HIPAA Policies Are Not Optional

You Have Handbook and Policies for Holidays, But No Policy to Protect Your Employee's Health Information? Huh?

All employers who sponsor group health plans, regardless of whether they are self-funded or fully insured, have substantial obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Complying simply isn't optional, and the failure to do so may result in significant exposure and substantial liability.

Most businesses have rules and protections in place in the form of an employee handbook that detail the relationship between the employer and their employees. Why then do so many plan sponsors ignore an essential component of that relationship by failing to provide policies and rules regarding the use and disclosure of protected health information ("PHI") under HIPAA?

Is it because employers and their Human Resource staff do not know that PHI must be protected under your group health Plan? Is it the cost, time and difficulty? All of that can be solved.

This article explains the critical need for a HIPAA policy that works for your group health plan, covered employees and dependents, and underscores the need for group health plan sponsors to have appropriate HIPAA policies and procedures, as well as Business Associate Agreements, in place to comply with the HIPAA requirements and reduce their exposure.

HIPAA Policies

Who needs a HIPAA policy? All group health plans with 50 or more covered persons are considered a "covered entity" under HIPAA, and as such, must have policies and procedures in place to govern the use and disclosure of PHI.

Do employers with under 50 covered persons need a HIPAA policy? Yes! Having fewer than 50 covered persons does not excuse plan sponsors from having to protect health information. These plan sponsors may not be subject to the same level of audit from the U.S. Department Health and Human Services ("HHS"), but they are still subject to claims relating to the amendment of PHI from participants and misuse of PHI from plaintiffs' lawyers.

Why do you need a HIPAA Policy? Simply put, without a HIPAA policy in place, ***the employer and your insurance broker cannot touch PHI.*** Even though group health plans often do not create PHI themselves, they have access to it, and a policy must be in place to ensure its proper use and disclosure. Without a policy that puts appropriate guideposts in place, a group health plan cannot disclose PHI to the plan sponsor (or your broker) or permit a health insurance issuer or HMO to do so.

Thus, covered entities must ensure that there is appropriate protection in place to comply with HIPAA. An effective HIPAA policy accomplishes this by detailing the following:

1. Naming an "authorized person" who may Access, Use, and Disclose PHI to administer the Plan;
2. Explaining the plan sponsor's legal obligations and role under HIPAA;
3. Regulating the flow of PHI by delineating proper uses and disclosures;
4. Addressing the security of PHI in a reasoned and appropriate manner for a group health plan that is not a health care provider;
5. Defining the rights of "covered persons" under HIPAA;
6. Creating appropriate procedures for addressing rights of covered persons and administration of the policy;
7. Providing the appropriate training for those involved; and
8. Assessing how to appropriately handle PHI breaches.

By maintaining and implementing a HIPAA policy, employers can avoid substantial liability – including employment practice and federal HIPAA law liabilities associated with violating these requirements.

Why don't more employers have HIPAA policies in place? Until recently, it has been too cumbersome and costly for group health plan sponsors to put HIPAA policies and procedures in place. That is, at least until EZ ERISA's HIPAA Compliance Module. Specifically designed for group health plans, EZ's HIPAA Compliance Module helps employers put practical guard rails in place to govern the use and disclosure of PHI and comply with these important requirements. It also provides breach assessment and notice preparation services in the event that an employer suspects a breach of PHI.

The government has also been slow to enforce the penalties associated with noncompliance, but that has changed in recent years. HHS reports an ***over 20% increase in penalties collected from 2017 alone, with averages in the millions of dollars.***

While the risk of audit or breaches may have seemed somewhat low, they are increasing, and the pain of having it happen is extremely high. Now is the time for plan sponsors to implement an effective HIPAA policy.

Do not wait for it to be too late to implement an appropriate HIPAA policy and procedures for your group health plan. If you are, someone could lose their job!

Business Associate Agreements

Who is a Business Associate? A Business Associate is any person or entity who performs or assists in the performance of functions or activities related to the Plan that involves the use and disclosure of PHI. Common examples include insurance brokers, claims lawyers, medical billing services, IT service providers and accountants.

What is a Business Associate Agreement? A Business Associate Agreement ("BAA") is a contract that covered entities enter into with Business Associates – any person or organization that is hired to handle, use, distribute, or access PHI – to ensure that they acknowledge they are subject to the HIPAA rules.

BAAs must contain certain elements specified in 45 CFR 164.504(e), such as describing the permitted and required uses of PHI by the business associate; providing that the business associate will not use or further disclose PHI other than as permitted or required by the contract or as required by law; and requiring the business associate use appropriate safeguards to prevent the use or disclosure of PHI outside of the purposes provided for by the contract.

Note, however, that a BAA without an underlying policy to implement the policies and procedures for the group health plan is useless.

Why do I need a BAA? HIPAA mandates that each covered entity obtain satisfactory assurance from business associates to ensure the appropriate safeguard of PHI they receive or create on behalf of the covered entity and consistent with the HIPAA policy in place. This satisfactory assurance is the BAA, and it must be documented in writing to ensure that neither party can disclaim liability by asserting that it is not subject to HIPAA.

When a covered entity becomes aware of a material breach or violation by the business associate of the BAA, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the BAA. If termination of the BAA is not feasible, a covered entity is required to report the problem to HHS. HHS continues to monitor and impose substantial penalties on covered entities who fail to comply with these rules.

Drafting BAA's and understanding when they are required can be a highly technical process, which is why EZ ERISA's HIPAA Compliance Module ensures compliance with the BAA requirements and includes a sample agreement for use, as well as providing custom breach assessment and notice preparation services.

Will a BAA work without a HIPAA policy? No! BAAs have absolutely no meaning without an underlying HIPAA policy. No matter how well-crafted, a BAA undertaken without an underlying HIPAA policy is useless.

Conclusion

Group health plan sponsors with 50 or more covered persons are considered covered entities under HIPAA and must have a HIPAA policy and BAAs in place to regulate the use and disclosure of PHI. PHI cannot flow within an organization or outside it without a compliant HIPAA policy, and BAAs are useless without one. Put plainly, employers that sponsor health benefits must have a HIPAA policy and BAAs in place to comply with the law and reduce their exposure and liability.