HIPAA Considerations for Intermediaries in Medical Tourism

By: Purvi B. Maniar, Partner, Epstein Becker & Green P.C.

Among the questions regarding legal matters often raised by organizations in the United States which are involved in facilitating travel abroad by U.S. patients for medical care are to what extent are they governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and what are their obligations under HIPAA with respect to patient privacy. This article is intended to examine the implications of HIPAA for “intermediaries” or “matchmakers,” in medical tourism, i.e. companies (in the United States) which facilitate overseas medical tourism in certain commonly used medical tourism arrangements.

By way of brief overview, HIPAA is a United States federal statute that includes various provisions intended to protect the privacy and security of personal health information of individuals. HIPAA privacy standards govern the use and disclosure of “protected health information” by “covered entities”. “Protected health information” (commonly referred to by its acronym “PHI”) generally refers to information created or received by a health care provider, health plan, employer, or health care clearinghouse which relates to the past, present or future physical or mental health or condition of or provision of health care to an individual or the past, present or future payment for the provision of healthcare to an individual, and that identifies (or provides the means to identify) the individual. “Covered Entities” are healthcare providers (e.g. physicians, hospitals), health plans (e.g., health insurance and managed care companies and employer sponsored benefit plans), and health care clearinghouses (e.g. WebMD, intermediaries between providers and payors which translate data into required formats). HIPAA security rules are applicable to covered entities which transmit, create or receive PHI in electronic form and these rules require reasonable physical, technical and administrative safeguards to protect the security of PHI. This article is intended to focus on the patient privacy implications of HIPAA, and therefore a full discussion of the application of the HIPAA security rules is beyond the scope of this article.

As a general matter, HIPAA does not directly require compliance by intermediaries which facilitate overseas medical tourism because these companies do not generally fall within the definition of “covered entities”. (However, as discussed below, these companies may be indirectly required to comply with the HIPAA privacy standards if they become “business associates” of covered entities.) Thus, in the scenario where an individual patient in the United States elects to travel abroad to receive medical care by arranging for such care either directly with an overseas hospital or through an intermediary that facilitates such travel, the intermediary arranging for the treatment would not be liable under HIPAA with respect to use or disclosure of medical information of the patient. Of course, the overseas hospital providing the care or the intermediary may still be held liable if violation of any applicable privacy laws of the local
country where the treatment was provided were to occur. (It is also unclear whether the overseas hospital would have liability under HIPAA and the answer may depend on the level and type of involvement it has in seeking patients in the United States.) The intermediary or the overseas provider may also be held liable if they violate any agreement which they entered into with the patient, or any policy to which they have adopted that the patient relied upon, governing the use and disclosure of the medical information of the patient.

As medical tourism is becoming more widely accepted in the United States, an increasing number of health plans, e.g. managed care companies and employer sponsored benefit plans are becoming interested in offering medical tourism as an option to their enrollees in an effort to manage costs while providing quality medical care. For a medical tourism intermediary, contracting with such health plans to provide medical care or to facilitate medical tourism by their enrollees represents a significant opportunity to attract patients in volumes rather than on an individual basis. However, because a health plan in the United States is a covered entity, it is not, in many instances, allowed to disclose protected health information to third parties unless the third party enters into an agreement to become a “business associate” of the health plan. As a “business associate”, the intermediary is required to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by its contract with the health plan, report to the health plan any use or disclosure of the information not provided for by its contract of which it becomes aware, and ensure that any subcontractor to whom it provides PHI agrees to the same restrictions and conditions that apply to the business associate with respect to such information. As a business associate, the intermediary will also be required to satisfy individual rights requirements as to access, amendment and accounting on behalf of the health plan, make internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services and return or destroy all PHI at the termination of the agreement.

Covered entities may be subject to civil and criminal penalties as well as imprisonment for violations of HIPAA. The penalties may consist of fines of up to $50,000 and, if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm, fines of up to $250,000. While HIPAA does not provide for direct liability of business associates to the government or to individual patients, the business associate agreement with the covered entity will often require the business associate to indemnify the covered entity for damage incurred by the covered entity arising out of violations by the business associate. Thus, the intermediary may be contractually liable to reimburse the health plan for penalties that the health plan may incur arising out of privacy violations by the intermediary.

For intermediaries in medical tourism, a successful, scaleable business model usually presumes contracts with managed care plans or self-insured employers who can refer a steady stream of patients who can take advantage of medical tourism. Such a relationship will inevitably require the intermediary to become a business associate of the health plan. To the extent that the intermediary can demonstrate that it is already compliant with applicable industry privacy and security standards by having effective policies, procedures and monitoring mechanisms in place, this will go a long way in reassuring the health plan that it is entering into a relationship with the right partner. Such measures could include retaining a designated HIPAA officer for implementation and oversight, which is not specifically required by HIPAA, but is one of the industry best practices.

As a final caveat, the intermediary should bear in mind that while HIPAA preempted all state privacy laws which were less stringent than HIPAA, to the extent a state’s privacy laws are more
stringent, they remain in effect and are applicable in addition to the requirements of HIPAA. Therefore, whether or not the intermediary is a business associate of a covered entity under HIPAA, it should also verify whether any state laws would be applicable in the state in which it is located and in which the patients that it facilitates reside.

If you have any questions or comments about this article or on this topic, please feel free to contact Purvi B. Maniar by email at pmani@ebglaw.com.

This publication is provided for general information purposes; it is not and should not be used as a substitute for legal advice.