Employers Beware: The Deadline to Comply with HIPAA’s Complex Privacy Regulations is Fast Approaching
December 31, 2002

On August 14, 2002, the United States Department of Health and Human Services ("HHS") published the final modifications to its "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Rule") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA" or the "Act"). These regulations were drafted to give individuals more control over their medical information by requiring health care providers to establish safeguards to protect the privacy of such information.

Along with the benefits that the Privacy Rule confers on the public at large come new and often burdensome responsibilities for employers. It is imperative for employers to be aware of these new responsibilities and to implement a strategy for complying with these new requirements. The fast-approaching compliance deadline for almost all "covered entities" under the Privacy Rule is April 14, 2003, so now is the time to plan both a short- and long-term strategy. This article will serve as a road map for human resource professionals, benefits personnel and in-house attorneys in need of a primer on the requirements of the Privacy Rule.

What Exactly Is The HIPAA "Privacy Rule"?

As a general matter, HIPAA's Privacy Rule restricts how "covered entities" may disclose and use "protected health information" ("PHI"). PHI is defined for purposes of HIPAA as any information, whether in oral, paper or electronic form, that:

- relates to any health condition of an individual, or any health treatment, or payments for health treatments, and
- identifies the individual or could reasonably be used to identify the individual.

HIPAA defines "covered entities" as:

- health plans (defined as any individual or group plans that provide, or pay the cost of, medical care, including "group health plans" of private and public employers);
- health care clearinghouses; and
- health care providers who transmit certain health information in electronic form.
Employers Beware: The Deadline to Comply with HIPAA'S Complex Privacy Regulations is Fast Approaching (continued)

Though employers are not specifically defined as "covered entities," there is no doubting the Privacy Rule's impact on employers that offer health benefits to their employees. Why? Because the Privacy Rule's coverage of "group health plans" effectively results in extending HIPAA coverage to employers that either play an active role in the management of a group health plan or provide self-insured group health plans. Furthermore, where a group health plan makes PHI available to an employer acting as the plan sponsor, the employer is obligated to comply with certain additional requirements to avoid potential sanctions under the Privacy Rule.

Is Your Company A "Plan Sponsor"?

One of HHS's objectives in formulating the Privacy Rule was to ensure that PHI does not play a role in any employment decisions. The Privacy Rule therefore places new restrictions on almost all employers that sponsor group health plans in connection with the way such employers use and disclose PHI of employee participants in the plan.

Under the Privacy Rule, plan sponsors who receive PHI (either from the group health plan or from a third party involved in the administration of health benefits) are required to amend the group health plan documents to identify which of the employer's employees, or class of employees, will be allowed access to PHI in the administration of the plan. This class of employees would typically include, for example, benefits and human resources personnel. The plan documents must also be amended to restrict the use of PHI to those tasks necessary for the administration of the benefit plan. Similarly, employers that are also plan sponsors must establish "firewalls" between those employees who have access to PHI and those who do not. Additionally, the plan documents must include an effective mechanism for resolving issues of improper access to, or use of, PHI.

Employers that fit within the Privacy Rule's definition of "plan sponsor" must then "certify" to the group health plan that the plan complies with the regulations. Specifically, each such employer must certify in writing that it will:

- use and disclose PHI only as permitted by the plan or as required by law;
- not use PHI in connection with employment decisions, or in relation to employee benefits other than those offered under the group health plan;
- provide for "adequate separation" between the plan and the employer to prevent disclosure of PHI to the plan sponsor's employees not designated to receive such information;
Employers Beware: The Deadline to Comply with HIPAA'S Complex Privacy Regulations is Fast Approaching (continued)

- ensure that its agents and subcontractors agree to respect the same restrictions with respect to the use of PHI;
- report to the group health plan any Privacy Rule violation in connection with the disclosure of PHI;
- allow plan participants to review, acquire and amend their PHI, subject to the procedures outlined in Privacy Rule;
- upon request by a plan participant, provide a summary of PHI disclosures made regarding that plan participant in the preceding six years, subject to the procedures outlined in the Privacy Rule; and
- make its internal records relating to the disclosure and use of PHI available to HHS for auditing to check for compliance with the Privacy Rule. Such audits may be initiated by the HHS, or by a third-party complaint, and are governed by procedures set forth in the Privacy Rule.

Employers that are plan sponsors should determine, based on the implications of complying with the Privacy Rule, whether they wish to continue to receive PHI from their group health plans (since it is the employer’s receipt of such information that triggers the Privacy Rule requirements) and, if so, what procedures they will implement to comply with the Privacy Rule.

