complicated.

If your organization distributes its BAA to anyone within the organization who can sign a contract, then you may not even be aware of the existence of some or several BAAs. Although we, as compliance professionals, are aware of the importance of entering into and tracking BAAs, our colleagues who are not so well-versed in the field of Compliance may not be. If this is the case, there could be two possible outcomes. One is that a contract could be entered into between a covered entity and a business associate without having a signed BAA. The other is that a BAA could be signed and filed away with the contract and no one,

other than the person signing the contract, realizes that the agreement exists. In either case, it is not a good result.

When the BAA is part of the contract, the person signing the contract may not even be aware of what a BAA is, overlook its importance, agree to the terms, and simply sign it. The contract is then filed away, and the BAA is more than likely forgotten about.

If your business associate agreements are handled as above, in the event of an OCR audit, it could take several days or even weeks to determine who your business associates are and find the BAAs with each of them if need be. What is worse is that you may not even be able to account for all of your business associates, which could trigger a “full blown” audit.

...in the event of an OCR audit, it could take several days or even weeks to determine who your business associates are...

Managing BAAs

If you want to make tracking easier, ask your executive staff to let you be the “keeper” of the BAAs, and educate everyone who is authorized to enter into contracts on what a business associate is and the

importance of having a BAA with them. By doing this, you should have a good knowledge of who your business associates are and be able to keep track of them and the agreements that come with them.

The easiest way to accomplish this is to be the only one with a working copy of the BAA. This way, no one can send out an agreement without you knowing about it. Sounds like a “power trip” but it works. Actually, a few other people in your organization should have a copy, but just a few, such as the chief executive officer, chief compliance officer, or legal counsel. However, everyone else knows to ask you for a copy when they need one.

When a copy of the BAA is requested, be sure to get the name of the business associate and nature of service that they will be providing to your organization. Type the name of the business associate into the agreement and get it signed by your company's authorized signer prior to sending the agreement out. Be sure and ask the business associate for a counter-signed copy to be returned to you for your record keeping. For tracking purposes, keep a list of each business associate along with their contact information, what services they are providing, the name of your organization's department and manager who is contracting with the business associate, and the date that the agreement was signed by the business associate. This will be a lifesaver if you are ever audited.

In the event that the business associate requests to use *their* BAA, be sure to send it to your Legal department for review prior to having it signed. Likewise, if they want to suggest changes or "red-line" your organization's

BAA, be sure to have those changes approved by your legal counsel. One would think that these agreements are all the same, but this is not always the case. Some business associates will sign and return your BAA with no questions asked. However, others will go through multiple red pens suggesting changes that are mostly in their favor.

Once the final version of the BAA is signed by both parties, keep an electronic copy and a hard copy of the agreement. You may also want to keep any email correspondence with business associates if you need to refer to that for future reference.

Conclusion

Keeping track of business associates and the BAAs that come with them can be difficult but, with some education and cooperation, it can be done. 📧

1. HHS.gov: Health Information Privacy: Business Associates. Available at <http://bit.ly/2GPOb91l>
2. Idem.
3. Idem.

TRAIN YOUR EMPLOYEES WITH HCCA'S TOP-RATED DVD

Compliance and Ethics:

An Introduction for Health Care Professionals

HCCA's video provides everything you need to conduct compliance and ethics training...

- 23-minute video with seven dramatizations (available in DVD)
- Trainer's Guide with suggested program agendas and discussion outlines
- Reproducible participant materials
- DVD includes viewer's menu for easy customization of training sessions

HCCA member price \$350 | non-member price \$395

Visit hcca-info.org for more information and to order.

Published by Health Care Compliance Association (HCCA) Copyright © 2018 HCCA. All rights reserved.

