PROSKAUER ROSE LLP®

# Client Alert

A report for clients and friends of the firm

October 2001 (as updated June 2004)

# HIPAA Compliance Update: Employers, As Group Health Plan Sponsors, Will Be Affected By HIPAA Privacy Requirements

***The U.S. Department of Health and Human Services published HIPAA rules relating to the privacy, security and transmission of individually identifiable health information. Although attention has focused thus far on how these rules affect health care providers and health insurers, the broadly drafted rules also place new responsibilities on employers and other entities in their capacity as sponsors of group health plans. This Alert summarizes some of the ways in which HIPAA's privacy rules reach employers and other plan sponsors, and the kinds of steps that may be required to assure HIPAA compliance, and also briefly summarizes the HIPAA Security and EDI Rules.***

## Introduction

The U.S. Department of Health and Human Services ("HHS") has published rules relating to the privacy, security and transmission of individually identifiable patient health information, pursuant to the "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). In general, the HIPAA rules impose obligations on "covered entities," which are defined in HIPAA as health plans, health care clearinghouses and certain health care providers.

Employers (in their capacity as such) technically are not subject to these rules as "covered entities." However, certain employers will be required to ensure compliance with HIPAA requirements because they sponsor "group health plans." HIPAA, relying in part on the Employee Retirement Income Security Act ("ERISA") for its definition of "group health plan," defines the term to include both insured and self-insured employee welfare benefit plans that (i) have 50 or more participants (or, if there are fewer than 50 participants, are administered by an entity other than the employer sponsor) and (ii) provide health benefits. Depending upon the nature of an employer-sponsored health plan, an employer may take on material responsibilities, under HIPAA, with respect to its health benefit activities.

Since the publication of HIPAA's privacy, security and electronic data interchange rules, many plan sponsors (including employers) have begun to inquire about what steps should be taken in order to comply with the requirements imposed by the rules. This Alert generally responds to these inquiries with a brief explanation of the rules, as well as an overview of the steps that may need to be taken in order to comply with them. Due to the comprehensive nature of HIPAA's privacy rules, and their relevance to group health plans and their sponsors, this Alert focuses primarily on those rules.

## The Privacy Rule

***The Basics.*** On December 28, 2000, HHS published the first final rule of "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Rule"), which relates to the privacy of oral, written and electronic health information. On August 14, 2002, HHS issued a revised, final Privacy Rule. The Privacy Rule imposes obligations on "covered entities" — health plans, health care clearinghouses, and most health care providers — to maintain the privacy of patient health information. In particular, the Privacy Rule controls the dissemination of "protected health information," which is defined as individually identifiable health information transmitted by electronic media, maintained in any electronic medium, or transmitted or maintained in any other form or medium. Covered entities, except "small health plans," as

defined in the Privacy Rule, were required to comply with the Privacy Rule by April 14, 2003. The Privacy Rule defines "small health plans" as health plans with annual receipts — *i.e.*, premiums or their functional equivalent — of less than $5 million, and these entities had an additional year (until April 14, 2004) to achieve compliance.

***Disclosure Prohibition.*** In general, the Privacy Rule permits group health plans to use and disclose an individual's protected health information without obtaining the individual's authorization *only* if the use or disclosure is to carry out "treatment, payment or health care operations" (and is not with respect to psychotherapy notes), or if the use or disclosure falls within one of the limited circumstances described in the Privacy Rule (*e.g.*, the disclosure is required by law or for public health activities). The Privacy Rule generally defines "treatment" as care provided by health care professionals, such as physicians. With respect to health plans, "payment" is defined in broad fashion to involve activities associated with eligibility and coverage determinations, coordination of benefits, claims management, utilization review and other related health plan administrative activities. "Health care operations," also broadly defined, appears to cover other health plan administrative tasks that may fall outside of the "payment" definition, such as quality improvement activities, health care professional selection and accreditation, activities related to obtaining health insurance policies or stop loss insurance, and legal and auditing functions.

