

Fully Insured Plans & HIPAA Privacy

There is a lot of confusion about whether or not a fully insured plan has to comply with HIPAA or even what minimum compliance steps a fully insured plan must take. Whether you read the HHS website or read the HIPAA Privacy Regulation, it appears that a fully insured plan has a variety of exceptions. However, first glances can be deceiving. The HHS website responses are accurate to the extent one knows how to read and understand the nuances of their statements in conjunction with the actual Privacy Regulation. In addition, most organizations have not taken the time to read the Privacy Regulation in its entirety to understand the relationships between the various provisions and how it truly relates to an organization's business operations. This article addresses the reasons why a fully insured plan should implement the HIPAA Privacy requirements.

The HIPAA Privacy Exemption

There is only one exemption in the HIPAA Privacy Regulation. The exemption has nothing to do with whether the plan is fully insured or self-funded. In order to be exempt from having to comply with all of the HIPAA Privacy requirements, the health plan must meet the following test.

1. The plan must have less than 50 participants. Participant is a much broader term than the term employee. Participants include all eligible employees and dependents under the plan; and
2. The plan must be entirely administered by the employer. This means the employer cannot have any other third party handling any part of the administering the plan (e.g. using a third party administrator or insurance carrier).

Few plans ever really meet this test since many employers utilize outside vendors to conduct the administration of the plan.

Evaluating Each Health Plan Separately

My organization has a medical plan and dental plan that are fully insured. We also have a flexible spending account. We don't receive any protected health information so we don't have to comply, right? Be very careful when you try and lump all of your plans together to determine your HIPAA compliance. Each plan needs to be evaluated separately. Having a flexible spending account that reimburses for health care costs will require you to complete all of the HIPAA Privacy requirements. Also be wary of the health plans that are being marketed as fully insured plans but have a high deductible that is paid by the employer. These plans are a mixed of fully insured and self-funded. As such, these plans will need to comply with all of the HIPAA Privacy requirements. The organization

needs to not only be careful with the labeling of the plans, but also in analyzing the way the plan is funded and actually operated. If the employer is paying for the deductible, there needs to be some sort of receipt of medical care before the employer can pay. As such either the employer or the employer's vendor acting as a third party administrator will be receiving protected health information. Again at this point, this type of plan would need to comply with all of the Privacy requirements.

The Fully Insured Health Plan Exception

Many fully insured group health plans believe that if they don't receive any protected health information, they will not have to comply with HIPAA. Believing this is really providing the organization with a false sense of security. The Privacy Regulation and HHS has stated clearly, that if the group health plan receives only summary health and enrollment/disenrollment they do not have to comply with **SOME** of the **ADMINISTRATIVE** requirements. It **DOES NOT** say the fully insured plan does not have to comply with the rest of the Privacy Regulation. The administrative requirements the plan may not have to comply with include:

1. Naming a privacy official and a complaint contact person
2. Training workforce
3. Safeguards
4. Complaint process
5. Sanctions
6. Mitigation
7. Documenting policies and procedures

Privacy requirements the plan may need to comply with include: disclosures, plan amendments, business associate contracts, privacy notice, authorizations, access to PHI, accounting of PHI, refraining from intimidating or retaliatory acts and waiver of rights to name just a few. In addition, this "exception" does exist under the Transaction Regulation or Security Regulation. The Transaction requirements include handling electronically enrollment/disenrollment information, claim status inquiries or responses and premium payments. The Security Regulation addresses electronic protected health information. Therefore, the fully insured plan needs to carefully evaluate its situation to determine the whether it still needs to comply with the other HIPAA regulations.

Who is really getting Summary Health Information?

So what is summary health information? Summary health information is basically de-identified health information that cannot be traced back to a specific individual in the plan. Many fully insured group health plans need to be careful in assuming that all they receive is summary health information for a variety of reasons.

