New HIPAA Requirements — Impact on Employers and Health Plans

By Jennifer Willcox

New technology has transformed the way society manages information, but has also raised significant privacy concerns, particularly when it relates to confidential personal matters such as health information. You undoubtedly have heard about the new HIPAA privacy requirements, but you should be aware of the impact of HIPAA on employers, which may affect their employment policies and practices and the administration of their health plans.

Federal privacy regulations issued in 2000 pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require sweeping changes in the way the health care system manages health information. Health care providers, health care clearinghouses and health plans (known as “covered entities”) are directly governed by these requirements, and the government regulators who wrote the HIPAA rules emphasize that they do not have statutory authority to regulate employers. However, depending on the structure of your health plan and your employment-related needs for health information, the regulations can significantly affect your operations. Understanding who is covered by the HIPAA regulations and what information is included in their reach can help you sort through the HIPAA morass.

THE HIPAA PRIVACY RULE AND EMPLOYER-SPONSORED HEALTH PLANS

The so-called “Administrative Simplification” requirements of HIPAA primarily address three separate components: 1) electronic transactions and code sets; 2) privacy; and 3) security. The electronic transactions and code sets requirements establish standard data content, codes and formats for submitting electronic claims and other administrative health care transactions. The standards are intended to promote the use of electronic transactions and provide some level of uniformity within the health care system. Compliance was required by October 16, 2002, but Congress gave a one-year extension to those entities that filed a “compliance plan.” The HIPAA Security Rule (compliance with which is required by April 21, 2005) applies only to electronic health information. This article primarily addresses the Privacy Rule, but note that the Security Rule requires many of the same administrative steps (business associate agreements, plan document amendments, appointment of an individual to lead the compliance effort, and policies and procedures), as well as a risk analysis and appropriate security measures to address your information systems. For the actual regulation text for all of these requirements and other helpful guidance from the government, see the U.S. Department of Health and Human Service's Web site at http://aspe.hhs.gov/admsimp/. The privacy component has received the most attention recently, since compliance was required by April 14, 2003. (“Small health plans,” defined as those with receipts of $5 million or less, have until April 14, 2004 to comply. For guidance on how to calculate “receipts” for determining your eligibility for this extended deadline, see http://cms.hhs.gov/hipaa/hipaa2/default.asp.) These detailed regulations, known as the “Privacy Rule,” generally regulate how covered entities use and disclose “protected health information” (PHI). PHI is any individually identifiable health information that is transmitted or maintained in any form. (The HIPAA Security Rule, in contrast (compliance with which is required by April 21, 2005) applies only to electronic health information. This article primarily addresses the Privacy Rule, but note that the Security Rule requires many of the same administrative steps (business associate agreements, plan document amendments, appointment of an individual to lead the compliance effort, and policies and procedures), as well as a risk analysis and appropriate security measures to address your information systems. Part 2 of this article will address further the HIPAA Security requirements.) As noted above, employers are not covered entities, but the broad definition of “health plan” means that the Privacy Rule will apply to a broad spectrum of employer-sponsored benefit programs, including:

- Medical benefit plans (insured or self-insured) that have 50 or more participants or plans of any size that are administered by an entity other than the plan sponsor;
- Long term care coverage;
- Dental plans;
- Vision plans;
- Prescription drug plans;

continued on page 2
Jennifer Willcox is an attorney in the Health Care and Employee Benefits departments at Wiggin & Dana, a New Haven, Connecticut-based law firm with offices also in Hartford and Stamford, CT as well as Pennsylvania and New Jersey. Ms. Willcox is part of the firm’s nationally-known HIPAA practice group, which assists clients ranging from Fortune 50 companies to small non-profit agencies in structuring and implementing their HIPAA compliance program. She may be reached at jwillcox@wiggin.com.

**HIPAA**

continued from page 1

- Some employee assistance plans or other mental health programs;
- Medicare Supplement plans;
- Flexible Spending Accounts/Personal Health Accounts; and
- Some executive physical programs.

**HIPAA AND SELF-INSURED PLANS**

If your organization offers any of the benefit programs listed above on a partially or fully self-insured basis (meaning some or all benefits are paid out of company assets, rather than by an insurance company), you may need to take the following steps to ensure that these benefit programs are in compliance:

- Developing and executing agreements with the plan’s “business associates” to ensure that they will comply with HIPAA’s privacy requirements;
- amending the documents that establish the plan to describe the ways in which information is used; implementing policies to safeguard the information you receive;
- appointing a Privacy Officer to oversee the compliance effort;
- distributing a Notice of Privacy Practices to all plan participants that describes how the plan uses and discloses health information;
- implementing policies to safeguard the information you receive; and
- training all personnel who have access to the information (such as employees in the Human Resources/benefits department, as well as financial or auditing staff);
- and developing ways to allow participants in these plans to exercise their HIPAA-guaranteed individual rights – the right to access and inspect records, the right to request amendment to information, the right to request certain restrictions on how information is used and disclosed, and the right to an “accounting,” or listing, of certain disclosures.

