How HIPAA Final Rules Affect Health Information Technology Vendors

Lisa W. Clark* and Neville M. Bilimoria†

In addition to healthcare reform, healthcare providers and their vendors now have to grapple with recently promulgated federal rules regarding privacy and security of health information. Key to the future of the healthcare reform efforts is health information technology (HIT), a broad term that is often used in conjunction with electronic health records (EHRs), mobile health (mHealth), telemedicine, health information organizations/health information exchanges (HIOs, also known as HIEs), and other developments that are revolutionizing the healthcare industry.

HIT supports the development of a national information highway to facilitate the transmission of health data for treatment, payment, quality analysis, and a myriad of other uses. HIPAA-covered entities and many of their vendors (e.g., HIO and EHR consultants, data analytic firms, data transmission facilitators, software vendors, device vendors) rely on HIT to accomplish their individual roles in the U.S. healthcare system. Large data companies, small entrepreneurs, and investors are all participating in the growth of HIT. These unsuspecting vendors of the HIT system may unwittingly violate HIPAA if they do not pay close attention to new rules affecting the privacy and security of health information.

While the use of HIT presents efficiency and potential quality improvements in healthcare, it also poses significant risks with respect to the privacy and security of health data. On January 25, 2013, the U.S. Department of Health and Human Services (HHS) announced the final omnibus rule amending HIPAA in accordance with the HITECH Act of 2009 (the "2013 Amendments"). The 2013 Amendments, which were effective on March 26, 2013 (with some exceptions), supplement and modify the HIPAA Privacy, Security, Breach Notification and Enforcement Rules (the "HIPAA Rules"). This article examines the key ways in which the 2013 Amendments impact HIT.

*Partner in the Philadelphia Office of Duane Morris LLP and a member of the Health Law Practice Group; phone: 215-979-1833; e-mail: lwclark@duanemorris.com. †Partner in the Chicago Office of Duane Morris LLP and a member of the Health Law Practice Group; phone: 312-499-6758; e-mail: nmbilimoria@duanemorris.com.

BUSINESS ASSOCIATES NOW INCLUDE HIOS, DATA TRANSMISSION SERVICES, AND OTHERS

The HIPAA Rules expanded the definition of a business associate to include any entity that *creates, receives, maintains, or transmits* protected health information (PHI) on behalf of a covered entity or other business associates. The 2013 Amendments now stipulate that a subcontractor of a business associate that handles PHI provided by the business associate qualifies as a business associate in its own right. Moreover, the revised definition specifically includes HIOs, e-Prescribing gateways, and any other entity that provides data transmission services. Data transmission services are a core building block of the national health information highway.

In HHS' view, a data transmission organization requires access to PHI *on a routine basis* to perform data transmission services. An HIO is a data transmission organization because it transmits data through an enterprise-based network, such as a hospital's internal or community-based network, or on a geographic basis, including a regional HIO. The 2013 Amendments do not define HIOs due to the fact that as the industry develops, HIOs will continue to evolve. However, HHS promises to issue guidance on HIOs in the future. Other data transmission organizations include e-Prescribing gateways that facilitate electronic prescribing, as well as entities that manage the exchange of PHI through a network, including providing record locator services and performing various oversight and governance functions. In addition, a data storage entity that "maintains" PHI qualifies as a business associate, even if it does not routinely access PHI. This is because, according to HHS, the data storage entity (like a paper record storage company) has a "persistent," as opposed to "transient," opportunity to access the PHI.

HHS gives examples of entities that provide data transmission services but do not qualify as business associates (called "conduits") due to the transient nature of their access to PHI. Those entities that provide "mere courier services"—such as Internet service providers (ISPs), broadband suppliers, and telecommunications companies—effectively

act like the U.S. Postal Service in transporting data. These entities do not routinely access PHI except on a *random or infrequent* basis to provide the transportation service, such as to ensure that the data are arriving at their intended destination or in temporary storage, or otherwise as required by law. However, the conduit exception is a narrow one, and it has to be determined on a case-by-case basis.

Finally, as specifically required under the HITECH Act, the definition of a business associate also includes a personal health record (PHR) vendor. A PHR is distinct from an EHR because the individual controls the PHR, whereas the covered entity such as a hospital controls the EHR (with certain rights, such as amendment, provided to the individual). In the preamble, HHS explains that a PHR vendor is a business associate when the hospital or other covered entity offers PHRs for its patients, such as through a patient portal, and the covered entity provides the vendor with access to PHI, such as the patient's laboratory results, to display in the PHR. By contrast, a PHR vendor is not a business associate solely because it maintains an interoperability agreement with a covered entity that governs the exchange of the data. In other words, the PHR vendor is not providing services for or on behalf of a covered entity, such as a hospital, solely because the PHR vendor and the hospital maintain an agreement that specifies, for instance, the technical specifications for exchanging data or that exchanged data will be kept confidential. In this situation, the PHR is independent of the covered entity, even if data are exchanged between them. (Whether the entity that is involved in transmitting or maintaining the data that the hospital receives from the PHR vendor qualifies as a business associate or is a mere conduit would be separately determined under the analysis of when a data transmission service is a business associate, as described above.)

