How HIPAA Regulations Will Affect Group Health Plan Sponsors and Service Providers

By FRED SINGERMAN and KATHY SCHWAPPACH

The HIPAA regulations to protect the privacy of health information and to establish standards for its electronic transmission will place significant burdens on group health plans and service providers. This article explains those regulations and suggests what steps to take to ensure compliance.

Fred Singerman and **Kathy Schwappach** are partners in the Employee Benefits Practice Group of Seyfarth Shaw. They have a combined 33 years of legal experience in the employee benefits arena. They may be contacted through the firm's Web site at www.seyfarth.com.

The reforms made by Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have been called the most sweeping since Medicare. HIPAA will completely change the way group health plans handle health care information.

The Department of Health and Human Services (HHS) has issued a small phone book of regulations designed to protect the privacy of health information and to establish standards for its electronic transmission. Under the HIPAA regulations, health plans, health care clearinghouses, and most health care providers that maintain or transmit protected health information (together referred to as covered entities) must implement extensive safeguards to ensure the information's integrity and confidentiality, and to protect against unauthorized use or disclosure of the information. In addition to covered entities, the regulations apply to anyone who handles protected health information on behalf of, or provides services to, a covered entity. These so-called business associates include third-party administrators, counsel, accountants, consultants, and other providers of services to health plans.

This article focuses primarily on health plans as covered entities, including self-funded and insured group health plans of private and government employers. Almost all employers will have significant obligations under the regulations as group health plan sponsors.

COMPLIANCE DATES AND PENALTIES

Health plans must comply with the electronic transaction regulations no later than October 16, 2002, and with the privacy regulations no later than April 14, 2003. The effective date for each requirement for small plans with annual receipts of $5 million or less is one year later. In practice, however, because the regulations will affect plan disclosures, policies, and service agreements that most employers will need to have in place for open enrollment, most employers will want to substantially comply well before the deadlines.

Failing to comply with the HIPAA regulations can result in civil penalties of up to $100 per person per violation, with a cap of $25,000 per calendar year. Criminal penalties for certain privacy violations include up to $250,000 in fines and possible imprisonment for up to 10 years. Although neither the statute nor the regulations create a private right of action to sue for violations of the federal privacy standards, litigation under other legal theories, such as breach of fiduciary duty under the Employee Retire-

ment Income Security Act of 1974 (ERISA), remains a risk.

IMPACT OF THE PRIVACY REGULATIONS

The basic thrust of the privacy regulations is to govern how health care providers, group health plans, and their business associates use and share protected health information. Protected health information is broadly defined to include almost any health information that could identify an individual. This includes information in electronic, paper, or oral format that is created or received by a health care provider, health plan, employer, or life insurer and relates to "the past, present, or future physical or mental health or condition of an individual … or the past, present, or future payment for the provision of health care." [45 C.F.R. § 164.500]

How onerous compliance with the regulations will be for a particular group health plan sponsor will depend largely on whether the health plan is fully insured—either through traditional indemnity insurance, health maintenance organizations (HMOs), or both—or is self-insured to any extent. Under the HIPAA regulations, a health insurer or HMO is a covered entity separately responsible for its own use and disclosure of protected health information. When the plan sponsor of a fully insured plan does not create, maintain, or receive protected health information, an exception to most of the administrative and notice requirements discussed below will apply to the plan (as opposed to the insurer). A fully insured plan would not fall within the exception, however, if the plan receives protected health information from either the insurer or the participant. This would occur, for example, if the employer retained input into final claims denials to manage potential litigation risks or if it intervened to assist a participant in getting a claim processed. This is not particularly unusual, and it may not be feasible for sponsors of larger insured health plans to eschew involvement in the claims process entirely.

Although fully insured plans that do not create, maintain, or receive protected health information will not have to comply with most of the administrative requirements described below, they will need to implement policies against intimidating or retaliatory acts against individuals exercising their privacy rights and may not condition treatment, payment, or enrollment in a health plan on a waiver of privacy rights. These policies must be appropriately documented. [45 C.F.R. § 160.530(k)]

This relatively basic conclusion—that fully insured plans are generally not subject to most of the HIPAA privacy requirements—is not particularly self-evident from even a careful reading of the regulations. The specific exemption provided by the regulations for insured health plans applies only if the plan does not actually receive protected health information (other than summary health information and information about enrollment or disenrollment). [45 C.F.R. § 160.530(k)(1)(ii)] Because the regulations broadly define protected health information to include any information that "relates to the … past, present, or future payment for the provision of health care," it is difficult to divine from the regulations how any employer performing even minimal health insurance enrollment functions could avoid having some protected health information. After all, the whole point of enrollment is to pay for the provision of health care.

