

COMPLIANCE CONNECTION

Business Associate Agreement (BAA): What Is It and Why Do I Need One?



As our “new normal” evolves to include telework, videoconferencing, and other telecommunication platforms you may be asked to participate or provide information to other companies, electronic platforms or software vendors in an effort to continue our work in the “social distancing, new normal” environment. Before you do—be sure to know whether or not there is a business associate agreement (BAA) in place. This requirement also applies to any other vendor, business partner (telecommunication or otherwise)

So, what is a Business Associate Agreement (BAA)? First, a *business associate* is any individual or entity that performs functions or activities on behalf of a covered entity (*that’s us*) and requires the business associate (*that’s them!*) to use and/or access DMHAS protected health information also known as PHI. Additionally the agreement (BAA) is required by HIPAA and the HITECH Act and is the legal contract that is designed to keep everyone (including vendors and our business partners) accountable for the patient data they access, use, store and in some cases—share.

Why do I need one? Simply put, it’s a requirement. Health and Human Services (HHS) states “The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information 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.”

Here’s a short list* of what else the business associate agreement tells us:

- The business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.
- The Business associate(s) are required to detail how they’ll access, use and disclose the covered entities’ PHI.
- It includes section(s) on how many days a business associate will have to notify the covered entity of a breach.
- The agreement e.g. contact, describes permitted and required uses of the CE’s (covered entity’s) PHI and its use by the business associate.
- States that the business associate “will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law.”

*This list is not meant to be all inclusive and only serves as short reminders.

*With integrity, you have
nothing to fear,
since you have nothing
to hide.
With integrity, you will
do the right thing.....
Zig Ziglar*