What Is a Business Associate?

“Information technology and business are becoming inextricably interwoven. I don’t think anybody can talk meaningfully about one without talking about the other.”
—Bill Gates, Founder, Microsoft

Changes to the Business Associate Relationship as a Result of the HITECH Act and the Omnibus Rule

Stated somewhat simplistically, a business associate is a person or entity that performs a service for or on behalf of a covered entity other than the provision of health care. The recent Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule expressly expanded the definition of a business associate, which includes the subcontractor liability of the business associate (discussed later). The liability of covered entities and business associates for breaches of protected health information (PHI) was expanded under the Omnibus Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH Act).
In the HITECH Act, Congress effectively made HIPAA business associates—persons or entities that provide a service for or on behalf of a covered entity other than the provision of health care—into covered entities, thereby expanding government regulation of health care to transcription services, copy services, billing services, medical marketing services, and the like. Note that nowhere in HIPAA or its implementing regulations is there a mention of foreign entities other than in authorizing certain disclosures to, among others, a foreign government agency that is acting in collaboration with a public health agency. Certainly, neither the definition of a business associate nor the exemptions therefrom exempt foreign entities from qualifying as business associates.

Before the HITECH Act, business associates had only to agree by contract—the business associate agreement is a contract—to implement reasonable and appropriate security measures to protect the security and privacy of PHI and to use and disclose PHI only as authorized by the agreement. The execution of certain ministerial duties was also agreed to by contract. Now, however, business associates must comply with the Security and Privacy Rules, be subject to audit by the Office of the Inspector General (OIG) of the Department of Health and Human Services (DHHS), and be subject to other HIPAA requirements. So now, under the HITECH Act, business associates are effectively, if not legally, covered entities. Even if that statement seems too broad, business associates clearly face the same civil and criminal liability as do covered entities and have to do most things that covered entities must do. For example, now a business associate maintaining or transmitting individually identifiable health information under a business associate contract will have to conduct a risk analysis, have a destruction plan, train staff on HIPAA, and the like. How a business associate or subcontractor is defined is crucial. For example, the standards promulgated by the International Organization for Standardization, known as ISO standards (i.e., ISO/IEC 17799), are international information...
security standards, which define a business associate in relation to federal HIPAA. In Texas, a business associate and a subcontractor are actually considered a “covered entity” according to the Texas Medical Record Privacy Act (H.B. 300). Section 181(b)(2) defines a covered entity as

any person who: (A) for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site; (B) comes into possession of protected health information; (C) obtains or stores protected health information under this chapter; or (D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information.

Unlike the federal definitions, which parse out covered entity, business associate, and subcontractor, Texas includes all three under the designation of “covered entity.” This distinction can become important if both federal HIPAA and state HIPAA are implicated in an international scenario because of what law may apply.

As will be discussed more fully later, the Omnibus Rule amplified this direct federal regulation of business associates by expanding the definition of business associates to include subcontractors and by providing for the liability of covered entities for the breaches of their business associates under the federal common law of agency.
Typical Overseas Business Associate and Subcontractor Services

Foreign business associates could include those who provide cloud computing, including hosting and backup of electronic health records, transcription services, billing services, data aggregation, and the sale and maintenance of electronic health records. These offshore services may be more responsive and cost-effective than domestic business associate services. For example, anecdotally from the authors’ clients, foreign transcription services may be more efficient and less expensive than domestic ones. One covered entity, for example, reported that its Indian transcription service was more responsive and more accurate than its previous domestic one because the Indian service used the same transcriptionist for each doctor over the long term so that the transcriptionist became very familiar with the doctor’s dictation and could transcribe it very quickly and accurately.

In 2012, the Ponemon Institute conducted a study, 2011 Cost of Data Breach Study: India. The relevant laws dealing with data protection are the Information Technology Act (2000) and the Indian Contract Act, 1872. The Ponemon report addressed root causes of breach and the cost and trends in compromised records, among other items. The total cost per capita, in Indian rupees, averaged 2,105. The organizational cost was much higher at 53,500 Indian rupees. The three top causes of attack were “system glitch [45%], negligence [35%] and malicious or criminal attack [20%].” Of the different types of attacks, the most costly type of breach was that caused by a criminal attack, most of which are inside jobs. And, although the companies were not identified, the data breaches reported ranged between 3,198 records and 98,514 records.

With services expanding overseas, including metadata collections, medical record analysis, and data center storage, it is imperative to appreciate the risks in a given country, as well as the laws and any
arrangements between the United States and the respective country. These factors should be considered when deciding whether or not to utilize a foreign business associate.

Advantages and Disadvantages of Foreign Business Associates

Multiple factors go into hiring a foreign business associate or subcontractor. Cost (usually the biggest factor), convenience, and technology advances are all considerations. Some of the advantages are lower costs, time zone differences, and tax rates. Some of the disadvantages are lower technology security standards, language barriers, and exposure to additional laws. Many business associates provide their services for covered entities in the United States. An unlikely scenario for a covered entity is to hire a shredding service from India to shred its paper records or to hire a British law firm to represent it, unless, in the latter case, the British firm has an office near the covered entity, which is part of a U.S. corporation located in London with lawyers licensed to practice in that jurisdiction.

But many other services do not depend on the physical proximity of the business associate. One example is a patient wearing a pacemaker and transmitting data to the medical device company, which has been designated as a business associate. Another example is utilizing a major cloud computing provider and discovering that the data is actually held in data centers across the globe. These are two common scenarios where data becomes more susceptible to attack and companies have heightened liability. Little difference exists between using Iron Mountain, headquartered in Boston, or Sify Storage in India to back up PHI in the cloud, other than, as will be discussed later, the legal issues inherent in having a business associate relationship with a foreign company.
Requirements for Business Associate Contracts

Stated somewhat simplistically, before the HITECH Act, covered entities were liable only for the breach of one of their business associates if they had actual knowledge of the breach and did not take any action to remediate it.23 Under the Omnibus Rule implementing the HITECH Act, however, covered entities will now be liable for breaches by business associates under the federal common law of agency.24 Such liability may include civil money penalties or the new federal lawsuit authorized by the HITECH Act.25

Under the HITECH Act, the “snitch provision” of the HIPAA Privacy Rule applies equally to a business associate and to a covered entity. Consequently, both the covered entity and the business associate have an affirmative duty to take reasonable steps to cure a breach or other violation. Notably, the actions or inactions of one group, including subcontractors, may adversely affect another group.

Recent actions by the Minnesota attorney general highlight the notion that covered entities are not the only group that needs to comply with the provisions set forth in HIPAA and the HITECH Act. Here, the attorney general alleged that Accretive Health, Inc., violated both laws as a business associate for exposing the PHI of more than 25,000 patients from two Minnesota hospitals with whom it had business associate agreements. The crux of the claim focused on Accretive’s failure to comply with the regulations in relation to implementing and maintaining appropriate administrative technical and physical safeguards, such as encryption, for PHI after agreeing with two covered entities that “it would not use or disclose protected health information in violation of HIPAA or HITECH and that it would use ‘appropriate safeguards’ to prevent the misuse or disclosure of protected health information.”

Another illustrative example is CVS Caremark Corp.’s 2009 violation of the Federal Trade Commission Act in relation to technical violations for failing to provide reasonable and adequate security measures for PHI after disseminating a privacy and confidentiality statement that consumers relied upon. The Federal Trade