FORD & HARRISON LLP
THE RIGHT RESPONSE AT THE RIGHT TIME
LEGAL ALERT

Legal Alert: Health and Human Services' Proposed Rule to Modify the HIPAA Privacy, Security, and Enforcement Rules

7/27/2010

On July 14, 2010, the Department of Health and Human Services (HHS) published a Proposed Rule outlining modifications to the Privacy, Security, and Enforcement Rules (HIPAA Rules) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Many of the proposed modifications to the HIPAA Rules are based on requirements imposed by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted on February 17, 2009, as part of the American Recovery and Reinvestment Act, while other modifications are technical corrections to the HIPAA Rules. This legal alert will focus on the more substantive proposed changes related to business associates, the Privacy Rule, the Security Rule, and the Enforcement Rule.

Effective Dates and Compliance Dates

HHS has provided, in the proposed rule, a compliance period to give covered entities and business associates time to comply with the requirements of this proposed rule once it has been finalized. Generally, covered entities and business associates will have 180 days after the effective date of the final rule to comply with its requirements. However, this compliance period does not apply to any Enforcement Rule provisions, which will be effective upon enactment of the final rule or as otherwise specified in the final rule. Also, the compliance period is subject to the transition period for business associate agreements described below.

Business Associates

The proposed rule most significantly impacts business associates in four ways.

• The definition of a business associate under the HIPAA Rules is expanded to include: (i) individuals or organizations engaged in patient safety activities if done on behalf of a covered entity; (ii) persons or organizations who provide data transmission services with respect to protected health information (PHI) and who require access to such PHI on a routine basis; (iii) vendors of personal health records; and (iv) subcontractors of a covered entity that have access to PHI as the subcontractor provides services to or for the business associate. The proposed rule also requires business associates (not covered entities) to establish a business associate

agreement with subcontractors who have access to PHI.

• A number of the HIPAA Privacy Rule requirements regarding the use and disclosure of PHI will apply directly to the business associate including the minimum necessary rule and the requirement to only use or disclose PHI as permitted or required under the HIPAA Rules.

• The proposed rule modifies the requirements for a business associate agreement. A covered entity would not be required to report any breach or violation of the business associate agreement to HHS even if termination of the business associate agreement is not feasible. Also the parties to a business associate agreement must include provisions in the agreement requiring the business associate to take reasonable steps to cure any material breach or violation of the business associate agreement between the business associate and a subcontractor, or terminate the contract. The business associate agreement must also contain provisions requiring a business associate to comply with the Security Rule, report breaches of unsecured PHI to the covered entity, and ensure any subcontractors comply with the same rules applicable to business associates.

• Finally, there is a transition period for business associates and covered entities to comply with the requirements under the proposed rule related to business associate agreements. The transition period provision provides that existing business associate agreements will be deemed compliant with the proposed rule until the earlier of the date of any contract modifications after the 180 day compliance period, or one year after the 180 day compliance period.

Privacy Rule

Several key changes to the privacy rule are outlined in the proposed rule, including:

• modifications to the definition of marketing to clarify when a valid authorization will be required before PHI may be used or disclosed to market a product or service to an individual;

• a requirement that the Notice of Privacy Practices include a statement describing the types of uses and disclosures of PHI that will require an authorization when psychotherapy notes, marketing communications, or the sale of PHI are involved and that other uses and disclosures of PHI not described in the Notice of Privacy Practices will require the individual's authorization; a statement explaining that a covered entity must honor requests to restrict certain uses and disclosures of PHI; and, to the extent applicable, a health care provider must include a statement that it intends to provide communications regarding treatment alternatives or other health related products or services where such communications have been paid for by another party. The proposed rule indicates that such changes to the Notice of Privacy Practices are material and will require republication and distribution of the Notice of Privacy Practices;

• details on how a covered entity may comply with the HITECH Act requirement that individuals be afforded a right to obtain or access a copy of their PHI in an electronic format; and

• a rule prohibiting a covered entity or business associate from receiving

direct or indirect compensation in exchange for the disclosure of PHI unless the covered entity has obtained a valid authorization or one of the exceptions apply. The authorization must include a statement that the covered entity or business associate is receiving compensation in exchange for disclosure of the PHI.

The proposed rule does not provide guidance on the minimum necessary standard under the Privacy Rule. Instead, comments are requested on what aspects of the minimum necessary standard should be addressed in future guidance.

Security Rule

The proposed rule clarifies that the administrative, physical, and technical safe guard requirements under the Security Rule will apply to business associates in the same manner such requirements apply to covered entities.

Enforcement Rule

The proposed rule clarifies that the Office of Civil Rights (OCR) is obligated to conduct an investigation if a preliminary review of the facts and circumstances indicate a potential violation due to willful neglect. Also, the definition of reasonable cause as related to the civil penalties for a violation of the HIPAA Rules is modified and defined as "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated [a provision of the HIPAA Rules] but, in which the covered entity or business associate did not act with willful neglect."

Employers' Bottom Line:

The rules described above are in proposed form and are not yet effective for covered entities or business associates. **However, note that the statutory requirements of the HITECH Act (e.g. application of Security Rule and certain Privacy Rule requirements to business associates, expanded definition of business associate, right to access electronic copies of PHI, etc.), upon which the proposed rule above is based, became effective on February 18, 2010 and compliance is currently required.** If the proposed rule is adopted, it will require certain further changes to HIPAA policies and procedures, business associate agreements and Notices of Privacy Practices. However, there will be at least a 6-month period to ensure compliance with the final rule.

Employers may submit comments on the proposed rules to HHS no later than September 13, 2010. Otherwise, employers should ensure compliance with the HITECH Act, continue to monitor developments in this area and await final regulations.

As further guidance is issued, Ford and Harrison is committed to keeping you abreast of changes impacting your workplace and employee benefits programs. If you have questions regarding the proposed rule or need assistance with HITECH Act compliance, please contact the author of this Legal Alert, Daniel T. Sulton, dsulton@fordharrison.com, any member of the firm's Employee Benefits practice group or the Ford & Harrison attorney with whom you normally work.