The answer lies in the preamble to the regulations, which creates a very significant exception to the definition of protected health information for enrollment functions. In explaining why plan sponsors are not subject to the electronic transmission standards (discussed below) when performing enrollment functions, the preamble states:

> Plan sponsors that perform enrollment functions are doing so on behalf of the participants and beneficiaries of the group health plan and not on behalf of the group health plan. For purposes of this rule, plan sponsors are not subject to the requirements of § 164.504 [limitations on the use and disclosure of protected health information] regarding group health plans when conducting enrollment activities.

[65 Fed. Reg. 82496] This position is expedient, since if plan enrollment were itself protected health information, all employers would be required to revamp their payroll practices and train their payroll personnel. It is nonetheless surprising to those who treat enrollment forms and procedures as plan administration functions and is somewhat inconsistent with a subsequent statement in the preamble referencing "eligibility and enrollment functions" as plan administration functions. [65 Fed. Reg. 82647]

The preamble also acknowledges that fully insured group health plans that do not receive or generate protected health information are exempt from a number of specific regulatory requirements; however, no specific exemption is provided in the regulations themselves. These requirements include

maintaining procedures to (1) provide access to protected health information to the individual to whom it relates, (2) amend protected health information, and (3) account for disclosures of the protected health information. [65 Fed. Reg. 82645] Although we are normally loath to rely on a preamble in the face of an inconsistent regulation, there is at least some comfort in the fact that HHS, the entity that wrote both the preamble and the regulations, is also the main cop on the beat. It is important to remember that ERISA will provide a cause of action for breach of any privacy provisions in the plan document.

Despite the general limits on the flow of health information between health insurers (including HMOs) and plan sponsors, the HIPAA regulations recognize that plan sponsors may require health information for purposes of modifying, amending, or terminating the plan, or soliciting bids from prospective health insurers. Additionally, a prospective health insurer may need claims information from a plan sponsor to provide rating information. The regulations permit a group health insurer to provide "summary" health information (from which individual identifying information has been deleted) to the plan sponsor to carry out these functions, provided that the plan document is amended accordingly and an appropriate privacy notice is provided to participants. [45 C.F.R. § 160.504(f)]

The regulatory burden will be far greater for sponsors of self-insured group health plans. Under a typical self-insured plan, the plan sponsor bears the ultimate financial responsibility for health care claims. The sponsor will therefore require access to protected health information (either directly or through a third-party administrator business associate) in order to review and pay claims, perform quality assessment, perform precertification functions, monitor funding requirements, and so forth. These plan sponsors will incur very significant administrative burdens in complying with the HIPAA privacy regulations, which will require

- Amendments to plan documents;
- Very significant revision to administrative services contracts;
- Adoption of extensive, written administrative procedures governing the plan's privacy practices, including training of employees who may handle protected health information; and
- Preparation and distribution of notices to participants regarding the plan's privacy practices.

These requirements are further discussed below.

Limits on the Use of Protected Health Information

Generally, a health care provider must obtain a patient's written consent prior to using or disclosing protected health information. In contrast, a group health plan generally does not need a participant's consent to use or disclose protected health information for purposes of treatment, payment, or health care operations. These terms have very specific definitions under the regulations:

- *Treatment* includes the provision, coordination, or management of health care and related services by health care providers, including the coordination or management of health care, consultation between health care providers, or the referral for health care.
- *Health care operations* include a covered entity's activities related to
  - —Conducting quality assessment and improvement;
  - —Reviewing the competence or qualifications of health care professionals, and health plan performance;
  - —Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and placing a contract for stop-loss insurance; or
  - —Conducting or arranging for medical review, legal services, and auditing functions.
- *Payment* includes the activities of a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and benefits, or the activities of a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Thus, group health plans can disclose protected health information to plan sponsors who conduct payment and health care operations activities on behalf of the plan if the additional requirements described below are met. For almost all other uses or disclosures of protected health information, however, a group health plan must obtain a participant's authorization, for which the regulations specify stringent content standards, or a specific public policy exception (e.g., law enforcement) must apply.

Although the privacy regulations permit the use or disclosure of, or request for, protected health information in connection with health care operations

and payment, the regulations impose the fundamental limitation that any such use or disclosure be limited, to the extent reasonable, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Many activities included in the definitions of the terms *health care operations* and *payment* are commonly referred to as plan administration functions. Plan administration functions do not include modifying, amending, or terminating the plan, or any employment-related functions or functions relating to any other benefits or benefit plans of the employer. Thus, a plan sponsor may not use protected health information in connection with determining or auditing claims under the sponsor's disability plan, absent an authorization from the participant. The regulations are inconsistent in their treatment of using health information for underwriting purposes or to solicit bids from prospective insurers. Although underwriting and soliciting bids are included as part of the definition of health care operations, the regulations nonetheless carve out a specific requirement that for these purposes, protected health information may be provided to a plan sponsor only in summary form.

