According to *Webster’s Dictionary*, “vulnerability” is defined as either “(1) the quality or state of having little resistance to some outside agent; or (2) the state of being left without shelter or protection against something harmful.” The world today is a global marketplace. Technology expands the reach and jurisdiction of goods and services beyond a single country’s borders within seconds. With that expansion comes increased legal, technical, and security vulnerability. Commerce is at risk, and, in turn, so are health care services by covered entities and the related services of business associates and their subcontractors.

In 1996, Congress established the Health Insurance Portability and Accountability Act (HIPAA)\(^1\) followed by the Privacy Rule and Security Rule, which were promulgated by the United States Department of Health and Human Services (DHHS) in 2002 and 2003 respectively. Nearly 13 years after HIPAA became law, the Health Information Technology for Economic and Clinical Health Act (HITECH Act)\(^2\) was enacted and subsequent interim rules and the 2013 Final Omnibus Rule\(^3\) followed.

Many U.S. covered entities and business associates use foreign entities to perform services for them involving individually identifiable health information. Such entities, whether foreign or domestic, are considered business associates of the covered entities that perform services on their behalf. Those companies or individuals (persons) that contract with business associates are referred to as subcontractors. The definitions of each category follow:
• Covered entity—health care providers who transmit any health information electronically in connection with certain transactions, health plans, and health clearinghouses.4

• Business associate—a person who “creates, receives, maintains, or transmits” (emphasis added) protected health information.5

• Subcontractor—a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate. This definition applies to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate agreement.6

Initially, express liability applied only to covered entities, while it was implied for business associates and subcontractors. The July 14, 2010, Proposed Rules7 and the final Omnibus Rule expressly extended liability to business associates and their subcontractors.

Since business is global and the creation, receipt, transmission, and maintenance of data are international, why wouldn’t liability be? It is. For example, HCA has hospitals in London, England; the University of Pittsburgh (UPMC) has transplant and cancer treatment facilities in Chianciano Terme, Italy; and the Cleveland Clinic has a partnership with i360, an Irish company, as part of its Innovation Alliance. According to an article in Becker’s Hospital Review, the “U.S. healthcare IT outsourcing market is expected to grow by 42.8 percent in the next five years, according to a report by MarketsandMarkets.”8 And, clinical services, especially “anesthesia, emergency department staffing, dialysis services, diagnostic imaging and hospitalist staffing” are also being outsourced.9

While outsourcing, joint ventures, and joint facilities span the globe, certain countries are particularly attractive for these activities. They include the United Arab Emirates, Japan, the Philippines, India, Australia, Canada, Mexico, and the United Kingdom and other European countries. First, Mexico and Canada border the United States. Second, India is one of the top emerging markets with a lot of growth potential. And, nearly all countries are aware of the brand
recognition of entities such as the Cleveland Clinic, as well as innovations and the focus on emerging markets.

It is not uncommon for certain physician functions to be outsourced to other countries—for example, having a radiologist in India interpret CT scans or X-rays. Legal considerations aside (and there are many), entities contracting with physicians in India should familiarize themselves with the Government of India’s Electronic Health Record Standards for India (Aug. 2013). Considered a “living document,” its ultimate goal is standardization. What is more interesting is the recognition of the set of diagnosis codes utilized by providers in claims processing, ICD10-CM (International Statistical Classification of Diseases and Related Health Problems (ICD)—10th Revision). ICD10-PCS is unique to America, so it is not surprising that it is not referenced in India’s law.

This excerpt provides a great deal of food for thought:

[O]rganizations may use the same information model, but use different vocabularies or code sets (for example, Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®) or ICD10-CM within those information models. To achieve interoperability at this level, standardizing vocabularies, or mapping between different vocabularies (using tools like Unified Medical Language System (UMLS)) may be necessary.

While this relates to communications in India, a lot can be applied to the United States in terms of reimbursement. First, consider the reference to different vocabularies. It is important for physicians and coders to be on the same page in terms of understanding what a particular condition means. For example, there is a significant difference between “disease” and “disorder”; failing to appreciate the difference can lead to an incorrect code, an increased cash gap, and delayed reimbursement.

Second, whether it is ICD-9 or ICD-10, make sure that the mapping and language are in sync between the provider and the insurance company. The insurance company can be a government entity
(e.g., CMS) or a private insurance company (e.g., Humana). Third, mapping codes are utilized in comparing ICD-9 to ICD-10. When appropriate, continue to utilize and prepare for the new ICD-10 implementation date of Oct. 1, 2015.

In sum, the same problems that can arise when having medical records reviewed abroad can arise in the United States. Just as it is important to ensure that the vocabulary and coding systems map appropriately when outsourcing, it is equally important to make sure that the same measures are taken when conducting business domestically. Doing so can allow a more consistent revenue stream.¹⁰

Some of the aforementioned countries are considered mature markets or safe countries. Others, such as India, fall into the BRICS category (Brazil, Russia, India, China, and South Africa) of countries that are considered high risk. This book will primarily focus on the United States, the United Kingdom, and India to provide a multifaceted comparison in terms of laws, contractual considerations, and liability. By choosing these three countries, we can compare a mature, western market and an emerging BRICS market to the United States.

From contracts to choice of law to breaches, execution and violations occur in a variety of countries. This book will provide a basic overview of some of the issues associated with international health care data transactions. Some of the topics addressed include the civil and criminal enforcement of HIPAA, choice-of-law provisions, jurisdictional issues, and conflict-of-law issues—to name just a few.

We hope you enjoy this book and use it as a starting point for strategic thinking and risk mitigation.