Office of Internal Controls, Audit Compliance & Information Security (IAC/S)

PRIVACY MATTERS

A Monthly Newsletter from the MDH Privacy Officer
December 2022

As a HIPAA hybrid entity, MDH conducts business activities that are both covered and non-covered functions. MDH designated payer programs and all Local Health Departments and State hospitals as Covered Components, meaning these programs are required to comply with HIPAA rules.

If your organization is a covered component, an important thing for you to know about is:

Business Associate Agreements

What is a Business Associate Agreement?

A Business Associate Agreement (BAA) is a particular type of contract dictated by HIPAA which outlines the responsibilities of another party you're doing business with when it comes to Protected Health Information (PHI). This HIPAA requirement applies to any third party/vendor (aka Business Associate (BA)) that creates, receives, maintains, or transmits PHI on your organization's behalf. The BAA contract is unique to HIPAA. In it, your BA provides assurances that they will protect the PHI of your patients, and you require your BA to take specific actions and restrict how they may use or disclose PHI.

When is a BAA required?

Only the Covered Components of MDH must have a BAA with each BA; non-covered components are not required to have BAAs. The BAA sets forth the expectations and requirements of both parties – both you and the vendor, and of course, as a contract, it is a legally binding document. As such, a BAA is required any time you are working with a vendor or contractor who will work with PHI on your organization's behalf.

Keep in mind, HIPAA requires you to sign the BAA with your business associate before sharing any PHI with them. This will help you avoid a privacy breach, as well as fines and investigations for failing to have a BAA in place.

Who isn't a Business Associate?

Not all parties who may come into contact with PHI meet the standard BA definition. For example, your workforce (including volunteers, interns, etc.); individuals or companies with very limited and incidental exposure to health

information (such as a telephone company, janitorial service, electrician, etc.); and companies that act as a conduit for PHI (such as the Postal Service, UPS, private couriers, etc.) are not BAs, so a BAA is not required.

Do BAs need BAAs with their subcontractors?

Yes. If a BA uses subcontractors to work with the PHI governed by a BA, the BA needs to have BAAs with each of these subcontractors. The documents would be essentially the same other than defining the relationship. Note: Covered Entities (Covered Components), Business Associates, and subcontractors of the BA can all be held liable for potential HIPAA violations.

What happens if PHI is shared without a BAA in place?

HIPAA compliance is important. If PHI is shared without first establishing a BAA, there can be serious consequences for your organization. The Department for Health and Human Services Office for Civil Rights (HHS/OCR) can impose large fines and enact undesired corrective action plans. Also, if there is an OCR audit, OCR will look at BAAs to determine if due diligence has been conducted with your BAs.

Need help with a BAA? Not sure if a BAA is needed?

Internal Controls, Audit Compliance & Information Security (IAC/S) is available to help!

Privacy Team: mdh.privacyofficer@maryland.gov

Strategic Data Initiative (SDI) Team: mdh.sditeam@maryland.gov

A newly revised Business Associate Agreement is now available! Please contact your program administer or the Privacy Office to obtain a copy.

IAC/S will be providing a Business Associate Training!

Be on the lookout for more information.