Although many third party administrators and other health plan vendors have become very familiar with the Privacy Rule’s requirements, in most cases they are not covered entities in their own right. This means that the compliance obligation (and associated penalties for noncompliance) ultimately fall to the health plan sponsor. If you have not yet already executed agreements containing the HIPAA-required contractual provisions (known as “business associate agreements”) with these vendors, look to see whether they can take on some of the HIPAA responsibilities on your behalf, such as facilitating the “individual rights” requirements. (“Business Associate” is the HIPAA term for a vendor that performs a function or provides a service to the health plan of another covered entity involving the use or disclosure of health information. Under HIPAA, such vendors must be bound by special contracts (known as “business associate agreements”) that obligate them to safeguard PHI.)

You may also want to consider adding indemnification language to the “standard” business associate contract provisions in the event they fail to properly safeguard the information or implement appropriate policies.

Finally, you must erect a “firewall” to ensure that PHI is not used for employment-related decisions (such as promotion or termination) and is not used by other benefit plans (such as utilizing information from the group health plan to determine a workers’ compensation claim). Since the Americans with Disabilities Act (ADA) arguably prohibits these actions as well, fine-tuning your policies to ensure that health information is only used for permissible purposes is important. Note further that HIPAA’s requirements are “scaleable” (meaning the reasonableness of a compliance effort will be judged in part by the resources available), and so these “firewalls” can be a simple matter of training and policy statements, or as complex as imposing layered access controls for digital or electronic information.

**HIPAA AND FULLY-INSURED HEALTH PLANS**

If all the benefits your company provides to its employees are fully insured, and if no identifiable health information is provided to your organization by the insurer or HMO, your health plan HIPAA compliance obligations will be minimal. You must refrain from retaliating against an individual for exercising his or her privacy rights (for instance, if an employee complains to the HIPAA regulators about the HMO’s use of her information), and may not require employees to waive their rights to file complaints as a condition of participating in the health plans.

continued on page 3
HIPAA

continued from page 2

plan. To document your compliance efforts with these provisions, review all enrollment materials to ensure they do not contain hidden waiver provisions, and adopt policies to implement the non-retaliation and non-waiver requirements.

WHAT’S OUTSIDE THE “HIPAA Box”? Some forms of insurance and other benefits are excepted from the HIPAA privacy requirements: life insurance, long- and short-term disability coverage, workers’ compensation programs, accidental death and dismemberment (AD&D), auto insurance, and reinsurance/stop loss coverage are not directly covered by the Privacy Rule (although they may be impacted, as discussed below). A health plan that is a covered entity, however, may not disclose PHI for use by these programs without an individual authorization. For instance, information from the health plan cannot be used to determine a workers’ compensation claim, although the information may flow in the opposite direction.

The Privacy Rule also contains an important exclusion for “employment records,” such as health information received in connection with sick leave requests, fitness-for-duty examinations, FMLA certifications, disability applications, requests for ADA accommodations, and other information that your company receives in its capacity as an employer. While this information generally is not subject to HIPAA, you should be aware that other state and federal confidentiality provisions may apply. For instance, the ADA’s confidentiality requirement applies even to information conveyed verbally, and many states have laws regarding the confidentiality of personnel and medical files.

OTHER HIPAA CONSIDERATIONS

If a company needs health information regarding its employees for reasons not related to the health plan, the HIPAA Privacy Rule will also impact how this information is collected. If a health care provider treating an employee is covered by the HIPAA Privacy Rule, he or she will not be able to release any information to the employer without a HIPAA-compliant authorization form. If your policies require that health information be sent directly to the employer (such as drug test results or FMLA forms), you will need to revise any internal release forms to meet the HIPAA requirements for a valid authorization. Note that there are some exceptions. Legally required disclosures such as the drug and alcohol tests for certain commercial drivers mandated by the Department of Transportation (DOT) will not require employee authorization, and disclosures to the employer that are necessary to comply with workers’ compensation laws are also permitted. The DOT recently issued guidance on this subject in the form of a question-and-answer, that can be accessed at www.dot.gov/ost/dapc/main/QandA_HIPAA05031.htm.

Special rules apply to in-house health care providers such as on-site clinics or occupational health nurses. Generally, if these providers engage in standard electronic transactions (claims for payment, first reports of injury, etc.) they will be covered by the Privacy Rule, which means they must have their own set of policies and procedures, a privacy officer, a Notice of Privacy Practices, and are subject to the whole panoply of HIPAA requirements. Such providers can disclose information relating to work-related illnesses or injuries to the employer, if the information is necessary for the employer to comply with its obligations under OSHA or similar laws, and if a notice to that effect is given to employees or posted at the clinic. If your organization contracts with outside medical providers covered by the HIPAA Privacy Rule to provide needed medical information (such as fitness-for-duty examinations), these providers can generally require that the employee sign an authorization form as a condition of providing the care. If any in-house or contracted medical providers are covered by the HIPAA Privacy Rule in their own right, you should ensure that they are aware of the HIPAA requirements and have implemented a compliance plan.

CONCLUSION

The HIPAA privacy regulations are lengthy and complex, and many employers are understandably confused about their effect and reach. Although the Privacy Rule does not directly regulate employers, self-insured health plans and other non-insured employer plans providing medical (especially flexible spending plans) have significant compliance obligations. As a practical matter the privacy requirements will require some changes in your employment policies and administrative practices. Assess the health information that you receive, revise your existing policies and forms if necessary, and contact legal counsel or expert HIPAA consultants for complicated compliance questions.

The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.