HIPAA Privacy Requirements Take Effect

April 14, 2003 is the date that many organizations must begin complying with the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations (April 14, 2004 for smaller health plans with less than $5 million in annual receipts.). These regulations were issued last fall and are intended to protect consumer health information. They require "covered entities" to ensure that "protected health information" is not misused or improperly disclosed. In addition, covered entities must establish clear procedures to protect patient privacy.

The bulk of the privacy rule's requirements apply to health care insurers and providers, such as doctors and hospitals. What is less clear is how employers that are not insurers or providers are covered. The Department of Health and Human Services (HHS), the agency responsible for issuing the regulations, does not have direct authority to regulate organizations in their role as employers. However, it does regulate the group health plans sponsored by employers.

So, if your organization provides group health care benefits to employees, you will have some compliance obligations, particularly if you provide a self-insured health plan. Find out below how your organization is covered and what steps you should take to comply.

* Important Definitions *

"Covered entities" are defined as health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically (such as electronic billing and funds transfer). (See 45 C.F.R. §160.103.)

Editor's Note regarding citations used in this article:

References to "C.F.R." refer to the Code of Federal Regulations, the official government publication for federal regulations.

A health plan is further defined to include a group plan that provides, or pays the cost of, medical care, as well as insurers and HMOs. (See 45 C.F.R. §160.103.) The rule, however, specifically excludes plans that have less than 50 participants and are self-administered. (See 45 C.F.R. §160.103.) Most employers that offer welfare benefits to employees under the Employee Retirement Income Security Act (ERISA), whether insured or self-insured, will effectively be covered by the regulation in their role as plan sponsor. (See 45 C.F.R. §164.501.)

"Protected health information" (PHI) includes all medical records and other individually identifiable health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally. (See 45 C.F.R. §164.501.) For example, information relating to a previous health condition, illness, propensity for a disease, and health care treatment is considered PHI, as is information relating to the payment for health care services received.

A point worth noting is that "employment records" held by an entity in its role as employer are not covered. (See 45 C.F.R. §164.501.)
does not specifically explain what employment records are exempted. However, according to the comments issued with the final rule, these records include any medical information needed by an employer to carry out its obligations under the Family and Medical Leave Act (FMLA), the Americans with Disabilities Act (ADA), and similar laws. In addition, the exemption includes files and records related to occupational injury, disability insurance eligibility, sick leave requests, drug screening results, and fitness-for-duty certifications. (Of course, you still must comply with the FMLA and ADA provisions that require keeping medical records confidential.)

* Basic Administrative Obligations for Covered Entities *

As a general rule, covered entities (insurers, providers, clearinghouses, and health plans) cannot use or disclose PHI without the consent or authorization of the person the information pertains to, except as permitted or required by law. (See 45 C.F.R. §164.502(a).)

To meet this obligation, covered entities must comply with a number of administrative requirements. For example, they must provide privacy notices to affected individuals, designate a privacy official for the organization, and establish privacy policies and procedures concerning protected health information. In addition, they must establish appropriate administrative, technical, and physical safeguards to prevent improper disclosure of health information. (For a detailed description of the administrative requirements, see 45 C.F.R. §§164.508, 164.520, and 164.530.)

Most group health plans also must amend their plan documents to restrict uses and disclosures of PHI by plan sponsors. (See 45 C.F.R. §164.504(f)(2).) The rule also imposes additional specific obligations on health care providers, health plan clearinghouses, and group plan providers regarding when and how they can use PHI.

* Employer Obligations if Not a Covered Entity *

As mentioned above, if your organization is not specifically a covered entity, it may still need to comply with the HIPAA privacy rule regarding the flow and use of protected health information, as a result of its role as a health plan sponsor. The extent of your obligations depends on the functions you perform on behalf of the health plan.

