HIPAA's Privacy Requirements: Not Just for Doctors

Insights
11.04.03

If you have seen a doctor in the past few months, you probably noticed that some of the pre-appointment paperwork you filled out referred to the new health information privacy requirements under HIPAA (the Health Insurance Portability and Accountability Act of 1996). While most people are familiar with the effect of these requirements on the medical profession, many people are unaware that the requirements also affect employers who are *not* part of the medical profession.

The HIPAA privacy requirements, which are set forth in regulations established by the U.S. Department of Health and Human Services (HHS), do *not* apply *directly* to employers. This is because there is some question regarding the authority of HHS to regulate employers for HIPAA privacy purposes. However, because HHS does have the authority to regulate healthcare plans, the privacy requirements do apply *indirectly* to employers if they sponsor certain group healthcare plans for their employees (e.g., medical plans, dental plans, healthcare flexible spending account plans, etc.). It is important to keep this distinction in mind, because the HIPAA privacy requirements assume a (largely fictional) separation between group healthcare plans and their sponsoring employers.

The degree to which the HIPAA privacy requirements affect an employer depends upon whether an employer-sponsored healthcare plan is fully-insured or self-funded, and whether the employer has access to protected health information (PHI), which generally includes any individually identifiable information used or maintained by the plan. For example, if an employer sponsors a fully-insured group healthcare plan and does *not* have access to PHI, then the HIPAA privacy requirements impose no significant compliance burdens on the employer. Most of the burdens of compliance with respect to the plan, which include the distribution of a notice of privacy practices to all plan participants, would fall on the plan insurer.

However, if an employer sponsors a self-funded group healthcare plan (other than a self-administered plan with less than 50 participants, which is exempt from the HIPAA privacy requirements), then the HIPAA privacy requirements impose several compliance burdens on the employer, even if the plan is administered by a third party administrator (TPA). These include (i) preparing and distributing a notice of privacy practices to all plan participants, (ii) providing plan participants with the right to review, amend and receive an accounting of their PHI, (iii) instituting administrative safeguards for the protection of PHI, which generally requires an amendment to the plan, a certification from the employer to the plan (keep in mind the fictional separation described above) regarding the appropriate use of PHI and the establishment of employer policies and

above) regarding the appropriate use of PHI and the establishment of employer policies and procedures for the safeguarding of PHI, and (iv) contracting with (or amending existing contracts with) business associates who may have access to PHI (e.g., TPAs, consultants, accountants, etc.) regarding the appropriate use of PHI.

The HIPAA privacy requirements became effective for most group healthcare plans on April 14 of this year. However, "small" group healthcare plans, which include those plans with less than $5 million in annual premiums (if fully-insured) or claims (if self-funded), have an additional year (until April 14, 2004) to comply with the requirements. Failure to comply could subject an employer to civil and even criminal penalties, in addition to lawsuits brought by employees and other plan participants.

Related People

Sheldon J. Blumling
Partner
949.798.2127
Email