Records and information management companies need to take steps to comply with the newly adopted HIPAA omnibus rule.

BY LISA J. SOTTO, RYAN P. LOGAN AND MELINDA L. MCLELLAN

preventive MEASURES

On Jan. 17, 2013, the U.S. Department of Health and Human Services (HHS) issued a final omnibus rule that modified prior regulations pertaining to protected health information (PHI) that were enacted pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As HHS Office for Civil Rights Director Leon Rodriguez aptly noted, the omnibus rule, "mark[ed] the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented."

Among the key changes that will come into effect this September is the addition of a provision that dramatically increases the number of organizations directly subject to the HIPAA Privacy, Security, Breach Notification and Enforcement Rules (collectively, the HIPAA Rules). Businesses that act as service providers to health care companies—including many entities in the information management industry—must consider new legal requirements and potential regulatory scrutiny of how they handle and safeguard customer data.

INCREASED FOCUS ON BUSINESS ASSOCIATES

HIPAA applies primarily to so-called "covered entities" (such as hospitals, pharmacies and health insurers). The HIPAA Rules also govern how covered entities interact with third parties that handle PHI in their roles as service providers to the covered entities. These third parties, known as "business associates," represent virtually every industry sector and include companies that perform PHI storage and destruction services for HIPAA-covered entities. The omnibus rule features two changes of particular note to the information management industry: (1) the new definition of a business associate now encompasses records management companies that merely "maintain" records containing PHI (regardless of whether the company actually accesses or reviews those records), and (2) the omnibus rule sets out the framework for business associates to be directly liable for noncompliance with the HIPAA Rules.

From its inception, HIPAA has required covered entities to enter into contracts with their business associates to govern the business associates' HIPAA-related obligations to safeguard the covered entity's PHI. These contracts are known as "business associate agreements" (or BAAs). The HIPAA Rules require that certain terms be included in BAAs. For example, BAAs must:

- Establish how the business associate is permitted or required to use and disclose PHI;
- Not use or further disclose PHI other than as permitted or required by the BAA or by law;
- Use appropriate safeguards to prevent PHI from being used or disclosed other than as permitted by the BAA;
- Comply with the HIPAA Security Rule;
- Report to the covered entity if it learns of any use or disclosure of PHI not provided for by the BAA; and
- Ensure that subcontractors that receive PHI from the business associate agree to the same restrictions and conditions on the PHI as are contained in the BAA.

BAAs also must include a provision that allows the covered entity to terminate the underlying agreement if the business associate violates a material term of the BAA. Most BAAs tend to follow a fairly standard format based on model provisions that were published by HHS in 2006 to provide examples of how covered entities could address the relevant HIPAA Rule requirements. HHS updated these provisions in January 2013 to coincide with the publication of the omnibus rule.

HIPAA requires covered entities to enter into BAAs with their business associates, though not all covered entities adhere to this obligation on a consistent basis. The omnibus rule, however, applies to business associates even in the absence of a BAA. Accordingly, information management companies that serve HIPAA-covered entities must comply with the relevant HIPAA provisions irrespective of the terms in their BAAs or service contracts with customers.

To prepare, records storage and destruction companies should start by reviewing their service agreements with customers they believe are HIPAA-covered entities to verify whether BAA clauses were included (either as an addendum or incorporated into the main agreement). Business associates should analyze the requirements imposed by BAAs that are already in place and assess their current compliance posture with respect to those contractual obligations. In addition, it may be prudent for information management companies to develop a template BAA for use when negotiating future service agreements with covered entity customers.

DIRECT LIABILITY FOR HIPAA COMPLIANCE

Prior to HHS issuing the omnibus rule, business associates were subject to breach of contract claims if they violated a provision of their BAA. Since the enactment of the Health Information Technology for Economic and Clinical Health ("HITECH") Act in 2009, business associates have been directly liable for violations of certain provisions of the HIPAA Rules, though HHS made clear when the HITECH Act was passed that it did not intend to bring enforcement actions against business associates until the regulations implementing the act were finalized. In short, prior to HITECH, business associates only had to concern themselves with the consequences of failing to comply with their customer contract terms, not with the possibility of being the subject of an HHS enforcement action for a HIPAA violation.

Business associates, including records storage, destruction and other information management companies, are now directly subject to enforcement actions for violations of certain sections of the HIPAA Security and Privacy Rules if they provide services to customers that are HIPAA-covered entities. In the preamble to the omnibus rule, HHS specifically notes that "data storage" companies are business associates subject to the rule if they have access to customers' electronic or hard-copy PHI. Thus, document storage companies that maintain PHI on behalf of covered entities are considered business associates subject to the HIPAA Rules regardless of whether the companies actually view the PHI they store. The definition of business associate was officially modified in the omnibus rule to include a person who "creates, receives, *maintains* (emphasis added) or transmits protected health information on behalf of a covered entity."

