Health-Tech

FOX ROTHSCHILD LLP

Elizabeth G. Litten

Fox Rothschild LLP
ATTORNEYS AT LAW

IsraelDesks
by NÍSHLÍS LEGAL MARKETING SETTING THE BENCHMARK

HIPAA Quirks: Tips for Israeli Companies Doing Business in the United States

If you are not sure whether the Health Insurance Portability and Accountability Act of 1996, as amended, and implementing regulations (collectively, "HIPAA") applies when you do business in the United States, you are not alone.

HIPAA, the most comprehensive U.S. privacy and data security law applicable to individually identifiable health information, has been around for more than 20 years, yet confusion about HIPAA persists. In short, if your company creates, receives, maintains, or transmits individually identifiable health information on behalf of a "health care provider", "health plan", or "health care clearinghouse" located in the United States ("covered entities" as defined under HIPAA), it is likely acting as a "business associate" and will be required to sign a business associate agreement ("BAA") and comply with HIPAA. A BAA and HIPAA compliance is also required if your company provides services to a business associate, and those services involve the use or disclosure of individually identifiable health information.

In short, if your company creates, receives, maintains, or transmits individually identifiable health information on behalf of a "health care provider", "health plan", or "health care clearinghouse" located in the United States, it is likely acting as a "business associate" and will be required to sign a business associate agreement and comply with HIPAA.

Determining if HIPAA applies can be tricky though, and a company looking to do business with a covered entity (or one of its business associates) should exercise caution when presented with a BAA. This list of HIPAA quirks may help you determine whether you need to sign a BAA with a U.S.-based customer and highlight a few tricky (but frequently included) BAA provisions to watch for.

Quirk #1: Application Developers: HIPAA only applies if the developer creates, receives, maintains, or transmits protected health information (or "PHI", another term defined under HIPAA that generally means individually identifiable health information created, received, maintained, or transmitted by a covered entity) on behalf of a covered entity or another business associate. However, if a consumer downloads an app offered by her health plan (a covered entity) that is also available as a separate direct-to-consumer version, HIPAA does not apply to the direct-to-consumer version as long as information from this version is kept separate and is not "part of the product offering" to the health plan.

Quirk #2: Mere Conduits: HIPAA does not apply to telecommunications companies or other entities that act as a "mere conduit" of PHI, meaning they only access PHI on a "random or infrequent basis" and do not have access to PHI "on a routine basis". By way of example, a telecommunications company that has access to PHI while it is temporarily stored incident to the transmission service is not a business associate subject to HIPAA, but if it maintains PHI for a longer period on behalf of a covered entity or another business associate, it is (even if it never actually views the PHI). The difference is the "transient versus persistent nature" of the opportunity to view PHI.

Quirk #3: De-Identification of PHI. Business associate agreements often include language permitting (or prohibiting) the business associate from de-identifying PHI it creates, receives, maintains, or transmits on behalf of the covered entity. PHI is considered "de-identified" under HIPAA when 18 specific identifiers have been removed, or a qualified person has applied "statistical and scientific principles and methods" to render the PHI un-identifiable and documented the methods and results of the analysis. However, even if the business associate agreement permits de-identification by the business associate, the agreement cannot allow the business associate to do anything otherwise prohibited under HIPAA. HIPAA permits covered entities and business associates to "use" PHI for specific purposes set forth in the regulations (such as "treatment", "payment", and "health care operations" purposes, all terms defined under HIPAA). If de-identification is not for an expressly HIPAA-permitted purpose (and is not expressly permitted under the business associate agreement), de-identification by a business associate is likely prohibited by HIPAA.

Quirk #4: Reporting of Security Incidents. A BAA must include a provision requiring the business associate to report "security incidents" to the covered entity. HIPAA defines "security incident" broadly, including as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." A BAA may include language designed to avoid repeated reporting of pings or firewall attacks that are unsuccessful, but if it lacks this language and requires reporting of every security incident, the failure to report could be construed by the covered entity as a breach of the BAA.

Quirk #5: Reporting of Breaches. HIPAA also requires business associates to report any acquisition, access, use, or disclosure not permitted under HIPAA (a "breach") to the covered entity no later than 60 days following discovery. The BAA often requires reporting to the covered entity within a much shorter timeframe (for example, within 24 hours after discovery), but this short reporting period can backfire on the covered entity. The clock starts ticking for the covered entity's notification obligations (for example, 60 days for notice to affected individuals and for notice to the U.S. Department of Health and Human Services ("HHS") when 500 or more individuals are affected) as soon as it receives notice of the breach from the business associate.

Quirk #6: Ransomware Attacks. If a ransomware or malware attack results in the inability to access PHI, it is presumed to be a breach. As per HHS guidance, even if the data appears not to have been viewed or taken, if there is a "high risk of unavailability of the data", the attack may be deemed to be a breach requiring notification.

As the minefields of privacy laws both in the United States and abroad continue to expand, navigating the peculiarities of HIPAA to ensure compliance can pose challenges for non-U.S.-based companies. Be sure to consult with legal counsel to help you determine whether and how HIPAA may impact your business operations and agreements.

Fox Rothschild LLP

Elizabeth G. Litten, Partner and HIPAA Privacy & Security Officer

Fox Rothschild LLP is a national law firm of 800 attorneys in 21 offices throughout the Unites States that delivers strategic and practical solutions. Our Israel Practice Group consists of experienced attorneys who understand the nuances and concerns of Israeli culture in business. We are well positioned to assist Israel-based companies in the full range of local and international issues. We counsel Israeli companies in navigating complex immigration laws and provide advice on all matters of U.S. law, including corporate, tax, intellectual property, employment and real estate. We have deep experience in national and cross-national litigation and arbitration matters, as well as insolvency and bankruptcy. Our team works closely with clients to develop initial business plans and structure Israel-related business transactions, including expansion into the U.S. market. We offer cost-effective solutions that help our clients meet and exceed their goals while minimizing legal fees.

Elizabeth G. Litten is a partner and co-chair of the Privacy and Data Security Practice at Fox Rothschild LLP. A leader within the firm, Elizabeth serves as the HIPAA Privacy & Security Officer, co-chair of the Government Relations Practice and as a member of the firm's Executive Committee. In her practice, she counsels national and regional regulated entities on a range of data privacy issues and serves as counsel to health care related entities including hospital systems, health care facilities, regulated and self-funded health plans, and health care technology companies. Elizabeth uses her sophisticated understanding of the law to advise health care providers, regulated health plans and self-funded employer plans on the evolving technologies and new models of health care delivery and payment, including direct employer plan-provider contracting and implementation of Accountable Care Organization models. A frequent speaker on health law and technology topics, Elizabeth is a regular contributor to the HIPAA & Health Information Technology Blog, which provides information regarding cutting-edge legal and practical developments that health care providers and businesses must consider in the handling and sharing of health information, including through the use of electronic health records.

CONTACT INFORMATION:

www.foxrothschild.com
office: +1 609 896 3600
elitten@foxrothschild.com