Wiley Rein & Fielding LLP

1776 K STREET NW
WASHINGTON, DC 20006

PHONE 202.719.7000
FAX 202.719.7049

THE HIPAA PRIVACY RULE: CHALLENGES AND OPPORTUNITIES

I. The Privacy Rule – An Overview

A. The Standards for the Privacy of Individually Identifiable Health Information (or the "Privacy Rule") directly apply to the following three types of entities (referred to as "covered entities").

1. Health Plans – include health insurance issuers and HMOs, employer group health plans (including any employer's own group health plan), and certain specified health care programs (such as Medicare, Medicaid, and the Federal Employees Health Benefits Program).

2. Health Care Clearinghouses – are defined as companies that convert health information received from entity from nonstandard content or format into standard data elements or a standard transaction, or vice versa. Although clearinghouses are covered entities in their own right, the Privacy Rule recognizes that in most relationships with clearinghouses, the clearinghouse will be a "business associate" (discussed below).

3. Health Care Providers – are covered by the Privacy Rule if they conduct one of the eight transactions covered by the HIPAA Standards for Electronic Transactions. Importantly, the Privacy Rule does not apply to those providers who choose not to send the specified electronic transactions.

B. The Privacy Rule also indirectly applies to "business associates" (discussed in section IV below).

C. Enforcement

1. The penalties applicable to the Privacy Rule (and all Administrative Simplification provisions) and include civil monetary penalties and criminal penalties.

2. The U.S. Department of Health and Human Services ("DHHS") intends to issue an enforcement regulation to provide guidance on the imposition of penalties.

D. The compliance date for the Privacy Rule is April 14, 2003.

II. Overview – Covered Entity

A. The Privacy Rule imposes three distinct requirements on covered entities: (i) that the covered entity use or disclose individually identifiable health information (referred to as protected health information or "PHI")* only as expressly authorized by the Rule; (ii) that the covered entity provide individuals certain rights with respect to their individually identifiable health information; and (iii) that the covered entity meet certain administrative requirements prior to using or disclosing individually identifiable health information.

B. There are special rules that apply to health plans when serving in their role as a covered *group health plan*.

1. The Privacy Rule distinguishes between the "plan sponsor" (the employer) and the "group health plan" (the covered entity) in part to reinforce the prohibition against an employer using PHI to make employment-related decisions.

2. Generally, the Privacy Rule holds that group health plans may disclose PHI to plan sponsors *only if* plan sponsors agree to amend their plan documents to include certain statements restricting the uses and disclosures of PHI.

III. Overview – Business Associate

A. A business associate is any entity who: (i) on behalf of a covered entity performs or assists in performing a function or service that involves the use or disclosure of PHI, or any other function regulated by the Privacy Rule; or (ii) provides legal, actuarial, accounting, consulting, data aggregation, management, accreditation, administrative, or financial services if the service involves the disclosure of PHI from the covered entity or from another business associate of the covered entity.

B. The business associate requirements include an exception for members of a covered entity's "workforce." This means, therefore, that employees, volunteers,

* "Protected health information" is defined as individually identifiable health information, including demographic information, collected from a member or created or received by a covered entity or an employer (when functioning on behalf of the group health plan) and that relates to: (i) past, present, or future physical or mental health or condition; (ii) providing health care; or (iii) past, present, or future payment for providing health care. Because of this expansive definition, PHI includes much more than medical diagnoses, and may include simply a member's name and address if this information has been provided for the purposes of securing payment for health care.

trainees, and other persons whose conduct in performing work for the covered entity is under the covered entity's direct control, regardless of whether they are paid, are not "business associates."

C. Other exceptions to the business associate requirements include:

1. Disclosures of PHI by network providers to a health plan for payment. In fact, DHHS (the Office of Civil Rights, "OCR") issued guidance recently that expressly provides that "[a] provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the 'business associate' of another."