Under these definitions, employers and other plan sponsors (such as the trustees of health plans established pursuant to collective bargaining agreements) should bear in mind that the group health plans they sponsor generally will be required to obtain the authorization of an affected employee in order to use or disclose protected health information *for purposes other than* treatment, payment or health care operations, such as for employment-related purposes.

***Sharing Information With Plan Sponsors.*** HHS has insisted that it does not intend to regulate employers under the Privacy Rule. However employers, in their role as sponsors of health benefits for their employees, and to the extent they have "in-house" benefits personnel (for example, human resources personnel that address health benefits issues, and managers serving as health plan fiduciaries under ERISA), are nevertheless required to take certain steps to protect individually identifiable health information.

The Privacy Rule accomplishes this indirect regulation by essentially providing that the employer, in its role as a group health plan sponsor, comprises a different legal entity under HIPAA than the ERISA-regulated group health plan that the employer sponsors. In-house employees who provide health benefit functions are considered to be HIPAA-regulated health plan personnel when serving those functions. These functions may include, for example, entering into agreements with and otherwise monitoring and interacting with health insurers, third party administrators and other health service vendors, making eligibility determinations, collecting and tallying employee medical receipts under self-administered flexible spending account plans established under Section 125 of the Internal Revenue Code, assisting in case management activities when costly health care items are involved, and monitoring health benefit utilization to identify appropriate incentives to control health benefit costs. Records and information that contain individually identifiable health information, and that are developed and used by this staff in performing these functions, are protected by HIPAA and are subject to the Privacy Rule's web of requirements.

One of the great puzzles of HIPAA is when, exactly, a transfer or disclosure of protected health information will be considered to occur between the component of an employer that constitutes a HIPAA-regulated health plan, and the component of an employer that constitutes a supposedly non-regulated health plan sponsor. What is clear is that unless the individual who is the subject of the transferred information provides specific permission for the transfer (which, in practice may prove an impractical approach if information pertaining to large numbers of employees is sought), whenever any such disclosure is made it will violate the Privacy Rule unless (i) the transfer is in furtherance of plan administration purposes; (ii) the health plan documents are amended to include certain very specific provisions set forth in the Privacy Rule; and (iii) the employer/sponsor agrees to take certain actions in order to control the permitted uses and disclosures of protected health information.

It should be noted that these requirements do not apply if the employer is fully insured with respect to the health plan benefits, and only is provided with (i) "summary health information," as defined in the Privacy Rule, for the purpose of obtaining premium bids or for modifying or terminating the plan, and/or (ii) information that consists solely of whether or not an individual has been enrolled or disenrolled from a health insurer or HMO offered by the plan. The Privacy Rule generally defines "summary health information" as claims-related information that is in a form that excludes individual beneficiary identifiers — such as names, addresses, social security numbers or other unique beneficiary-identifying numbers or characteristics.

It should also be noted that HIPAA "health plans" also include traditional health insurance entities, such as HMOs and health insurance companies. This means that if an employer's human resources department wishes to have access to the HIPAA-protected health information maintained by a health insurer, and does not desire "summary health information" (for example it may wish to conduct a detailed audit of insurer performance or it may

require individually-identifiable information to engage in case management activities for groups of beneficiaries using high-cost services), it will be necessary to make appropriate amendments to plan documents and to take the required actions with respect to the information that is obtained.

In general, the mandated amendments to the health plan documents include provisions to establish the permitted and required uses and disclosures of the HIPAA-protected information by the plan sponsor. They also include provisions that the group health plan will only disclose protected health information to the sponsor upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the mandated provisions.

Specifically, the provisions that must be incorporated into the plan documents (and the provisions to which the plan sponsor must agree) include, but are not limited to, the plan sponsor's agreement: (i) not to use or further disclose protected health information other than as permitted or required by the plan documents or as required by law; (ii) to ensure that any agents to whom it provides protected health information agree to the same restrictions and conditions as apply to the plan sponsor with respect to such information; (iii) not to use or disclose the information for employment-related actions and decisions or in connection with any other benefit or benefit plan; (iv) to report to the plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware; (v) to make available protected health information in accordance with the rules regarding access of individuals; and (vi) to ensure separation between the sponsor and the plan (*i.e.*, to create "firewalls"). With regard to this last point, the plan documents must identify the individuals or classes of individuals who have access to the information, restrict access so that only those identified individuals will have access to such information for the plan administration functions that the sponsor performs for the plan, and provide for an effective mechanism for resolving any issues of noncompliance by such persons.