THE SECURITY RULE AND HIT

Because the HIPAA Security Rule applies to all *electronic* PHI (ePHI) that is created, received, maintained, or transmitted by a covered entity, Security Rule compliance has always been key for HIT entities in arrangements with covered entities. Under HITECH and the 2013 Amendments, business associates and their subcontractors are now directly subject to the HIPAA Security Rule. HIT entities that now fall under the definition of a business associate as a data transmission service or a PHR vendor, or that are business associates to business associates, must ensure compliance with the HIPAA Security Rules.

The Security Rule applies a long list of required and addressable administrative, technical, and physical standards that covered entities and now business associates must implement in order to be HIPAA-compliant. These standards include administrative safeguards (comprehensive security policies, training, security incident procedures, etc.), physical safeguards (workstation security, device and media controls, etc.), and technical safeguards (audit controls, transmission security, etc.). Covered entities and business associates are required to enter into agreements that ensure compliance with the Security Rule standards.

The 2013 Amendments did not amend the basic Security Rule standards except, significantly, that the standards now apply directly to business associates and their subcontractors that handle PHI. Thus business associates and their subcontractors that handle PHI, such as a software company providing maintenance services for a business associate that require access to PHI, will now be subject to penalties for violations of the Security Rule, and must enter into agreements that address compliance with the Security Rule standards. HITECH also provided monies for a pilot security audit program, in which HHS conducts Security Rule compliance audits on a random basis. Although the pilot program has ended, the government will continue its security audit activities when, for instance, a breach is investigated.

HIT AND THE BREACH NOTIFICATION RULE

The Breach Notification Rule applies to "unsecured PHI" that has been accessed, acquired, used, or disclosed. Unsecured PHI is data that have not been rendered unusable, unreadable, or indecipherable through a use of a technology or methodology specified by HHS. In 2009 guidance, HHS identified encryption and destruction in accordance with certain standards published by the National Institute of Standards and Technology (NIST) (see www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html). Any breach of PHI that is unsecured must be reported.

Significantly, breach reporting will become even more common because the 2013 Amendments lowered the standard for what constitutes a "breach." A use, disclosure, acquisition, or access that violates the Privacy Rule is presumed to be a breach, unless the covered entity or business associate can demonstrate that there is a "low probability" that the PHI has been compromised based on four factors, including the likelihood of re-identification and the extent to which the risk to the PHI was mitigated. For HIT entities, ensuring that PHI is encrypted and destroyed according to the NIST standards is vital.

"ELECTRONIC MEDIA" DEFINITION EXPANSION

The definition of PHI includes individually identifiable health information that is transmitted by or maintained in "electronic media" or any other form. When the HIPAA Rules were originally drafted, HIT was not yet prevalent. In accordance with current technology, the definition of "electronic media" now includes electronic storage

material on which data are or may be stored electronically, including hard drives and any removable/transportable memory medium such as a memory card. HHS notes that photocopiers, fax machines, and other devices that store, or potentially store, PHI are subject to the HIPAA Rules.

"Electronic media" also includes transmission media used to exchange information already in electronic storage media—such as the Internet, extranet or intranet, leased lines, dial-up lines, and private networks—as well as the physical movement of electronic storage media. However, certain transmissions, such as by faxes, voice, or telephone, are not considered electronic media transmissions if the information did not exist in electronic form "immediately" prior to the transmission. This exclusion covers, for instance, the transmission of a fax that originated from printing from an electronic file.

CHANGES TO THE PRIVACY RULE

While the Security Rule addresses the "locks and keys" that are necessary to protect ePHI, the Privacy Rule describes the confidentiality standards that apply to all PHI—not just electronic PHI. The principal changes in the HITECH rules that concern HIT are found in the Security Rule. However, there are new requirements in the Privacy Rule that impact HIT. Covered entities must provide to individuals a copy of the PHI held in an electronic designated record set (e.g., an EHR). Covered entities must also ensure that their HIT systems are able to address the other new Privacy Rules: restricting PHI regarding an item or service provided to a health plan upon request by an individual, and new restrictions on the use of PHI for marketing, fundraising, and sale purposes. Finally, not only does a business associate have to support the covered entity in meeting these requirements, but a business associate is also directly subject to HIPAA penalties in its own right for violations of these new Privacy Rule standards.

HHS has promised further guidance in some areas under the Privacy Rule, such as marketing. In addition, HHS has not yet issued a final Accounting Rule regarding the HITECH Act's requirement that covered entities and business associates provide an accounting of all disclosures for the prior three-year period. (The proposed Accounting Rule was issued on May 31, 2011.) The anticipated Accounting Rule may be delayed because of the burdens that would be imposed on covered entities and business associates whose designated record sets are not yet digitized. As HIT becomes more widespread, especially with the focus on mHealth, the duties on covered entities and business associates under HIPAA will increasingly focus on their uses of technology to deliver healthcare.