Employers That Provide Self-Insured Group Health Plans May Be Hit The Hardest

In addition to the Privacy Rule obligations applicable to employers that are plan sponsors, employers that administer a group health plan must also comply with the requirements that HIPAA places on health insurers and health providers. Specifically, such employers must:

- designate a privacy official responsible for the development of policies and procedures;
- designate a contact person responsible for receiving complaints and establishing a process for individuals to complain about the group health plan's compliance with its policies and procedures under the Privacy Rule;
- establish policies, procedures and training concerning the use and disclosure of PHI that comply with the Privacy Rule;
- formulate appropriate safeguards to protect PHI from intentional or unintentional use or disclosure in violation of the Privacy Rule;
- establish appropriate sanctions against employees who violate the covered entity's Privacy Rule policies; and
Employers Beware: The Deadline to Comply with HIPAA’S Complex Privacy Regulations is Fast Approaching (continued)

- mitigate any harmful effect resulting from a known use or disclosure of PHI in violation of the Privacy Rule.

"Business Associates" Under The Privacy Rule - The HIPAA Catch-All

HIPAA does not apply solely to employers that are directly involved in health care or the administration of group health plans. Under the "Business Associate" provision of the Privacy Rule, any individual or company that engages in business with a covered entity that results in the disclosure of PHI is required to enter into certain mandated agreements with the covered entity. For example, Business Associates include entities that perform the following functions for a covered entity involving the use or disclosure of PHI: claims processing, quality assurance, billing, and legal and actuarial work. Under the Privacy Rule, Business Associate contracts must:

- outline the allowable uses and disclosure of PHI;
- require the business associate to use appropriate safeguards to prevent the unauthorized use or disclosure of PHI and to report any known unauthorized use or disclosure to the covered entity;
- require the business associate to give individuals access to their own PHI, permit individuals to request amendments to their PHI, and provide written accountings of disclosures of PHI to those individuals who request it, in accordance with requirements of the Privacy Rule;
- ensure that contractual restrictions regarding the disclosure of PHI apply to the agents and subcontractors of the business associate; and
- allow the covered entity to terminate the contract if the business associate has violated a substantive term of the contract.

Thus, any organization doing business with covered entities that requires the use or disclosure of PHI should be prepared to execute written agreements containing provisions similar to those outlined above. The HHS website includes sample contract provisions in order to assist companies in meeting the Business Associate agreement requirements. The HHS website link containing the sample contract provision can be found at www.hhs.gov/ocr/hipaa/contractprov.html.

The Intersection Of HIPAA And Other Employee Protections
Employers Beware: The Deadline to Comply with HIPAA'S Complex Privacy Regulations is Fast Approaching (continued)

When drafting the Privacy Rule, HHS recognized that covered entities must also comply with other laws that implicate the use and disclosure of PHI, including the Americans with Disabilities Act (the "ADA") and the Family and Medical Leave Act (the "FMLA"). As a general matter, employers subject to HIPAA and other federal privacy regulations should obtain written authorization before disclosing an employee's PHI. In this regard, employers should note the following:

- Under HIPAA's Privacy Rule, employers must obtain written authorization before obtaining PHI from a health care provider for FMLA or ADA purposes;
- Like the Privacy Rule, the ADA requires that only the "minimum necessary" information may be disclosed or used by a covered entity, even where there is written authorization from the employee;
- Even where a use or disclosure is permitted by the ADA or FMLA, employers may not disclose PHI without written authorization; and
- HIPAA's "firewall" requirement, discussed above, is similar to employer obligations under the ADA, which requires that an employee's medical information be kept separate from his or her personnel file.

It is also worth noting that the Privacy Rule specifically excludes workers' compensation and disability insurance from the definition of "health plan." This exclusion was included in the final modification of the Privacy Rule in order to avoid a disruption of these existing systems.

The Consequences Of Non-Compliance With The Privacy Rule

HIPAA provides for substantial civil and criminal penalties for non-compliance. Penalties for violation of patient confidentiality standards include monetary fines and, in some cases, imprisonment. For example, the fine for violating certain HIPAA privacy standards can be as much as $100 per person per violation, and up to $25,000 per person for consistent violation of a single standard for a calendar year.

The good news is that the HHS Secretary may reduce the amount of a fine or waive it entirely if the violation was not due to willful neglect of the requirements and if the entity in violation corrects the violation within 30 days of becoming aware of it.
Federal criminal penalties may also be imposed on covered entities that knowingly and improperly disclose information or obtain information under false pretenses. Penalties would be higher for actions designed to generate monetary gain. For example, HIPAA provides for criminal penalties of up to a $100,000 fine and up to five years' imprisonment for obtaining protected health information under "false pretenses," and up to a $250,000 fine and up to ten years' imprisonment for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Conclusion

Virtually all employers and health plans must be in compliance with the Privacy Rule by April 14, 2003. (Small health plans with annual receipts of $5 million or less have until April 14, 2004 to comply.) As this deadline draws near, employers should become familiar with their obligations under the Privacy Rule, and should implement any necessary changes in plan documents and human resource policies and procedures in order to comply with what experts agree is a complex and burdensome new set of employer obligations.