Are TPA-Administered Health FSAs Subject to the HIPAA Privacy and Security Rules?

EBIA Weekly (May 22, 2025)

QUESTION: Our company plans to offer a health FSA next year. We will use a third-party administrator (TPA) to administer health FSA claims. We know that our company's fully insured major medical plan is subject to the HIPAA privacy and security rules, but we've taken a hands-off approach for protected health information (PHI) (receiving only summary health information and enrollment information from the insurer) to limit our privacy and security obligations. Can we take the same approach with the health FSA?

ANSWER: Not quite. The definition of a health plan under the HIPAA privacy and security rules is broad enough to include health FSAs, with only one very limited exception. If a health FSA has fewer than 50 participants and is administered by the employer, it is not subject to HIPAA 's privacy or security rules. Because a TPA will administer claims under your company's health FSA, this exception is not available to you.

Note also that the HIPAA privacy and security rules use a broader definition of the term "health plan" than the HIPAA portability provisions use. As a result, even though health FSAs generally are excepted benefits and therefore are not subject to HIPAA's portability provisions, the privacy and security rules typically still apply to them.

Under the privacy rules, if the sponsor of a fully insured plan takes the hands-off approach for PHI, most of HIPAA 's privacy requirements apply to the insurer but not to the health plan or the plan sponsor. Specifically, the plan and plan sponsor are subject only to the privacy prohibitions on retaliation and waiver. Because most health FSAs are not fully insured, this exception to the privacy rules does not apply to them. Therefore, the privacy rules will apply to your health FSA, and your company will be responsible for compliance.

The security rules do not draw a distinction between fully insured and self-insured plans, so all sponsors of group health plans must consider whether they have access to any electronic PHI and apply the HIPAA security rules accordingly. While it is common for sponsors of fully insured plans to have less PHI (because the insurer assumes greater responsibility for administering the plan), a hands-off exception is not available under the security rules.

Under both the privacy and security rules, you can ease your compliance burden by delegating many plan administrative functions to the TPA to minimize the amount of PHI used by or disclosed to your company. Because the TPA will be considered a HIPAA business associate of your health FSA, a business associate contract between the health FSA and the TPA must set forth the TPA's HIPAA compliance obligations before the TPA can use or disclose PHI.

For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections VI ("What Plans are Subject to HIPAA's Portability Requirements"), XXII ("Privacy, Security, and EDI: What Information Is Protected and Which Entities Must Comply?"), XXIII ("How the Privacy and Security Rules Affect Group Health Plans and Plan Sponsors"), and XXIX ("Security Requirements: General Concepts"). See also EBIA's Cafeteria Plans manual at Section XXII.I ("When Do HIPAA's Requirements Apply to Health FSAs?").

Contributing Editors: EBIA Staff.