Is Your Health Plan HIPAA Compliant?

Insights
8.03.15

Data breaches with respect to medical information are on the rise, given that such information is generally more valuable on the black market than stolen credit card data. The 2015 breach of healthcare company Anthem, Inc., which saw over 37.5 million records exposed, affected one in four Americans. In addition to the growing threat of data theft, plan sponsors are at a heightened risk of being subject to a HIPAA audit.

While many sponsors were historically lax about HIPAA compliance, times are quickly changing. Here's what you need to know about your HIPAA obligations and where your plan might be falling short.

HIPAA Compliance Obligations
HIPAA creates privacy and security obligations for certain organizations categorized as "Covered Entities." Covered Entities include healthcare providers, healthcare clearinghouses, and health plans. As explained below, some health plans have reduced compliance requirements. However, many others have full-blown compliance obligations, which include:

- maintaining HIPAA privacy and security policies;
- distributing a Notice of Privacy Practices;
- honoring individual rights created by HIPAA;
- contracting with third-party vendors to protect health information;
- amending the plan to allow it to share information with the plan sponsor;
- certifying that the plan sponsor will protect such information;
- training personnel;
- securing IT systems; and
- conducting annual risk assessments.

The Value Of A "Hands-Off" Approach
Compliance obligations may vary, depending on whether the health plan is fully-insured or self-insured. Fully-insured plans can maintain a "hands-off" approach to personally identifiable medical information (known as "Protected Health Information," or PHI) by ensuring the plan sponsor never sees PHI. In such a case, the law allows the plan to comply with HIPAA by simply using the

sees PHI. In such a case, the law allows the plan to comply with HIPAA by simply using the insurance carrier's HIPAA policies and procedures, and there is no need to maintain separate HIPAA policies.

But the sponsor must be vigilant to avoid receiving individually identifiable information, including information produced by claims assistance. This type of service for employees can interfere with a plan's "hands-off" approach. In addition, sponsoring a flexible spending account may also negate the "hands-off" exception for plan sponsors.

Self-Insured Plans Must Implement Full-Blown Compliance

While fully-insured plans may be able to avoid full-blown HIPAA compliance by following a "hands-off" approach to PHI, this is not the case for self-insured plans. The law assumes that plan sponsors of self-insured plans will see PHI, and for this reason, self-insured plans must maintain their own compliance programs, separate and apart from any third-party administrator or stop-loss carrier.

HIPAA Compliance Is More Important Than Ever

Final regulations under the Health Information Technology for Economic and Clinical Health Act (HITECH Act) became effective in 2013. The Act created new HIPAA obligations for both Covered Entities and Business Associates. Notably, the HITECH Act also requires the U.S. Department of Health and Human Services, the entity responsible for HIPAA enforcement, to complete a defined number of HIPAA audits per year. Penalties for HIPAA noncompliance are steep; several prominent cases saw fines in excess of $1 million. HIPAA also imposes criminal penalties for some willful acts of non-compliance.

Fisher Phillips offers a flat-fee HIPAA Privacy and Security compliance program designed to meet all of a health plan's HIPAA compliance needs. For more information, please contact a member of the Fisher Phillips Benefits Practice Group.

For more information, contact the author at TGeorge@fisherphillips.com or 504.522.3303.

Service Focus

Employee Benefits and Tax

Counseling and Advice