

HIPAA Compliance for Fully Insured Plans Guide March 2025

While every effort has been taken in compiling this information to ensure that its contents are totally accurate, neither the publisher nor the author can accept liability for any inaccuracies or changed circumstances of any information herein or for the consequences of any reliance placed upon it. This publication is distributed on the understanding that the publisher is not engaged in rendering legal, accounting, or other professional advice or services. Readers should always seek professional advice before entering into any commitments.

Table of Contents

Introduction **3**

Relationship Structure for Fully insured Plans **4**

Entities Involved 4

Relationship Between Entities 4

Consider Access to PHI **4**

Level 1 Approach to PHI 4

Level 2 Approach to PHI 4

Compliance Obligations for Plan Sponsors with a Level 1 Approach to PHI **5**

Consider Group Health Plans **5**

Look at ALL Plans Sponsored 5

When the Only Self-Funded Plan Is a Health FSA (HFSA) 6

Can HRAs Be Treated Like HFSAs? 6

Other Issues for Plan Sponsors Taking a Level 1 Approach **6**

Business Associate Agreements 6

Assisting Employees with Claims Issues 6

Receiving Information for Purposes of Soliciting Bids 7

Employer Reporting 7

Compliance Obligations for Plan Sponsors with a Level 2 Approach to PHI **7**

Summary **7**

Introduction

Employers often wonder what their HIPAA compliance obligations are with respect to their group health plans. The general rule is that all employers that sponsor group health plans must comply with the requirements under the HIPAA Privacy and Security Rules. The only blanket exception is for the uncommon situation in which an employer sponsors a group health plan that has fewer than 50 participants and the employer also self-administers the plan – i.e., does not use a third-party administrator (TPA).

However, there is another exception to the general compliance requirements that applies to certain employers that sponsor a fully insured group health plan.[1] In many cases, employers that sponsor fully insured group health plans have very limited access to the plan's protected health information (PHI). The insurance carrier assumes most of the plan administration responsibilities, and the employer maintains a relatively "hands-off" approach. In this case, an employer's compliance obligations are much more limited.

To help employers better understand this exception, this paper will focus on plan sponsors of *fully insured* group health plans and will outline what their obligations are with respect to those plans.

[1] Plan sponsors of *self-funded* group health plans are subject to all HIPAA's privacy and security requirements, even if virtually all PHI is handled by the plan's TPA and other vendors.

Relationship Structure for Fully Insured Plans

Entities Involved

In the case of a fully insured group health plan, two covered entities are involved:

1. The group health plan itself; and
2. The insurance carrier issuing/administering the plan.

Relationship Between Entities

There is no business associate relationship between the group health plan and the insurance carrier. Instead, each is a covered entity, and each is therefore responsible for complying with HIPAA privacy and security requirements.

(Note: In the case of a self-funded group health plan, there is only one covered entity – the employer-sponsored health plan. Any administrator, TPA, or insurance company administering a self-funded plan would be considered a Business Associate.)

Consider Access to PHI

Level 1 Approach to PHI

Employers who sponsor fully insured plans may choose to take what we call a “Level 1” approach to their plan’s PHI and limit the PHI they receive to just summary health information and/or enrollment information.

- **Summary Health Information**: Information that summarizes claims history, claims expenses, or types of claims experience of the plan, and that is stripped of all individual identifiers other than a five-digit zip code.

- **Enrollment Information**: The definition of "enrollment information" for this purpose is not entirely clear. The regulations refer to "disclosure of whether the individual is participating in the group health plan or is enrolled in or has disenrolled from a health insurance [carrier] offered by the plan." On the other hand, the preamble to the final regulations provides a more expansive definition of enrollment information – but even here, the preamble indicates that enrollment information must not include anything more than what is “situationally required by the standard transaction.” The most cautious strategy for employers relying on the Level 1 approach would be to ensure that enrollment/disenrollment information includes only high-level, nonclinical information (and not, for example, a copy of an ID card or any claims/cost-sharing information).

A plan sponsor should be certain that its access to PHI is limited to summary health/enrollment information prior to adopting a Level 1 approach. (Note that, under ERISA, the plan sponsor has certain fiduciary duties that may make it difficult to avoid having access to more detailed PHI. Therefore, employers that sponsor group health plans should carefully assess their true level of access to PHI to determine whether the Level 1 approach is appropriate.)