2. Disclosures by a group health plan to a plan sponsor (if certain requirements of the Privacy Rule are met).

D. The Privacy Rule requires that business associates execute contracts with the covered entity to provide satisfactory assurance that the business associate will appropriately safeguard PHI. Thus, when a health insurer is a business associate (*e.g.,* as a TPA) it must execute a Business Associate Contract with the covered group health plan. Likewise, a health plan's PBM and behavioral health care contractor must each execute Business Associate Contracts with the health plan.

E. In summary, a business associate cannot use or disclose PHI in a manner that would be prohibited if done by the covered entity. In other words, a business associate is under the same constraints as the covered entity with which it has contracted with regard to permitted or required uses and disclosures of PHI (*i.e.,* it stands in the shoes of the covered entity). Consequently, a business associate would not be permitted to use or disclose PHI in a manner that would be prohibited under the Privacy Rule if undertaken by the covered entity with which it contracts. Therefore, the purpose of the Business Associate Contract is to ensure that a business associate is committed by contract to the same use and disclosure limitations and various other obligations as the covered entity.

F. The Privacy Rule contains a list of provisions to be included in the Business Associate Contract.

1. In summary, the required contract terms include that the business associate will:

a. Only use or disclose PHI as permitted under the contract and not in a manner that would violate the Privacy Rule if such actions were taken by the covered entity;

b. Report any known misuse of PHI to the covered entity;

c. Impose the same requirements on any subcontractors and agents of the business associate;

d. Generally make an individual's PHI available and provide to the individual an accounting of certain disclosures (or provide such access or accounting to the covered entity to provide to individuals) as required by the Privacy Rule; and

e. Make its internal practices, books and records relating to the use and disclosure of PHI available to DHHS.

2. In addition, the business associate contract must allow the covered entity to terminate the contract if it determines that the business associate has violated a material term of the contract. If feasible, the business associate must return or destroy all PHI and retain no copies upon termination of the contract. If return or destruction is not feasible, the protections of the contract must be extended to the PHI, and the business associate must limit further uses and disclosures to the purposes that make the return or destruction infeasible.

G. With respect to their business associates, any covered entity violates the Privacy Rule *only if it knew* of a pattern of activity or practice of the business associate that violated the contract, and (i) the covered entity failed to take reasonable steps to cure the breach, or, (ii) if cure was unsuccessful, the covered entity failed to terminate the contract (where termination was feasible) or failed to report the breach to DHHS (where termination was not feasible).

H. Typical Business Associate Relationships for health plans

1. As a TPA providing administrative services to its self-insured group health plan customers;

2. As a clearinghouse;

3. Agents and brokers working on behalf of the health plan;

4. Contractors whose services involve the creation, use or disclosure of PHI, such as contracted PBM, behavioral health care vendor, or dental or vision carriers;

5. NCQA and other accreditation organizations;

6. Attorneys who handle claims litigation; and

7. Various consultants who use or disclose PHI received from the health plan.

IV. Implementation Obligations for a Covered Entity and a Business Associate

A. As noted previously, the Privacy Rule imposes three distinct obligations on covered entities: (i) that the covered entity use or disclose individually identifiable health information only as expressly authorized by the Rule; (ii) that the covered entity provide individuals certain rights with respect to their individually identifiable health information; and (iii) that the covered entity meet certain administrative requirements prior to using or disclosing individually identifiable health information.

B. Use and Disclosure Restrictions

1. The Privacy Rule governs when and how covered entities may use and disclose PHI without authorizations.

2. The Privacy Rule imposes *uniform* obligations on covered entities and business associates with regard to the uses and disclosures of PHI. In other words, the Rule does not distinguish between a covered entity and business associate concerning how PHI may be used and disclosed. Thus, the same limitations imposed on a company when it is a covered entity apply when it is a business associate.

3. The general rule is that a covered entity (or its business associate) may use and disclose PHI without consent or authorization for "treatment, payment, and health care operations (TPO)," for "national priority purposes," and as otherwise permitted by the Privacy Rule.

4. The functions included within the "TPO" category include most of the day-to-day functions that need to be undertaken by a typical covered entity in the administration of its various benefit programs or other health care services. The "national priority" category includes many of the disclosures of health information that covered entities may need to make (*e.g.,* in response to subpoenas, to health oversight agencies, when disclosure is required by law).

