HIPAA Privacy Rule Deadline Looms

2004-02-17

Small health plans will be required to comply with new federal health data privacy regulations by April 14, 2004. Federal law gave small health plans (those with $5 million or less in annual receipts) a year longer than most covered entities to meet privacy requirements under the Health and Insurance Portability and Accountability Act of 1996 (HIPAA). On April 14, 2004, those small health plans will be required to be in full compliance with the privacy rules, joining the healthcare providers, healthcare clearinghouses and large health plans that were subject to an April 2003 compliance deadline. In addition, April 14 is the deadline for entities covered by HIPAA to add required privacy assurances to their agreements with third-party "business associates" that receive access to individually identifiable protected health information (PHI).

HIPAA requirements and compliance deadlines are discussed in several Hale and Dorr Internet Alerts.

HIPAA Compliance Burdens Are Minimal for Certain Plans

Despite the April 14, 2004 deadline, certain plans will be exempt from either all or most of HIPAA's privacy requirements. Self-funded, self-administered plans with fewer than 50 participants are exempt from the HIPAA privacy rules. In addition, employers that sponsor fully insured health plans have, in most cases, minimal compliance obligations with respect to those plans.

Caution--Health FSAs Will Be Subject to HIPAA

Many employers may be surprised to learn that their health flexible spending accounts (health FSAs) will likely be required to fully comply with the HIPAA privacy rules. Health FSAs are considered health plans under HIPAA. Because health FSAs are self-funded, if the employer has 50 or more participants with health FSAs, or hires a third-party administrator to run the health FSA, the plan will be fully subject to the HIPAA privacy rules. As such, employers should ensure that their health FSAs are HIPAA compliant.

All entities covered by HIPAA--including large and small health plans--are already subject to HIPAA standards for code sets and data formats used in electronic health transactions. These rules became mandatory on October 16, 2003. New health data security standards will become mandatory on April 20, 2005 for all covered entities except small health plans, which will have a

compliance date of April 20, 2006.

Compliance with the HIPAA Privacy Rule

The HIPAA privacy rule requires health plans to take steps to protect the privacy of PHI that the plans either maintain or transmit. Those self-insured plans, including health FSAs, that have not already complied with the privacy rules will be required by April 14, 2004 to:

- Give notice to individuals as to how PHI about them is used and disclosed
- Limit the use and disclosure of PHI
- Implement internal privacy policies and procedures
- Ensure individuals' rights to access and amend their PHI
- Amend plan documents to reflect HIPAA privacy measures
- Obtain written authorizations for a wide range of uses and disclosures of PHI
- Obtain written privacy assurances from third-party "business associates" that receive PHI, such as third-party administrators

Bringing Your Plans into Compliance

With two months remaining until the April 14, 2004 deadline, there is still plenty of time for small health plans to comply with HIPAA. For more information on HIPAA privacy rule compliance for employee health plans, please contact a member of Hale and Dorr's Employee Benefits Group.

Amy A. Null
amy.null@haledorr.com

William H. Schmidt
william.schmidt@haledorr.com

Linda K. Sherman
linda.sherman@haledorr.com

Authors

Amy A. Null

PARTNER

amy.null@wilmerhale.com

+1 617 526 6541

Linda K. Sherman

RETIRED PARTNER

+1 617 526 6000