Protecting Health Plan Information Is More Important Than Ever

Insights
6.02.16

It's common for employers outside the healthcare industry to believe they can avoid issues brought about by the Health Insurance Portability and Accountability Act (HIPAA) and other health plan data laws. After all, most employers with fully insured plans never see individually-identifiable health information, and HIPAA is a law for hospitals and doctors, right?

Not exactly. There are a few reasons all employers need to stop and think about the safety of your health plan data. A data breach could be costly and embarrassing, and could erode employee trust. Health plan data is being increasingly targeted by criminals. Even if you don't store or see data from your health plan, you have a fiduciary duty to ensure it is safe in the hands of your vendors. Accordingly, data protection procedures should become a regular part of your fiduciary due diligence.

In addition, while most employers outside the healthcare industry assume they have no HIPAA obligations, they actually may have them based on their roles as health plan sponsors. These obligations are more pressing than ever. The Department of Health and Human Services (HHS) - the agency responsible for HIPAA enforcement - has just announced phase two of its audit program. Employers, particularly those who sponsor self-insured plans, could face costly penalties if they are audited and their compliance efforts fall short.

The Danger Of Data Breaches
Large-scale data breaches of insurance carriers illustrate the growing risk to healthcare data. Such data often includes names, birth dates, social security numbers, and credit card accounts. Unlike stolen credit card information, however, it is harder to detect a breach of plan data because it may be months before identity theft or credit card fraud can be traced to a data breach.

Because medical files have more information and a longer shelf-life, they are also more valuable in underground markets such as the dark web. The FBI estimates that such data is worth 10 to 20 times more than stolen credit card information. Due to this heightened risk, plan sponsors need to consider who is maintaining their data and how it is being protected.

Data Protection Is Part Of Fiduciary Duty
Under ERISA, plan fiduciaries have a duty to act prudently. Increasingly, employers have come to understand that protecting health plan information is part of this duty. To ensure you have met your

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

understand that protecting health plan information is part of this duty. To ensure you have met your fiduciary obligations, you should work with your benefits committee to create a plan for protecting information that is stored both onsite and with third-party vendors, and also record your protection plan.

You can also involve your IT department to secure information they store. For vendors, you should consider safety measures such as contractual provisions, audit procedures, privacy and security reports, and privacy and security questionnaires.

HHS Initiates Phase Two Audits

Another reason to focus on health plan data is that a new round of HIPAA audits is on the way. The HITECH Act, enacted in 2009 to help stimulate the use of electronic health records, required HHS to begin performing compliance audits. From 2011 to 2012, the department implemented a pilot audit program to assess the compliance efforts of 115 covered entities.

Earlier this year, HHS announced phase two of its audit program. Over the next year or two, the department plans to conduct over 200 desk and onsite audits. The first round of desk audits will focus on covered entities, while the second will focus on business associates. Auditors will pay particular attention to risk analyses and risk management, Notices of Privacy Practices, access and response to requests for access, and content timeliness of notifications. As expected, onsite audits will have a broader scope than desk audits.

To prepare, employers who sponsor health plans should review their obligations with counsel. Employers with self-insured plans in particular should confirm they have met the full range of HIPAA compliance obligations, including maintaining written privacy and security policies, appointing privacy and security officials, amending plan documents, conducting an annual IT risk assessment, maintaining a Notice of Privacy Practices, and executing updated Business Associate Agreements with plan vendors.

Fisher Phillips offers a HIPAA compliance kit for a flat-rate fee. For more information, or if you would like assistance preparing notices that reflect your internal policies and procedures, please contact your Fisher Phillips attorney or any member of our Employee Benefits Practice Group.

For more information, contact the author at TGeorge@fisherphillips.com or 504.529.3845.

Service Focus

Privacy and Cyber

Employee Benefits and Tax

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.