

September 9, 2010

U.S. Department of Health and Human Services
Office of Civil Rights
Attention: HITECH Privacy and Security Rule Modifications
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act (RIN: 0991-AB57)

To Whom It May Concern:

Congress established the Office of Advocacy (Advocacy) under Pub. L. 94-305 to represent the views of small business before Federal agencies and Congress. Advocacy is an independent office within the U.S. Small Business Administration (SBA); as such the views expressed by Advocacy do not necessarily reflect the views of the SBA or of the Administration.

Background

The provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) resulted in the Department of Health and Human Services (HHS) promulgating rules (the Privacy Rule, the Security Rule and the Enforcement Rule) designed to prevent inappropriate use and disclosure of individuals' health information and to require organizations which use health information to protect that information and the systems which store, transmit, and process it. The aforementioned HIPAA rules generally apply to three types of "covered entities:" health care providers who conduct covered health care transactions electronically, health plans and health care clearinghouses.

On July 14, 2010, HHS published in the *Federal Register* a proposed rule titled, Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act (HITECH Act).¹ HHS

¹ 75 Fed. Reg. 40868, July 14, 2010.

indicates in the introductory section of this proposed rule that the purpose of the modifications is to implement recent statutory amendments under the HITECH Act, to strengthen the privacy and security protection of health information, and to improve the workability and effectiveness of the HIPAA rules.²

One of the primary aspects of this proposed rule includes extending the applicability of certain of the Privacy and Security Rules' requirements to the "business associates" of covered entities. The HIPAA rules define "business associate" generally to mean a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. Business Associates include: "third party administrators or pharmacy benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information."³

The rule states that business associates of covered entities will be liable for civil and criminal penalties for the failure to comply with these provisions. Business associates of covered entities will be civilly and criminally liable under the Privacy Rule for making uses and disclosures of protected health information that do not comply with the terms of their business associate contracts.⁴ The additional privacy and security requirements of subtitle D of the HITECH Act will be applicable to business associates and the requirements must be incorporated into business associate contracts. Lastly, this proposed rule requires that organizations that provide data transmission of protected health information to a covered entity or business associate and that require routine access to such information are to be treated as a business associate under the HITECH Act and requires them to enter into a business associate contract.

HHS certified that this rule will not have a significant impact on a substantial number of small entities pursuant to the requirements of the Regulatory Flexibility Act (RFA).

HHS' regulatory analysis indicates that for the purposes of this regulation it is treating all health care providers affected by this rule as small entities, because 90 percent or more of the health care providers meet the U.S. Small Business Administration's size standards either by way of their annual receipts or nonprofit status. The rule will also apply to health insurers and third party administrators, but HHS is not in possession of their

² Id.

³ 75 Fed. Reg. at 40872.

⁴ Sections 164.308(b) of the Security Rule and 164.502(e) of the Privacy Rule require a covered entity to enter into a contract or other written agreement or arrangement with its business associates. The purpose of these contracts or other arrangements, generally known as business associate agreements, is to provide some legal protection when protected health information is being handled by another person (a natural person or legal entity) on behalf of a covered entity.

annual receipts and therefore it cannot determine if they are to be deemed small businesses. Despite treating all of the affected health care entities as small for the purposes of this rule, HHS chose to certify that this regulation will not have a significant impact on a substantial number of small businesses under §605 of the RFA.

The RFA requires that if the regulatory agency certifies that the rule will not have a significant impact on a substantial number of small businesses, it must include a statement providing the factual basis supporting the certification. The factual basis supporting HHS' certification can be located in the Regulatory Flexibility Analysis.⁵ The analysis indicates that the proposed rule would have an impact on covered providers of healthcare, health insurance issuers, and third party administrators acting on behalf of health plans, which is estimated to total 701,325 entities. Of the approximately \$166.1 million in costs HHS is able to identify, the private sector will incur approximately 71 percent of the costs, or \$118.1 million. The average cost per covered entity is therefore approximately \$168.⁶

Advocacy is concerned with HHS' computation of the costs of the rule and because certain affected small entities approached Advocacy with their concerns that the business associate provisions of the rule will result in a significant burden on their businesses. These concerns run counter to HHS' certification of no significant impact on the entities covered by this regulation. Advocacy believes that there is merit in bringing these small business concerns to the attention of HHS in the hope that it will add to the transparency of the regulatory flexibility analysis contained in the final rule.