***Other Compliance Duties.*** The Privacy Rule contains other administrative requirements applicable to group health plans that may also impact employers and other sponsors of such plans. Specifically, health plans are required by the Privacy Rule to: (i) adopt privacy policies and procedures; (ii) designate a privacy officer responsible for the development and implementation of the plan's policies; (iii) train all health plan workforce with respect to privacy policies and procedures; (iv) establish appropriate administrative, technical and physical safeguards to protect the privacy of protected health information; (v) establish a process for complaints; (vi) establish and apply sanctions for failures to comply with privacy policies and procedures; (vii) maintain all HIPAA compliance-related documentation for at least six years; and (viii) assure that the plan has written agreements with its business associate(s) that require those business associates (such as third party administrators and brokers) to comply with a subset of the Privacy Rule requirements. It should be noted that if a group health plan provides benefits solely through an insurance contract with an HMO or other health insurer (*i.e.*, it offers no self-administered flexible spending account plans or other self-funded health benefits), and the health plan does not create, receive or maintain protected health information (other than summary health information or enrollment/disenrollment/participation information), then the group health plan is relieved from complying with these organizational mandates.

Group health plans, as HIPAA-covered entities, also are required to provide named participants with a privacy notice, which sets forth the permissible uses and disclosures of protected health information and explains individuals' rights, as well as the duties of covered entities, with respect to protected health information. In the case of self-insured group health plans, the notice must be provided by the HIPAA-regulated group health plan (although this requirement may be delegated contractually to a third party administrator). In the case of plans that provide benefits through a health insurance issuer or HMO, the notice must be provided by the issuer or HMO. Even in the latter case of fully-insured health plans, the group health plan itself may be obligated to maintain the notice and provide it to individuals upon request, if the plan creates or receives protected health information in addition to summary health information or enrollment/disenrollment information. The Privacy Rule includes specific requirements as to the content, timing and manner of distribution of the notice.

## The EDI Rule

On August 17, 2000, HHS published as a final rule the "Standards for Electronic Transactions," *i.e.*, "electronic data interchange" or "EDI" (the "EDI Rule"). On February 20, 2003, a revised final EDI Rule was issued. The EDI Rule establishes standards for the format of certain electronic transactions relating to health care, including medical claims, eligibility inquiries, enrollment and premium payments. The EDI Rule also mandates the use of certain medical data code sets to be used in those transactions. A code set is any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes or medical procedure codes.

The code sets adopted as the initial requisite code sets under HIPAA are the code sets already in use by many health plans, health care clearinghouses and health care providers. The EDI Rule also contains requirements regarding the use of those standards by health plans, health care clearinghouses and certain health care providers. Covered entities (except for small health plans) were required to either comply with the EDI Rule by October 16, 2002, or submit a one-year

extension for the compliance deadline. Small health plans automatically had an additional year to comply.

The first step for the group health plan in EDI Rule compliance, is to determine whether it conducts any transaction covered by the EDI Rule. If it does, the next step toward compliance is to determine the ability of the plan's (or its outside administrator(s)') computer systems and operations to use and accommodate the standard transactions and code sets. Like the Privacy Rule, the EDI Rule does not directly regulate employers and plan sponsors. Therefore, transactions that are deemed to be actions of the plan sponsor (*e.g.*, premium payments) need not be in HIPAA-compliant EDI format.

## The Security Rule

On February 20, 2003, the Centers for Medicare and Medicaid Services ("CMS") of HHS published as a final rule "Health Insurance Reform: Security Standards" (the "Security Rule"). This rule, compliance with which is required by April 20, 2005 (except for small health plans which have an additional year to comply), requires health plans to adopt certain safeguards, and satisfy certain administrative requirements, to protect the security of individually identifiable health information that is electronically maintained or electronically transmitted.

