Basics of the HIPAA Privacy Rule for Employers

Labor & Employment Law Update

on July 30, 2018

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses, among other things, the use and disclosure of individually identifiable health information, referred to as "protected health information" or PHI. Many employers are confused as to how the HIPAA Privacy Rules apply to them. With requests for FMLA and accommodations for disabilities, employers are handling very sensitive and private information about their employees on a daily basis. While it is impossible to thoroughly address the multitude of issues within the HIPAA privacy rules in a short article, following are some basic points that should help most employers in navigating compliance with HIPAA privacy rules.

HIPAA privacy rules generally do not directly affect employers unless they are a "covered entity" as defined under HIPAA. Covered entities typically include health plans, health care clearinghouses, and most health care providers. Even a health care provider may not be directly subject to HIPAA Privacy Rules in their role as an employer. HIPAA regulations provide an example involving a health care employee: When a clinic employee visits a doctor for treatment, her medical file is PHI. However, when that employee takes the doctor's note she received during her visit and turns it in to HR for attendance purposes, the document is now part of her employment file and is no longer PHI in that setting.

Avoid receiving PHI from your group health plan. If you do not maintain a self-insured health plan you can minimize the need to comply with HIPAA privacy rule requirements simply by restricting your insurer from sharing the information. Generally an insurer should not be sending PHI to the employer unless the plan document specifically states which employees may receive PHI and for what purposes. Your plan document should not unnecessarily designate employees to receive PHI. It is a good idea to review insurance contracts and plan documents and make sure they limit the role the employer plays in administering the group health plan.

Outsource Administration of group health plans, including flex spending accounts. If you have a self-insured health plan and/or a flex spending plan, you need to make sure those plans are administered in compliance with HIPAA privacy rules. However, if you hire a third party administrator, you can and should shift the flow of the PHI to the third party administrator who will be handling the claims. This step greatly simplifies what an employer has to do to be in compliance with HIPAA as it greatly limits the amount of PHI the employer

receives. Instead, you can focus on making sure you have a Business Associate Agreement in place with the third party administrator.

As with everything, there are exceptions to these basic points. For example, the privacy rules contain special provisions relating to workers' compensation laws allowing for an employer to obtain PHI directly from a health care provider when "necessary" to comply with workers' compensation laws. Another exception exists in the privacy rules excluding self-administered plans with fewer than fifty (50) participants from being subject to HIPAA privacy regulations. It is always best for an employer to consult with counsel on any of these issues.