Health Plan Documents

To permit the disclosure of protected health information to the plan sponsor, even for the permitted purposes described above, the plan sponsor must amend the group health plan document to:

- Establish the permitted and required uses of protected health information by, and disclosures of such information to, the plan sponsor;
- Provide that the group health plan will disclose protected health information to the plan sponsor only on receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate specified provisions, and that the plan sponsor agrees to abide by those provisions; and
- Provide for adequate separation between the group health plan and the plan sponsor, by describing which employees will have access to protected health information, restricting this access to plan administration functions, and providing a way to resolve privacy violations by these employees.

The regulations take a double approach to disclosures to the plan sponsor. Not only is the health information protected by HHS under the regulations themselves, but a contractual protection that is presumably enforceable by plan participants and the Department of Labor is added to the plan document. Additional protection is then required in the form of the employer's certification and written implementation of the administrative standards discussed below.

Service Provider Contracts

The privacy regulations reach a group health plan's service providers by making the plan responsible for ensuring that its business associates (e.g., service providers) take steps to avoid prohibited uses and disclosures of protected health information. Thus, the group health plan must enter into specific contractual provisions with its business associates to ensure compliance with the privacy rules. Further, the plan may be held liable for privacy violations by its business associates if it is aware of a violation but fails to take any steps to end the violation, or if the required contract provisions are not included in the parties' arrangement.

The privacy regulations will require that specific terms be included in the contracts between a group health plan and its business associates. In particular, the contract must:

- Establish the permitted and required uses and disclosures of protected health information by the business associate;
- Not allow the business associate to use or further disclose the information in a manner that would violate the privacy rules, except that the contract may permit the business associate to
  - —Use and disclose protected health information for the proper management and administration of the business associate, and
  - —Provide data aggregation services relating to the health care operations of the covered entity;
- Provide that the business associate will:
  - —Not use or further disclose the information other than as permitted or required by the contract or required by law,
  - —Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract,
  - —Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware,
  - —Ensure that any agents, including a subcontractor, to whom it provides protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information,

—Give a participant access to his or her protected health information,
—Enable a participant to amend his or her protected health information on request or explain a denial of the request,
—Provide a participant, on request, with an accounting of all disclosures of his or her protected health information, except for disclosures to carry out treatment, payment, and health care operations,
—Make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information, and
—At termination of the contract, return or destroy all protected health information, or if that is not feasible, limit further uses and disclosures of the information; and

- Authorize termination of the contract by the group health plan if the plan determines that the business associate has violated a material term of the contract.

Because the privacy regulations become effective for most health plans in April 2003, these requirements will become an important factor in negotiating third-party administration contracts for health plans and medical reimbursement accounts, and contract renewals, in the next year to 18 months. Employers should consider, in particular, whether they have any contractual protection if a third-party administrator fails to comply with the HIPAA regulations, or whether (as is often the case) the employer will be in the position of indemnifying the administrator for its negligent violations. Many third-party administrators are only now beginning to address HIPAA, and their "form" agreements do not yet reflect the new requirements.

Administrative Procedures and Safeguards

In addition to requiring the revision of plan documents and the negotiation of new plan service agreements, the privacy regulations require group health plans—and by extension, the plan sponsor—to implement detailed, written administrative procedures governing their privacy practices. These practices will significantly alter how the plan operates, and will necessitate a significant compliance effort well in advance of the 2003 deadline. Except for fully insured group health plans that do not receive protected health information (which are nonetheless subject to item 8 below), plans must, for example:

1. Designate a privacy official who is responsible for the development and implementation of the plan's privacy policies and procedures;
2. Train employees on the privacy policies and procedures governing protected health information;
3. Provide procedures for individuals to request copies of their protected health information, to request amendments to their protected health information, and to file complaints concerning the plan's privacy policies and procedures;
4. Adopt and apply appropriate sanctions against members of its workforce who fail to comply with the plan's privacy policies and procedures;
5. Mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the privacy requirements by the plan or its business associates;
6. Track all disclosures of protected health information, other than permitted disclosures in the course of treatment, health care operations, and payment;
7. Track all violations of, or complaints regarding, the plan's privacy policies and document how the violations or complaints were resolved;
8. Refrain from any intimidating or retaliatory acts against anyone who exercises his or her rights under the privacy rules, including the filing of a complaint, or who files a complaint with the Secretary of HHS; and
9. Adopt appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This last requirement may include, for example, requiring documents containing protected health information to be stored separately within the employer's facilities, and physically restricting access to the information.

It is not enough for the plan to have in place commonsense practices to protect the privacy of protected health information. Rather, the plan is required to formally implement policies and procedures with respect to protected health information that are designed to comply with the standards, specifications, and other requirements of the privacy rules. These must be in writing, and compliance must be documented as well. The regulations require that the plan retain such documentation for at least six years from the date of its creation.