Advocacy Comments on HHS' Economic Analysis

The Office of Advocacy believes that HHS may have failed to identify all of the costs to small entities associated with the rule and in appropriately assessing which covered entities will bear the burdens imposed. HHS calculated the entire cost of the rule as being derived from the costs of 'notifying individuals of their new privacy rights' (for a quantification of the rule's per entity costs see footnote 6). Advocacy believes this approach for assessing per entity costs is inadequate for purposes of a RFA analysis.

Advocacy's guidance for performing a threshold analysis to determine whether an RFA certification is appropriate specifically directs agencies to separately estimate the number of small entities in each industry segment or sector that will be covered and determine the costs to entities in that sector. Advocacy does not believe that HHS correctly followed this procedure in the proposed rule. First, HHS estimates only the new costs of notification, none of which appear to fall on newly covered 'business associates' of health providers and insurers. However, because these entities will have new requirements for monitoring contract performance and ensuring compliance, Advocacy believes they will have costs associated with implementing all of the health information security and privacy protocols, including developing new plans and procedures and implementing the resultant practices, as well as possibly renegotiating contracts. Without

⁵ 75 Fed. Reg. at 40910.

⁶ Id.

this information it is not possible for HHS to determine that there are no significant costs on covered ‘business associates,’ and therefore the factual basis of the certification is insufficient. Advocacy believes that HHS should revisit this issue and adequately estimate compliance costs on covered ‘business associates’ and then make a determination as to whether those costs are significant and whether a certification is still appropriate.

Second, HHS ignores lost revenues of covered entities that currently distribute health information for remuneration. In the discussion of costs related to the various requirements, HHS assumes that covered entities will not incur any costs for any ‘disclosures related to marketing and sale of protected health information’ because if individuals simply refuse to sign disclosures when asked, covered entities will simply stop selling health information.⁷ While this may be true, HHS has a duty to estimate as costs of the rule the revenues that covered entities will lose by modifying their current business practices. HHS’ assumption in this regard will effectively prevent covered entities from selling health information, a practice some currently undertake, and thus the requirements of the proposed rule are the cause of these entities losing this revenue. The RFA directs agencies to include lost revenue as a cost in estimating the impacts of a rule on small entities. Advocacy urges HHS to consider these impacts on small businesses.

Advocacy believes that HHS should estimate all of the above costs and then determine whether the proposed rule has no significant impact on small entities, or whether it would be more appropriate to prepare an Initial Regulatory Flexibility Analysis (IRFA).

Small Entity Concerns with the Rule

The small businesses, including health record storage companies, that approached Advocacy will be considered “business associates” as defined by this proposed rule. They voiced two primary concerns with this rule:

- 1) Because of the increased fines and liabilities included in the HITECH Act, small entities are concerned that covered entities will be allowed to pass on risk by forcing business associates into signing business associate agreements that require indemnification. The businesses acknowledge that HHS has offered an alternative in the Regulatory Flexibility Analysis section of the rule indicating that it will provide sample language for the revision of business associate agreements.⁸ However, the small businesses are concerned, and even HHS indicates, that the sample language may not be sufficient for complex business associate agreements.⁹ The affected small businesses request that HHS clarify in the rule that while business associates have their own risks and responsibilities under the HIPAA-related laws, no law or rule requires business associates to absorb any of the risks and responsibilities that properly belong to covered entities.

⁷ 75 Fed. Reg. at 40907.

⁸ 75 Fed. Reg. at 40910.

⁹ Id.

- 2) Small businesses are also concerned that HHS does not consider common carriers such as the United States Postal Service, United Parcel Service, FedEx, or other courier services to be business associates under HIPAA rules; this is because HHS has determined that these businesses do not “use” or “disclose” protected health information and are performing a function that covered entities are not capable of performing themselves. Small entities assert that in their experience most HIPAA-related breaches involving members of the record storage industry occur during the process of transporting information, not when storing information. Record storage small businesses believe that they should be afforded the same type of exemption that couriers are given, depending on the level of service they offer to covered entities.

Conclusion

Advocacy requests that HHS take Advocacy’s RFA comments and the concerns identified by the affected industry into consideration as the Agency finalizes this rule. Thank you for your attention to the above matter. If you have any questions or concerns, please do not hesitate to contact me or Linwood Rayford at (202) 205-6533, or linwood.rayford@sba.gov.

Sincerely yours,

Winslow Sargeant, Ph.D.
Chief Counsel for Advocacy

Linwood Lee Rayford, III
Assistant Chief Counsel Advocacy

Cc:
Cass R. Sunstein, Administrator, Office of Information and Regulatory Affairs