Level 2 Approach to PHI

Employers who sponsor fully insured plans may instead choose to take what is called a “Level 2” approach to their plan’s PHI and access more detailed types of PHI (e.g., claims data or other individually identifiable health information) in preparation for carrying out plan administrative functions. In this capacity, the plan sponsor functions similarly to a plan sponsor of a self-funded plan – i.e., is more actively involved in plan administration and regularly accesses PHI as part of this function.

Compliance Obligations for Plan Sponsors with a Level 1 Approach

When a plan sponsor takes a Level 1 approach to its fully insured plans, then its compliance obligations with respect to such plans are limited. Specifically, its privacy obligations are limited to:

1. A prohibition on retaliation; and
2. A prohibition on requiring participants to waive their rights as a condition of enrollment.

When the plan sponsor receives enrollment/disenrollment information from the carrier, the plan sponsor does not need to treat such information as PHI and may disclose this information to a third party (such as a broker) without invoking the need for a business associate agreement. This is the case because the plan sponsor isn't a covered entity, and it hasn't assumed a covered entity's compliance obligations under HIPAA (as the plan sponsor of a self-funded plan does), since it's receiving only very limited PHI from its health plan.[2]

There is no similar broad-based exemption for Level 1 plan sponsors under the security rule; therefore, the exact nature of a plan sponsor's security requirement is less clear. However, from a practical standpoint, plan sponsors should take at least the four steps outlined below to demonstrate due diligence regarding its health plan's obligations under the security rule. HIPAA security rules require that an employer, as plan sponsor:

1. Conduct a "risk assessment" to determine the type of steps that need to be taken to protect electronic PHI (ePHI). A plan sponsor with no access to ePHI should at least conduct an analysis to verify and document that the plan sponsor truly doesn't have access to ePHI (beyond summary health or enrollment/disenrollment information);
2. Designate a Security Official to act as a point of contact for any questions or issues that may arise with respect to the group health plan's ePHI (even if there is no access to it, questions may still arise, and at least some level of coordination with the carrier will be needed);
3. Document the extent to which the plan sponsor is relying on the carrier's policies and procedures to ensure compliance with the security rule; and
4. Ensure that there are processes in place to respond to and provide notification of any breaches of unsecured ePHI – in particular, any of which the plan sponsor may become aware.

Consider Group Health Plans

Look at ALL Plans Sponsored

HIPAA applies to more than just the employer's medical plan. Dental, vision, prescription, and other plans providing health-related coverage are also subject to HIPAA. An employer may sponsor a variety of different plans, some of which might be fully insured and some of which might be self-funded. In general, if an employer sponsors any self-funded plan, the employer needs to comply with all the HIPAA Privacy and Security Requirements. This is true even if other plans are fully insured and the employer, as plan sponsor, is taking a Level 1 approach to those fully insured plans. For this reason, it's important to look at each group health plan to determine what the plan sponsor's compliance obligations are.

---

[2] Although a Business Associate Agreement with a broker or other third party is not required, see the discussion below outlining a more conservative approach to Business Associate Agreements for plan sponsors taking a "Level 1" approach.

When the Only Self-Funded Plan Is a Health FSA (HFSA)

A health FSA (HFSA) is a self-funded plan and therefore is subject to all HIPAA's Privacy and Security Requirements. However, plan sponsors typically take a hands-off approach to HFSA plan administration, relying predominantly on the HFSA administrator to process claims and appeals. Therefore, if a plan sponsor's only self-funded plan is an HFSA, and if the employer, as plan sponsor, structures the HFSA in such a way that it doesn't receive any PHI from the HFSA administrator beyond summary health/enrollment information, it seems reasonable to take a simplified approach to compliance. Such an approach would be similar to that outlined above for plan sponsors taking a Level 1 approach to their fully insured plans, with some additional obligations to account for the existence of a self-funded group health plan.

Can HRAs Be Treated Like HFSAs?

Employers who sponsor a health reimbursement arrangement (HRA) have additional compliance obligations beyond those that apply to a health FSA. Because of an employer's fiduciary obligations under ERISA, it is more difficult for an employer to avoid accessing PHI from its HRA; therefore, the simplified compliance approach referenced above for plan sponsors of fully insured group health plans plus an HFSA is not suitable for sponsors of HRAs.

