RUSKIN MOSCOU FALTISCHEK P.C.
Counselors at Law

HIPAA Privacy Regulations: Worth Their Weight?

By: Melvyn B. Ruskin,
Chair, Health Law Department
and Keshia B. Haskins,
*Health Law Department**

June 6, 2001

Introduction

Federal privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") [1] became final on April 14, 2001 ("HIPAA privacy regulations"). [1]

These regulations require "covered entities" [2] in the health care industry and "business associates" [3] with which such entities do business to protect the confidentiality of patient health information. These regulations also provide individuals with significant rights to ensure that entities which possess their health information keep it confidential.

The HIPAA privacy regulations have received mixed reviews, with privacy advocates trumpeting them as much needed regulatory consumer protection and the health care industry labeling them as overbroad, burdensome and excessively costly to implement. Regardless of one's position in this debate, the HIPAA privacy regulations are here to stay and this article provides important information about them. This article explains how the HIPAA privacy regulations fit into the HIPAA administrative simplification scheme and details: (1) who must comply, (2) what information is protected, (3) the penalties for non-compliance, and (4) the initial steps affected entities should take on the road toward compliance.

What is HIPAA and how do the HIPAA privacy regulations fit into the HIPAA regulatory scheme?

HIPAA was enacted by Congress in 1996 as part of a broad Congressional attempt at incremental health care reform. [4] Among its many purposes, the HIPAA legislation requires "administrative simplification" within the health care system. [5] The HIPAA administrative simplification standards

[6] are designed to improve the efficiency and effectiveness of the health care system by establishing standards for the electronic transmission of health information while protecting confidential information from inappropriate access, disclosure and use.

Congress anticipated that regulations (or additional legislation) [7] would be adopted to implement HIPAA's administrative simplification standards, including: (1) information privacy, (2) transaction coding, (3) security, (4) enforcement, (5) format and content for health transactions, and (6) national identifiers for patients, providers, health plans, and employers. To date, only two sets of administrative simplification regulations have been published in final form – the Electronic Transactions and Code Sets Regulations (the "electronic transaction/code regulations"), [8] and the HIPAA privacy regulations. [9] The electronic transaction/code regulations require most entities in the health care industry that transmit and receive health information electronically to use standardized codes when processing business documents. [10] The deadline for compliance with the electronic transaction/code regulations is October 16, 2002. [11] The HIPAA privacy regulations create national standards concerning: (1) the use and disclosure of protected health information [12] and (2) a patient's right to access, amend, and receive a list of the disclosures of his or her protected health information. [13] The deadline for compliance with the HIPAA privacy regulations is April 14, 2003. [14]

Who must comply with the HIPAA privacy regulations?

Covered Entities

The HIPAA privacy regulations mainly apply to "covered entities." [15] Covered entities include health plans, [16] heath care clearinghouses, [17] and health care providers who transmit health claim information via computer. [18] A host of entities that deal with health information are covered entities. Hospitals, nursing homes, doctors' offices that transmit health information electronically, billing companies, third party administrators, and health insurance companies (including health maintenance organizations) are examples of covered entities.

Business Associates of Covered Entities

The HIPAA privacy regulations also apply to "business associates" [19] of covered entities. A business associate is not a covered entity, but to the

extent that a business entity receives, uses and/or discloses health information on behalf of a covered entity, it becomes subject to the HIPAA privacy regulations. [20] For example, an accounting firm would be a business associate where its activities involve the use of protected health information of its hospital or physician client. [21] A business associate must protect the confidentiality of the health information in accordance with the "use and disclosure" provisions of the HIPAA privacy regulations. [22]

Specifically, the regulations require a covered entity to obtain "satisfactory assurances" that its business associates will comply with the use and disclosure provisions of the privacy regulations. [23] A covered entity can meet this requirement by adding appropriate language to its contracts with business associates. A covered entity that discloses protected health information to a business associate without first obtaining satisfactory assurances will be out of compliance with the HIPAA privacy regulations. [24]

What health information is protected under the privacy regulations?

The privacy regulations cover "protected health information." [25] Protected health information is "individually identifiable health information" [26] that: (1) is maintained in any form or medium, (2) relates to, identifies, or could identify the person that the health information concerns, and (3) is transmitted or maintained by a covered entity. [27] Individually identifiable health information includes information created by a health care provider, health plan, employer, or health care clearinghouse that identifies [28] an individual and relates to his or her health condition. [29]

Interestingly, the privacy regulations suggest that a covered entity can reduce the amount of protected health information it handles by "de-identifying" or removing identifying information, like names or social security numbers, from its health records. [30] De-identified health information is not considered to be individually identifiable health information and is, therefore, not protected health information. [31]

What obligations do the new privacy regulations impose upon covered entities?