Given that HHS highlighted the fact that data storage companies are business associates, the customers of such companies will expect compliance with the HIPAA requirements applicable to services involving PHI. To achieve compliance,

information management companies may be required to:

- Draft and implement internal policies and procedures that comply with HIPAA Security Rule requirements and implement specific technical measures such as audit controls to monitor activity in information technology systems;
- Review existing BAAs with covered entity customers to ensure they are complying with all the requirements contained in the BAAs;
- Evaluate the information security practices of all subcontractors (especially third-party vendors that handle electronic media containing PHI), and enter into written agreements with these subcontractors that contain information security requirements substantially similar to the requirements contained in a BAA;
- Review current data management practices and develop policies and procedures to comply with the HIPAA requirement to only use, disclose or request the "minimum necessary" PHI during the provision of services; and
- Develop (or revise) data security incident response plans to incorporate the requirement to conduct a four-factor risk assessment in the event of a potential security breach involving PHI.

The broad scope of the new definition of business associate means that any subcontractor, no matter how far removed from the HIPAA-covered entity or primary business associate, is considered a HIPAA business associate if it handles PHI. It is therefore critical that information management companies maintain an exhaustive inventory of all subcontractors to (1) identify those that create, receive, maintain or transmit their covered entity customers' PHI and (2) ensure that their contracts with those subcontractors contain BAA provisions.

Business associates must comply with the provisions of the omnibus rule by Sept. 23, 2013, with a limited extension with respect to the BAA provisions. BAAs that were validly entered into before Jan. 25, 2013, must be revised to reflect the new BAA content requirements of the omnibus rule by the earlier of (1) the date the BAA is renewed or modified on or after Sept. 23, 2013, or (2) Sept. 22, 2014.

VIOLATIONS AND PENALTIES

Under the omnibus rule, a business associate in the information management industry could be subject to liability for a HIPAA violation in many ways. A violation could occur if a business associate:

- Neglects to enter into an agreement with any subcontractor that creates, receives, maintains or transmits PHI on the business associate's behalf that contains the same restrictions on the use and disclosure of PHI as in the BAA;
- Fails to notify a covered entity customer of a security breach affecting that customer's PHI within 60 days;
- Fails to implement any of the administrative, physical and technical safeguards in the HIPAA Security Rule;
- Uses or discloses a customer's PHI in any manner not permitted by the BAA or the HIPAA Privacy Rule; or
- Fails to follow the "minimum necessary" standard (i.e., not limiting permitted uses or disclosures of, or requests for, PHI to the minimum necessary).

Business associates in the information management industry must familiarize themselves with the HIPAA Security Rule's numerous administrative, physical and technical safeguard requirements.

Administrative safeguards include assessing risks to the electronic PHI an organization maintains and implementing policies and procedures for granting access to electronic PHI.

Physical safeguards include developing procedures for removing PHI from electronic media before reusing the media and tracking the movements of hardware and electronic media that contain PHI.

Technical safeguards include implementing a mechanism to terminate an electronic session after a predetermined time of inactivity and encrypting PHI whenever deemed appropriate.

Monetary penalties for HIPAA violations can be substantial. A company may be fined up to $1.5 million per year for violating a specific HIPAA requirement. In many cases, multiple violations occur simultaneously and continue for several years, resulting in much higher potential dollar amounts. HHS has been increasingly active in the enforcement arena, as have state attorneys general (who also have the power to enforce HIPAA violations).

The omnibus rule will subject a much larger pool of entities to direct HIPAA enforcement beginning in late 2013. Thus, it is likely that the number of HIPAA-related enforcement actions will grow. Business associates such as records storage and destruction firms may be targets of greater scrutiny since their information security practices affect the PHI of multiple HIPAA-covered entities and have the potential to put exponentially more PHI at risk.

TAKE STEPS TO COMPLY

Immediate action is necessary to ensure business associates comply with the HIPAA Rules by September 2013. Firms that serve customers in the health care industry would be well-advised to assess their compliance posture and develop a plan to implement compliance solutions. SDB

Lisa J. Sotto is managing partner of the New York office of Hunton & Williams LLP and head of its global Privacy and Data Security practice. Ryan P. Logan and Melinda L. McLellan are associates on the Hunton & Williams Privacy and Data Security team. More information is available at www.hunton.com/privacy_and_data_security.