In general, the Security Rule addresses administrative, physical and technical requirements. The administrative requirements include establishing and maintaining personnel security policies and procedures; the physical security requirements include installing physical access controls; and the technical security requirements include access, audit and authorization controls, and data and entity authentication.

Various other Security Rule requirements obligate health plans to have disaster recovery plans, to include security provisions in its business associate agreements with certain service providers, and to retain records (in written or electronic form) of security compliance policies and procedures. The Security Rule is intended to be scalable, taking into account the size, complexity, capabilities, technical infrastructure, hardware, and software of the covered entity, as well as the compliance costs and probability of risks to the security of the electronic protected health information.

In general, employers that are self-insured with respect to their health plans (and/or fully-insured employers who receive more than summary health information or enrollment/disenrollment information, as discussed above), will need to ensure that their third party administrators comply with the Security Rule, and will further need to ensure that their benefits department personnel comply, to the extent that such personnel maintain or transmit electronic protected health information as part of health plan administration.

## Penalties

The Administrative Simplification provisions of HIPAA establish civil monetary penalties for violations of the Privacy, EDI and Security Rules by covered entities. Penalties may not exceed $100 per violation, or $25,000 per year for violations of an identical requirement. These penalties can be imposed on covered entities. An interim final rule on "Civil Money Penalties: Procedures for Investigations, Impositions of Penalties and Hearings" was issued by HHS on April 17, 2003. Many HIPAA enforcement questions and issues remained unaddressed by this interim rule. HHS announced that a complete, final rule was to be forthcoming, but none has been issued to date.

The Administrative Simplification provisions also establish criminal penalties for violations of the Privacy Rule by covered entities for knowingly using, obtaining or disclosing individually identifiable health information. The statute contains three levels of criminal penalties. First, up to $50,000 and/or up to 1 year in prison for knowingly obtaining or disclosing individually identifiable health information in violation of HIPAA (known as a "simple violation"). Second, up to 5 years in prison and/or up to a $100,000 fine for knowingly obtaining individually identifiable health information under "false pretenses." Third, up to 10 years in prison and/or up to a $250,000 fine for knowingly using or disclosing individually identifiable health information for commercial advantage, personal gain, or malicious harm.

Finally, it is generally anticipated that the new HIPAA privacy protections will be considered by many courts to create a new standard of reasonable and prudent practice in the care of individually identifiable health data. Accordingly, it is predictable that in the years to come, HIPAA standards will serve as the basis for state law actions seeking damages for the breach of an individual's right to the confidentiality of his or her medical information.

NEW YORK • LOS ANGELES • WASHINGTON

BOSTON • BOCA RATON • NEWARK • PARIS

## Proskauer's HIPAA Practice Group

**Proskauer Rose's HIPAA Practice Group combines the unmatched expertise and experience of Proskauer's labor/employment, health care and employee benefits law departments. It is available to assist you in interpreting HIPAA's complex rules and their applicability to you and your group health plans. HIPAA Practice Group attorneys have worked extensively on behalf of health care and employer clients in this area, developing efficient and practical approaches, preparing required procedures and documentation, and otherwise helping to identify and implement timely, cost-conscious HIPAA compliance strategies.**

## For further information, please contact:


**Ira Golub**
212.969.3008 — igolub@proskauer.com

**Edward Kornreich**
212.969.3395 — ekornreich@proskauer.com

**Roberta Chevlowe**
212.969.3949 — rchevlowe@proskauer.com

**Sara Krauss**
212.969.3049 — skrauss@proskauer.com

**Ellen Moskowitz**
212.969.3232 — emoskowitz@proskauer.com


## You may also contact any other member of Proskauer's Labor and Employment or Health Care Department in:

| | |
|---|---|
| **New York** | **212.969.3000** |
| **Washington** | **202.416.6800** |
| **Boston** | **617.526.9600** |
| **Boca Raton** | **561.241.7400** |
| **Los Angeles** | **310.557.2900** |
| **Newark** | **973.274.3200** |

Proskauer Rose is an international law firm that handles a full spectrum of legal issues worldwide.



You can also visit our Web site at **www.proskauer.com**