Other Issues for Plan Sponsors Taking a Level 1 Approach

Business Associate Agreements

Technically, plan sponsors taking a Level 1 approach to PHI are not required to enter into Business Associate relationships with any third-party entity with whom they may share summary health/enrollment information. This is the case because plan sponsors are not themselves covered entities (their plans are the covered entities), and the plan sponsor has only summary health/enrollment information, which the plan sponsor does not have to treat as PHI under the Level 1 approach. Therefore, the plan sponsor may share this information with a third party, such as a broker, without first entering into a Business Associate relationship.

Note that the above describes a specific situation in which access to PHI is fairly limited. If access is actually broader, then a business associate agreement (BAA) will probably be necessary. Because interactions can often be much more complex, the safest approach is generally to have a BAA in place. Our general recommendation is that it is usually safest for brokers to put a compliant BAA in place with their employer clients. Doing so will protect the employer, as plan sponsor, if the employer were to inadvertently share information with its broker that goes beyond the allowable summary health/enrollment information. (But keep in mind that if employers do have more extensive PHI, they will also need to consider additional compliance obligations under HIPAA.)

Assisting Employees with Claims Issues

A plan sponsor taking a Level 1 approach has limited itself to receiving only summary health/enrollment information and agreement information from its plan. Therefore, it is naturally limited in what information it can obtain for purposes of assisting employees with claims issues. In this situation, if an employee brings a particular issue to the plan sponsor to gain assistance, the plan sponsor can use the information that the employee voluntarily discloses; however, if any additional plan information is required, it will be necessary to obtain written authorization from the employee before obtaining the information from the plan. Accessing more detailed PHI in the absence of written authorization will jeopardize the plan sponsor's Level 1 status.

Receiving Information for Purposes of Soliciting Bids

For a Level 1 plan sponsor, receiving summary health/enrollment information for purposes of "modifying, amending, or terminating the group health plan" (so-called "settlor functions" under ERISA) is permitted. But what if more detailed information is required? According to the preamble to the final Privacy Regulations, the regulators seem to have taken the position that summary health/enrollment information should be sufficient for this purpose. Receipt of more detailed information, such as individual participant high claims data, could interfere with the plan sponsor's Level 1 status.[3]

Employer Reporting

Much of the information needed to complete Forms 1094-C and 1095-C should be available from an employer's employment records (and therefore not subject to HIPAA). Even information about whether an employee enrolled in a particular plan would not be considered PHI if it was gathered by the employer in facilitating the enrollment process. To the extent that such information is not considered PHI, the employer may use it for reporting purposes without implicating HIPAA.

Compliance Obligations for Plan Sponsors with a Level 2 Approach

When employers, as plan sponsors, take this more involved approach, the exemption that exists for plan sponsors taking a Level 1 approach does not apply, and the plan sponsor must comply with all the requirements under the HIPAA Privacy and Security Rules. In other words, it must implement policies and procedures; put a plan amendment in place to permit the disclosure of PHI by the plan to the plan sponsor; conduct training for workforce members who have access to PHI; and have processes in place to respond to individuals' requests concerning their PHI. However, while the plan sponsor is responsible for maintaining a copy of the Notice of Privacy Practices (NPP) and for issuing it upon receiving a request from an individual, the carrier still maintains the primary responsibility for distribution of the NPP.

Summary

Every plan sponsor of a group health plan needs to pay attention to HIPAA compliance requirements. Although sponsors of fully insured group health plans may have fewer obligations under HIPAA if they limit the type of PHI they have access to, this does not mean that they are completely off the hook. And access should be reviewed carefully among ALL group health plans sponsored. Certain ERISA fiduciary responsibilities may make it difficult, on a practical level, to maintain limited access; and even if a plan sponsor takes a Level 1 approach to one of its fully insured plans, it may be taking a Level 2 approach to other plans or have other self-funded plans that require more extensive compliance.

---

[3] Even for Level 2 plan sponsors, the ability to receive more detailed information for purposes of soliciting bids isn't clear, since "soliciting bids" is not considered a plan administrative function. Therefore, regardless of a plan sponsor's approach to PHI, it is not evident that receiving more detailed information for purposes of soliciting bids would be permitted under any circumstance. One option for Level 2 plan sponsors may be to have the insurer share more detailed information with a Business Associate of the plan (i.e., a broker). But the broker would need to limit the information it then shared with the employer. This would not be an option for a Level 1 plan sponsor.