5. Disclosures under the Privacy Rule generally are *permissive* rather than mandatory (even for many of the national priority purposes). Therefore, in situations where a covered entity is permitted to use or disclose PHI, it may do so, but typically is not required to do so.

C. Individual Rights

1. The Privacy Rule also imposes *uniform* obligations on covered entities and business associates to provide individuals certain rights with respect to their PHI.

2. Accordingly, a *covered entity* and a *business associate* is required to establish mechanisms for providing individuals the following privacy rights:

   a. Right to request restrictions on uses and disclosures of PHI;

   b. Right to request communications by alternative means or alternative locations;

   c. Right of access to PHI in designated record sets;

   d. Right to request amendment of PHI; and

   e. Right to an accounting of certain disclosures of PHI.

D. Administrative Obligations

1. The Privacy Rule imposes ***different*** obligations on covered entities and business associates with respect to the administrative obligations they must meet. Thus, the difference between status as a covered entity and status as a business associate will be seen in the administrative obligations that the Privacy Rule imposes.

2. Under the Privacy Rule, the administrative obligations placed on a covered entity are far more extensive than those the Privacy Rule imposes on business associates. In practice, however, a business associate (*e.g.,* a TPA) may agree, by contract, to implement the administrative obligations on behalf of its covered entity (*e.g.,* the covered group health plan). Thus, operationally these differences may not be significant in all instances.

3. Administrative obligations of a *covered entity*

   a. Appoint a privacy official;

   b. Establish a contact office;

   c. Distribute a Notice of Privacy Practices;

   d. Develop privacy policies and procedures;

   e. Train the workforce on the privacy policies and procedures;

   f. Execute business associate agreements with all business associates;

   g. Establish reasonable administrative, technical and physical safeguards to protect PHI from any intentional or unintentional use or disclosure that violates the Privacy Rule;

h. Establish a process by which individuals may file complaints;

i. Develop appropriate sanctions that will be applied to workforce members that fail to comply with the privacy policies and procedures;

j. Develop a mitigation strategy to address known violations of the privacy policies and procedures, or of the Privacy Rule; and

k. Ensure that workforce members refrain from:

(i) Taking any retaliatory actions against individuals or others for exercising their rights under the Privacy Rule, or for filing complaints; and

(ii) Requiring individuals to waive their rights under the Privacy Rule as a condition of receiving treatment, payment, enrollment in a health plan, or eligibility for benefits.

4. Administrative obligations of a *business associate*

a. Enter into business associate agreements with its various covered entities (*e.g.,* group health plans);

b. Establish reasonable safeguards to protect PHI;

c. Report to the contracted covered entity any use or disclosure of which it becomes aware that does not comport with its business associate agreement;

d. Require all agents and subcontractors to which it supplies PHI received from (or on behalf of) the covered entity to agree to the same restrictions and conditions that apply to the business associate with respect to the use and disclosure of the PHI; and

e. Make its internal practices, books and records relating to the use and disclosure of PHI received by (or on behalf of) the covered entity, available to the Secretary of DHHS to determine the contracted covered entity's compliance with the Privacy Rule.

E. Summary –Implementation Considerations

1. To meet its obligations under the Privacy Rule, some of the major initiatives a covered entity will need to undertake are:

a. Establish policies and procedures to ensure internal uses and external disclosures of PHI comport with the Privacy Rule;

b. Develop and roll out the Notice(s) of Privacy Practices;

c. Provide workforce privacy training;

d. Develop a contract amendment strategy for business associates, and a contract amendment strategy when the covered entity itself is a business associate;

e. Establish processes and workflows to ensure its compliance with the "individual rights" provisions (*e.g.,* developing a process to track those disclosures that must be accounted for; establishing a process to provide individuals access to PHI in designated record sets, etc.)

For further information on the HIPAA Privacy Rule or its effects on covered entities and others affected by the HIPAA rules, please contact Kirk J. Nahra at 202.719.7335 or Knahra@wrf.com or Dot Powell-Woodson at 202.719.7150 or Dpowell-woodson@wrf.com.