HIPAA & Your Group Health Plan

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that was enacted to improve the portability and continuity of health coverage, to combat waste and fraud, and to simplify the administration of health insurance.

There have been several amendments to HIPAA since 1996, including the privacy rule in 2000 which created national regulations for the use and disclosure of protected health information (PHI) in treatment, payment, and operation of health plans, as well as the security rule in 2003, which set standards for protecting the confidentiality and integrity of electronic PHI.

Who is a Covered Entity (CE)?

Health plans (including employer sponsored group health plans), health care clearinghouses, and health care providers

Business Associate (BA):

is a person or entity who creates, receives, maintains or transmits PHI on behalf of a Covered Entity or provides services to a covered entity. A member of the covered entity's workforce is not a business associate. Examples can include organizations providing legal, actuarial, accounting, benefits consulting including insurance brokers, data aggregation & transmission, management services provided by a TPA, administration, accreditation, or financial services.

Protected Health Information (PHI):

Individually identifiable information relating to the health status of an individual, treatment of a health condition, or payment for past, present, or future healthcare services. PHI includes treatment information, medical test results, diagnosis, and prescription information. It does not include information in educational and employment records. e.g. sick leave requests, records needed under FMLA, files for workers' compensation The PHI must be individually identifiable, e.g. name, dates of birth, admission/discharge dates from hospital, account number, email/other addresses, if it is stripped of identifiers, it is not protected.

Examples of PHI: Explanations of benefits, medical provider bills, appeals of denied claims, FSA receipts/requests for reimbursement, HRA receipts/requests for reimbursement, an employee's wellness program testing results, even an employee's appointment reminder with a physician is PHI.

The HIPAA privacy rule only applies to covered entities. These entities often use the services of third parties to help administer and carry out the functions of the plan and the provision of health care. The privacy rule permits covered entities to disclose PHI to these third parties when they are business associates. Business associates are only allowed to the use PHI in limited ways and are required to safeguard the information from misuse.

Under HIPAA, a business associate must have an agreement in place with the covered entity that:

- Describes the permitted and required uses of protected health information by the business associate;
- Provides 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; and
- Requires the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Is an Employer a Covered Entity?

Generally, no, unless the employer is in the health care field. Even though employers as plan sponsors are not covered entities, their employer sponsored group health plan itself is a covered entity, and the employer becomes responsible with the health plan's compliance with HIPAA. In some ways the employer steps into the shoes of the health plan to help the health plan meet its obligations under HIPAA. The employer often ends up handling PHI during the administration of the plan unless it is a fully insured plan in which the employer takes a "hands off" approach.

What is "hands off?" – A fully insured group health plan that provides health benefits through an insurance contract and neither the employer-sponsored plan or the plan sponsor (employer), create, maintain, or receive PHI, the plan is hands off. A plan or plan sponsor that receives more than summary health information for the sole purpose of obtaining premium proposals, or modifying, amending, or terminating the plan, will not be considered hands-off. Very few fully insured employers are truly "hands off." A self-funded health plan cannot be considered hands off.

The use and disclosure rules under HIPAA require that covered entities obtain specific authorizations for most uses of PHI or disclosures of PHI other than those disclosed or used for treatment, payment, and health care operations of the plan

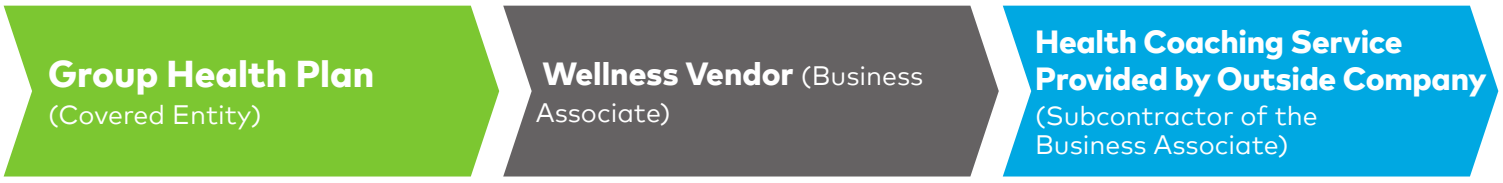
If the health plan utilizes a third party administrator, attorney, accountant, or consultant- including an insurance brokerage- and PHI is used or disclosed, a business associate agreement (BAA) or contract must be entered.

Subcontractors

Covered entities are not the only types of business that delegates functions, activities or services to third parties– sometimes a business associate will rely on a third party as well. For instance, a Third Party Administrator (TPA), who processes claims could utilize a medical review company to ensure services provided under the plan are medically necessary. The review company would be a subcontractor of the business associate. Similarly, a group health plan could hire a wellness vendor to implement a wellness program, and the wellness vendor could then contract with an outside company that provides health coaching services to employees who are not within the target health goals of the wellness program.

Example:

Example:



If the subcontractor is going to access the covered entity's PHI, the business associate must take certain steps to ensure that subcontractors agree to all the same restrictions and conditions that apply to the business associate, as it relates to creating, receiving, maintaining, or transmitting PHI. This requires the business associate to obtain a written agreement from its Subcontractors agreeing to meet all the requirements under HIPAA's privacy and security rule.

There is no limit to the number of subcontractors that this obligation flows down to- if a subcontractor uses another third party who will access the PHI, the rules will continue to apply, all the way to end of the chain.

Business Associate to Business Associate

A group health plan might wish to have two separate business associates share information with each other – the business associate contract should contemplate that and identify the authorized disclosures between the two parties.

Common Scenarios in Which a BAA is Needed:

1. An employer that sponsors a group health plan (covered entity) engages an insurance brokerage to consult with, advise the plan, obtain price quotes, and assist with other matters relating to the plan. The group health plan needs a BAA agreement with the brokerage.

2. A group health plan (covered entity) has a robust wellness plan and utilizes a population health management company to review their wellness data and assist the plan in making design choices to help plan participants stay healthy. The population health management company aggregates data as part of their work product. The group health plan needs a BAA agreement with the population health management company.

3. A group health plan (covered entity) has over 100 participants and has a trust, therefore it is required to conduct an audit of the trust under ERISA. If the accountants have access to health information that is not de-identified, the group health plan will need a BAA agreement with the accountants.

4. An employer sponsored health FSA (covered entity) uses a Third Party Administrator to substantiate, process and reimburse employee's medical expenses. The TPA receives plan enrollment and eligibility data from the employer and provides eligibility reports for the employer to review. The group health plan needs a BAA agreement with the Third Party Administrator.