HIPAA of a Job: 7 Compliance Steps for Your 'Small Plan'

HIPAA of a Job: 7 Compliance Steps for Your "Small Plan"

Insight — 5/19/2004 12:00:00 AM

Regulations that are already effective require many employers with more than 50 employees to take special actions to limit disclosure of employee health-related information, particularly to prevent it from being used to discriminate against employees. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department of Labor and the Department of Health and Human Services have issued series of regulations and amendments to protect the privacy of medical records ("Privacy Rule"). The Privacy Rule was effective April 14, 2003 for all covered entities other than small health plans. Small health plans are insured plans with total annual premiums of less than $5 million, or self-insured plans with total annual claims of less than $5 million; these plans have an extended effective date of April 14, 2004.

To comply with the Privacy Rule, small health plans should now take the following steps as soon as possible:

1. Identify sources and uses of Protected Health Information.

"Protected Health Information" ("PHI") is any information, in any media, that is created or received by a "Covered Entity" (health care providers, health care clearinghouses and health plans) or an employer and relates to the past, present or future physical or mental health of an individual, if the information is created or received by a Covered Entity or an employer and can be used to identify the individual (by name, address or social security number, etc.).

The Privacy Rule provides that a Covered Entity may not use or disclose PHI, except (i) for treatment, payment and plan operations, (ii) with the authorization of the individual who is the subject of PHI, or (iii) as permitted or required by the Privacy Rule. When using or disclosing PHI or when requesting PHI from another Covered Entity, a Covered Entity must take reasonable steps to limit PHI to information that is the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Employers, as sponsors and administrators of group health plans (particularly self-insured group health plans), may have access to and process PHI, and therefore, may be responsible for some compliance steps. Note that medical information needed for an employer to carry out its obligations under the FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave, drug screening, workplace medical surveillance, and fitness-for-duty tests of employees may be part of the employment records maintained by

an employer and are not PHI.

2. Appoint a privacy officer.

While the Privacy Rule requires the appointment of a privacy officer, a more comprehensive approach is to appoint a HIPAA privacy team. A privacy team should include members from each department that may assist in the regulation and protection of PHI (e.g., HR, benefits, accounting, information systems, legal). The team should be headed by the appointed privacy officer and establish an internal timeline and meeting schedule to implement the steps for compliance with the Privacy Rule.

3. Amend ERISA plans.

Employers must amend health plan documents in order to receive PHI from the health plan. The amendments must describe how the employer will use PHI; identify employees who will have access to PHI and under what circumstances; establish a method for resolving any issues of non-compliance; and provide that the health plan will disclose PHI to the employer only if the employer provides a certification of its agreement to certain conditions designed to safeguard PHI.

Next, the employer must certify to the health plan its commitment to safeguard PHI, agreeing not to use or disclose PHI other than as permitted or required by the health plan or by law; to ensure that its agents similarly will safeguard PHI; not to use or disclose PHI for employment-related actions; to report to the health plan any impermissible use or disclosure; to provide plan participants with the ability to review their PHI and to amend or correct their PHI; to maintain records sufficient to provide plan participants with an accounting of the uses and disclosures of their PHI; to make its policies and procedures, books and records relating to the use and disclosure of PHI available to HHS for audit purposes; if feasible, to return or destroy all PHI received from the health plan once such PHI is no longer needed; and to ensure that adequate separation exists between the health plan and the employer to protect the confidentiality of PHI.

To back up its certification, an employer should create a "firewall" between the group health plan and the human resources department and ensure that PHI is not used or disclosed for employment purposes or for the purposes of a benefit plan other than the health plan.

4. Develop a "Privacy Policy" and procedures to govern the use and disclosure of PHI, both within and outside of the organization.

A Privacy Policy is required to address the routine use and disclosure of PHI, minimum necessary requirements, individual authorization, de-identification of PHI, employee training and sanctions, record retention and security. The Privacy Policy should also address employees' rights to gain access to their PHI and receive an accounting of its use and disclosure and implement procedures to obtain authorizations, enforce individual rights, handle complaints, provide a mechanism for resolving non-compliance with the Privacy Rule and for developing, maintaining and

distributing the Notice of Privacy Practices, described below.

5. Prepare employee communications and authorizations, including a "Notice of Privacy Practices."

A Notice of Privacy Practices must be prepared and distributed by employers sponsoring self-insured plans (including flexible benefit plans and employee assistance plans). Electronic distribution of this notice is permitted. Employers sponsoring insured group health plans may rely on the insurance company or third-party administrator to distribute the Notice of Privacy Practices for the health plan, but the employer should be prepared to answer employee questions regarding it, and if applicable, include provision of the Notice of Privacy Practices as the administrator's duty under the Business Associate contract.

6. Identify business partners that receive PHI from the employer or create PHI on behalf of the employer ("Business Associates") and establish an agreement that meets HIPAA requirements.

Sponsors of group health plans should identify the Business Associates that provide services to their group health plans, including any flexible benefit plan, employee assistance plan, and wellness benefit program. Health plans should enter into a Business Associate contract with each of its Business Associates. Business associate contracts must describe the permitted and required uses of PHI by the Business Associate; provide that the Business Associate will not use or further disclose PHI other than as permitted or required by the contract or as required by law; and require the Business Associate to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the contract. Business associate contracts should be executed by April 14, 2004.

7. Develop and hold training programs for applicable employees.

Employees who will potentially deal with PHI should be trained in the permitted uses and disclosures of PHI under the Privacy Rule. Any training should cover the following groups: benefits staff will need training on the implementation and maintenance of firewalls to protect PHI; HR staff will need training on the prohibition against improper use of PHI; managers and supervisors will need training regarding the impact of the Privacy Rule on the use and disclosure of PHI for purposes other than treatment, payment and plan operations. Track and document all training.

All employees will require some level of training, as the Privacy Rule will affect employees' relationships with benefits and HR personnel. Employees may be required to contact only designated persons with regard to their issues and concerns related to health plans. Employers will have to communicate these changes to their employees and should be prepared to respond to grievances with the new systems should complications arise.

Enforcement and Penalties

Employers should begin taking steps to implement the requirements under

the Privacy Rule as soon as possible or be subject to substantial penalties. Generally, penalties will be based on the harm to the individual for noncompliance, as well as the willingness of the group health plan to become compliant. The civil penalty for noncompliance is up to $100 per person per violation, with a maximum of $25,000 per person for the violation of a single rule in a calendar year. Criminal penalties may also be imposed for the knowing misuse of PHI, and additional penalties may apply for the sale of PHI or the use of PHI under false pretenses. The HHS has publicly announced that it will respond to complaints of violations of the Privacy Rule by working with the Covered Entity that is the subject of the complaint to bring that entity into compliance.