Employers that receive protected information as a plan administrator for "plan administration functions" have greater compliance obligations than employers that simply engage in "plan sponsor functions." "Plan administration functions" include claims procedures and benefit determinations, whereas "plan sponsor functions" are more limited and include enrollment and disenrollment activities. (See 45 C.F.R. §164.504(d).) Described below are the different levels of obligation employers have depending on the type of plan offered, beginning with the least amount of compliance required.

1. Fully insured plans that receive only summary health information and do not perform plan administration functions.

A group health plan has limited obligations under the privacy rule, if it: (1) provides benefits "solely" through an insurance contract with an
insurer or HMO; and (2) does not create or receive PHI, except for "summary health information" or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from an insurer or HMO. (See 45 C.F.R. §164.530(k).)

"Summary health information" consists of claims history, expenses, or types of claims stripped of certain personal identifiers. (See 45 C.F.R. §164.504(a).) Under this definition, an employer may receive summary health information if it agrees to limit its use of the information to obtaining bids for providing health insurance coverage to group health plans or to modifying, amending, or terminating the group health plan. (See 45 C.F.R. §164.504(a).) If the summary identifies participant information, the plan must inform individuals of the disclosure.

If your plan meets the above criteria, you only have to comply with two administrative requirements: (1) adopt an antiretaliation policy stating that you will not retaliate against any individuals who exercise their rights under the privacy rule; and (2) adopt a policy stating you will not require individuals to waive their rights under the rule. (See 45 C.F.R. §164.530(g) and (h).) You do not have to amend your plan documents or provide a privacy notice.

2. Self-insured group health plans that receive only summary health information and that do not perform plan administrative functions.

A self-insured plan creates more obligations for employers, even if you receive only summary health information. In this case, you still must comply with all of the administrative requirements of covered entities (described above). The privacy notice for larger employers should be distributed to all employees enrolled in the health plan on or before April 14, 2003, and, for smaller health plans, on or before April 14, 2004. Any employees who enroll after these dates should receive the notice upon enrollment. (See 45 C.F.R. §164.520(c)(2).)

3. Self-insured group health plans that perform plan administration functions.

Employers that provide these plans must comply with the same obligations as self-insured plans that receive only summary health information. In addition, you must amend the health plan documents to permit the disclosure of PHI from the plan to the employer for plan administration purposes. Further, you must certify to the plan that the PHI will be used only as permitted by the privacy rule. Duties under the certificate include preventing the unauthorized use or disclosure of PHI and providing "firewalls" to limit access to PHI except by specifically identified employees. (For a detailed explanation of the certification requirements, see 45 C.F.R. §164.504.)

4. Fully insured plans that perform plan administration functions.

Employers with these plans must amend the plan documents, implement the administrative requirements, and provide the above certification to the insurer or HMO since PHI will be received. Regarding the notice requirements, these plans only have to provide the privacy notice to a plan participant upon request. The insurer or HMO is responsible for providing a separate privacy notice to participants. (See 45 C.F.R. §164.520(a)(2).)
* Advice for Small Plans: Wait and See *

There is no way around it - the HIPPA privacy rule is complicated. Even though it is relatively short in length (about 40 pages of regulatory verbiage compared to nearly a hundred pages for the FMLA) it is not user-friendly and does not directly discuss what employers must do. It refers to "covered entities" and "group health plans," but does not give any easy guidelines for employers.

So, a good starting point is to identify whether you must comply as a covered entity or as a health plan administrator or sponsor. If your obligations result from your health plan, then take a look at the four categories described above to determine which steps you should take to implement the privacy rule.

Remember, too, if you are a small employer, your health plan may not have to begin complying until next year. Health plans with less than $5 million in receipts do not have to implement the privacy protections until April 14, 2004. As a practical matter, many HIPAA experts are advising smaller plans to take a "wait and see" attitude. Some speculate that the rule may be further revised based on the experience gained as larger organizations begin complying.

Even if you don't think you have to comply until next year, make sure you review your status with legal counsel before beginning your preparations. You still will need to understand how you are covered and what changes are necessary.