First, the plan needs to determine whether or not it is or someone acting on its behalf (e.g. broker or agent) is truly receiving only summary health information. The majority of brokers indicate receiving more than summary health information in order to properly bid out the plan to other carriers or conduct renewals. Once the claims aggregate data includes any identifier such as birth dates, social security numbers, plan member numbers, etc... it no longer meets the summary health information definition. As such, the health plan does not meet the exception, and would then be required to comply with **all** of the HIPAA Privacy requirements. It doesn't matter that the plan never sees the information. The fact a third party acting on the plans' behalf is obtaining the protected health information is enough to require the health plan to comply with all of the HIPAA Privacy requirements. In addition, even if the census information is separate from the claims aggregated data, the fact that the two could be combined may mean it is not summary health information.

Second, the fully insured plan needs to evaluate its size. HHS has indicated if a plan receives summary health information, but yet can determine from a review of the information which individuals in the plan it belongs to, then the information is not considered summary health information. Therefore, plans that are considered small employer plans or organization that utilize a small staff to handle all human resource functions, disability issues and health plan benefits may easily determine individual's claims when looking at a summary health report. In these cases, the exception will not be met. This determination alone will eliminate many plans from this exception.

Third, enrollment forms are not defined under HIPAA. It is reasonable to assume that enrollment forms include name, address and dependent information. However, what about the enrollment forms that contain the medical questions. These questions are often asked for medical underwriting purposes or apply a preexisting limitation under the plan. Because these types of questions contain individually identifiable health information, there is a reasonable argument that the plan would not meet this exception because of receiving protected health information.

Why Comply with HIPAA Privacy

HIPAAAnswers™ often hears from clients, brokers and attorneys that simply eliminating the receipt of protected health information, the fully insured health plan will be protected. In today's society, your organization should really ask if this is really practicable. Just consider the following:

Employees come to the human resources department to get help in payment of their claims, issues with their benefits, COBRA, etc... In all such instances, the organization better understand what the requirements are for a HIPAA compliant authorization if they want to help their employees. In addition, most employers must interact with providers in conducting FMLA, ADA, disability or workers

compensation programs. These providers must follow HIPAA and will require a HIPAA compliant authorization before releasing any protected health information to the employer. In addition, because there is so much focus on an individual's privacy today, the courts will likely hold employers to a standard as set forth in the HIPAA privacy standards when the employer is in dealing with its employees' protected health information.

Finally, even if you believe that the organization may never be subject to the HIPAA penalties, the state laws and common law causes of action still exist. Many states recognize a statutory or common law duty of confidentiality of protected health information. A breach of this duty can lead to significant recovery of monetary damages. Other state law claims include: invasion of privacy, consumer protection laws for "unfair or deceptive practices", torts of fraud, defamation, publication of private facts, placing a person in a false light, misappropriation of a person's name and breach of contracts. Damages under these laws can be substantial. In many states, awards may potentially include treble damages and attorney fees. So is it really worth the effort to try to "avoid" protected health information in conducting your business on a day to day basis? The time to consider this question is not after your organization has been sued.

Conclusion

The amount of work in determining if the fully insured plan is not receiving more than summary health information seems to be more time consuming than if the organization just drafted the privacy policies and procedures. Complying seems to be make good business sense especially since many of the requirements are likely be handled informally already in your organization. Employers are constantly changing plans and options from fully insured to being self-funded. In a matter of a few seconds, the group health plan can be required to comply with the HIPAA requirements, but may never know it. Putting the organization at substantial risk to federal fines and penalties and state law actions, may not be worth it in the long run. While the employer may still be sued in state court, having documented policies and procedures for handling protected health information and workforce training, will greatly reduce or eliminate damages that can be assessed against the organization.

Annette Miller is the Vice-President of Compliance Services/Corporate Counsel for HIPAAAnswers™. She has over 15 years experience in the health insurance industry. Annette graduated from William Mitchell College of Law, cum laude and holds a masters degree in public administration with a minor in health care administration from Drake University. Contact us at sales@HIPAAAnswers.com or call us at **866.326.6785**. Visit our website at www.HIPAAAnswers.com for further information about our products and services.