Notice of Privacy Practices

A self-funded group health plan must notify participants of its uses and disclosures of protected health information and of the participants' rights and the plan's legal duties with respect to the information. Different rules apply to insured group health plans, where the insurer is generally required to provide a privacy notice to participants. The privacy regulations specify the required elements for the content of the privacy notice. For example, the privacy notice must contain the following statement as a header or otherwise prominently display the statement:

> THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Note that the plan sponsor may not require an individual to provide a blanket waiver of his or her rights under the privacy rules as a condition of the provision of treatment, payment, enrollment, or eligibility for benefits, although specific authorizations for use are permitted.

ELECTRONIC TRANSACTION REGULATIONS

The HIPAA regulations require health plans, health care clearinghouses, and most health care providers to exchange certain health information electronically using uniform codes and formats. Currently, hundreds of different formats are used in exchanging health data electronically. Under the HIPAA regulations, certain exchanges of health information must be sent according to a prescribed standard. For most group health plans, satisfying the electronic transaction regulations will require a major upgrade in computer systems.

A group health plan sponsor can determine whether it is required to follow a prescribed standard by asking the following questions:

- Is the exchange of information (the transaction) one for which a standard has been identified? (See Exhibit 1.)
- Are the parties on either side of the transaction covered entities, or has a covered entity engaged a business associate to conduct the transaction on its behalf?

If the answer to each of these questions is yes, the electronic transaction regulations may apply to the exchange of the information. Note that the electronic transaction regulations do not apply to a plan sponsor's enrollment functions on behalf of its employees or to certain transactions between the plan and its own business associates.

Exhibit 1. Standards Applicable to Electronic Transactions

Transaction	Standard (version may change)
Health care claims or equivalent encounter information	• Retail drug claims: NCPDP, v. 5.1 • Dental, professional, and institutional claims: ASC X12N 837, v. 4010
Health plan eligibility	• Retail drug: NCPDP, v. 5.1 • Dental, professional, and institutional: ASC X12N 270/271, v. 4010
Referral certification and authorization	• ASC X12N 278, v. 4010
Health care claim status	• ASC X12N 276/277, v. 4010
Health plan enrollments and disenrollments	• ASC X12N 834, v. 4010
Health care payment and remittance advice	• Retail drug claims: NCPDP, v. 5.1 • Dental, professional, and institutional claims: ASC X12N 835, v. 4010
Health plan premium payments	• ASC X12N 820, v. 4010
Coordination of benefits	• Retail drug claims: NCPDP, v. 5.1 • Dental, professional, and institutional claims: ASC X12N 837, v. 4010

Generally, the standards are a prescribed set of rules and protocols for describing the particular products or services and required related information. These standards are developed and maintained by external organizations, accredited by the American National Standards Institute, that develop and maintain standards for information transactions or data elements. At this writing, the implementation guidelines were available at www.wpc-edi.com and www.ncpdp.org. Additional information about the HIPAA regulations may be obtained from the HHS Web site at www.hhs.gov.

CONCLUSION

How significant are the new HIPAA regulations? For self-insured plans and their third-party administrators, the regulations will fundamentally affect all as-

pects of plan administration. The regulatory burden may cause some employers to rethink their in-house administrative functions and may make self-insurance for smaller plans significantly less attractive.

Compliance necessarily includes an action plan of items and tasks that must be completed. Sponsors of both insured and self-insured health plans should consider the impact of HIPAA on all of their provider contracts at their next renewal period. Doing so will place the sponsor in a significantly better position than waiting until HIPAA becomes effective in the middle of a contract period.

Plan sponsors of self-insured plans (or insured plans that receive protected health information) should be more proactive, taking the following steps to ensure compliance no later than April 2003:

- Apprise key management personnel of the scope of HIPAA and the consequences of noncompliance.
- Develop a compliance program and implementation time frames.
- Budget for HIPAA expenses.
- Focus on establishing the appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
- Review and revise group health plan documents.
- Confirm compliance with HIPAA by any insurers.
- Appoint a privacy officer to develop the plan's policies and procedures and a contact person to receive complaints concerning the plan's policies and procedures.
- Review and renegotiate contracts with business associates.
- Draft forms for
  - —Consent;
  - —Authorization;
  - —Certification by the plan sponsor that plan documents have been amended; and
  - —Notice of the plan's privacy practices.
- Train employees about privacy obligations.
- Develop policies and procedures to
  - —Address requests for access to, accounting for, and amendment of protected health information;
  - —Document compliance and provide for retention of documentation;
  - —Provide a process for participants to make complaints concerning the plan's policies and procedures or the plan's compliance with them; and
  - —Apply sanctions against employees who fail to comply with the plan's policies and procedures.
- Make required operation and system changes to implement standard transactions.
- Audit and monitor the plan's detailed HIPAA policies and procedures and its compliance with the HIPAA regulations.