Use and Disclosure Requirements [32]

The HIPAA privacy regulations place various restrictions on a covered entity's use and disclosure of protected health information. [33] With some exceptions, the regulations require that proper patient "consents" [34] and "authorizations" [35] be obtained by covered entities before they disclose an individual's protected health information. The regulations also limit the quantity of protected health information that a covered entity may disclose. When disclosing health information, covered entities must apply a "minimum necessary" standard and disclose only the minimum amount of health information necessary to accomplish the intended purposes of disclosure. [36]

Individuals' Access to Their Protected Health Information

In addition to use and disclosure requirements, the HIPAA privacy regulations require covered entities to permit individuals to access their health information. [37] Access includes a right to view, amend or correct, and receive copies of health information. [38] Once during each 12-month period, without a fee, an individual may also obtain a list of parties and entities that have received his or her health information from the covered entity during the six (6) years prior to the date of such request. [39]

Covered entities must develop privacy policies that implement the HIPAA privacy regulations. They must ensure that patients receive notice of their rights under the privacy regulations. [40] Detailed provisions in the privacy regulations explain what information such notice must contain. [41]
What consequences do non-compliant covered entities face?

If a covered entity fails to adhere to the privacy regulations, it is subject to civil and/or criminal penalties initiated by the Department of Health and Human Services ("HHS"), which is charged with the responsibility to monitor and enforce these regulations. Significantly, the privacy regulations do not grant individuals a private right of action against an entity which violates the HIPAA privacy regulations. Rather, any person seeking to complain that an entity is not complying with the privacy regulations may file a complaint with the Secretary of HHS. [42]

Non-compliant entities are subject to civil monetary penalties ranging from $100 to $25,000, depending upon the extent of non-compliance. [43] Misdemeanor or felony criminal penalties apply where a covered entity wrongfully and knowingly discloses health information in violation of the privacy regulations. [44] Criminal violations are punishable by fines (up to $250,000) or imprisonment (a maximum of 10 years) or both. [45]

What should you do, if you think you are a "Covered Entity"?

By April 14, 2003, covered entities (excluding "small health plans") must comply with the HIPAA privacy regulations. [46] They must adjust personnel responsibilities, designate a privacy officer, establish mechanisms for monitoring compliance, and make adjustments to software and other technology that transmits, stores, or receives protected health information.

On July 6, 2001, the Bush Administration released "Guidance" to interpret and clarify questions about the HIPAA privacy regulations. [47] This Guidance makes clear that the Bush Administration may modify the privacy regulations in accordance with the Administrative Procedures Act until April 14, 2002. [48] Notwithstanding expected modification to the privacy regulations, the Guidance states that "*covered entities can and should begin the process of implementing the privacy standards in order to meet their compliance dates*." [2]

Because the HIPAA privacy regulations are so extensive, covered entities should presently begin to transition toward compliance. They should, for example, (1) become familiar with the detailed requirements of the HIPAA privacy regulations and (2) determine the processes they will employ to implement the regulations. We recommend that covered entities seek assistance from information technology experts and special counsel with HIPAA expertise as they embark upon the road to mandatory compliance.

Conclusion

The Health Care Financing Administration (which announced its adoption of the new name "Centers for Medicare and Medicaid Services", effective June 14, 2001) has predicted that there will be increased efficiency in the health care industry and significant long-term savings resulting from the implementation of the HIPAA administrative simplification regulations. In

connection with implementing various HIPAA administrative simplification requirements, the government has mandated the confidentiality of patient health records in accordance with the HIPAA privacy regulations. The enormity of these regulations will require covered entities to devote substantial time, money, and resources to education and compliance efforts over the next two years. Whether the HIPAA privacy regulations are ultimately worth the costs associated with their implementation will depend upon whether HIPAA's administrative simplification regulations produce the predicted long-term savings. In the short term, however, covered entities must invest in compliance with the HIPAA privacy regulations (and the electronic transaction/code regulations) and hope that this investment eventually pays off.

_____

*Melvyn B. Ruskin is a Partner and chair of the Health Law Department at Ruskin Moscou Faltischek, P.C..
Keshia B. Haskins is an associate in the firm's Health Law Department and Seniors' Housing Group