Articles + Publications | June 28, 2023

Storm Clouds Form Offshore Under Updated Florida Electronic Health Records Exchange Act

WRITTEN BY

James Koenig | Erin S. Whaley | Brent T. Hoard | Emma E. Trivax

Background

On July 1, an amendment to the Florida Electronic Health Records Exchange Act (the Act)[1] will go into effect. The Act focuses on information safety and sets forth stringent requirements that prohibit health care providers from storing patient information in offshore Electronic Health Record (EHR) and related technology.

HIPAA Versus the Act

The Act acknowledges that the standards set forth by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) already exist for information security, however, it seeks to implement its own policies to protect patient information entrusted to health care providers. For instance, the definition for "health care provider" is very broad and mirrors the HIPAA definition, which effectively includes any type of provider, such as anyone licensed by an agency, providers' clinical and nonclinical staff, pharmacies, home health aides, continuing care facilities, and more.[2] However, on other items, such as utilizing EHR technology, the Act is far more limiting.

Qualified EHR Patient Information Restricted to US, Its Territories, and Canada

According to the Act, any "health care provider that utilizes certified [EHR] technology must ensure that all patient information stored in an offsite physical or virtual environment, including through a third-party or subcontracted computing facility or an entity providing cloud computing services[3], is physically maintained in the continental United States, its territories, or Canada." The Act makes clear that the scope of this offshore prohibition "applies to all qualified electronic health records that are stored using any technology that can allow information to be electronically retrieved, accessed, or transmitted." This expands the scope of the storage restriction beyond just a provider's certified EHR technology to any system it uses to store qualified electronic health records, which are defined as "an electronic record of health-related information concerning an individual which includes patient demographic and clinical health information, such as medical history and problem lists, and which has the capacity to provide clinical decision support, to support physician order entry, to capture and query information relevant to health care quality, and to exchange electronic health information with, and integrate such information from, other sources."[4]

Due to some ambiguity in drafting, whether offshore *access* is also prohibited has been a matter of some debate. While time will tell, the intent of the reference to access (along with retrieval and transmission) seems better suited to expanding the scope of technologies covered by the Act (*i.e.,* any technologies that can access, retrieve, or

transmit such patient information, not just EHR platforms) as opposed to a prohibition on offshore access.

Novel Annual Certifications of Compliance With the Act and Prohibition of Business Relationships With Foreign Countries of Concern for Licensees

Another meaningful change to Florida law is that any licensee[5] must sign an affidavit upon their initial license application or renewal license application that they are compliant with this new offshore prohibition. This is concerning because this places the onus on the health care provider to understand every aspect of the EHR vendor with which it contracts. The licensee must also ensure that no person or entity that holds a controlling interest in the licensee[6] holds an interest[7] in an entity that has a business relationship with a foreign country of concern.[8] Because this requirement is fast-approaching, Florida licensees must immediately determine if any controlling person or entity holds an interest in a foreign country of concern: The People's Republic of China; The Russian Federation; The Islamic Republic of Iran; The Democratic People's Republic of Korea; The Republic of Cuba; The Venezuelan regime of Nicolás Maduro; and The Syrian Arab Republic.[9]

Five Key Steps That Should Be Taken Prior to July 1, 2023

1. **Determine If the Act Applies to Your Data.** This change means that Florida-based health care providers must begin investigating whether their contracted EHR and other technology vendors that store qualified electronic health records have an offsite storage environment, either virtually or physically, that is hosted outside of the continental United States, its territories, or Canada.

2. **Develop Contractual Safeguards for All Arrangements Restricting Data Subject to the Act to US and Canada.** If their vendors do utilize offshore storage, the health care providers will need to enter into agreements, or amend their existing agreements, with such vendors that would limit any storage of patient information to the permitted countries.

3. **Assess Existing Arrangements.** Additionally, any EHR or other qualified electronic health records technology vendor that works with Florida-based health care providers and stores patient data must also re-evaluate their offshore storage arrangements to ensure that they can maintain their business relationship with those health care providers impacted by the Act (*i.e.*, make sure their storage is limited to the U.S., its territories, and Canada).

4. **Review Ownership of Licensee.** Florida licensees must determine whether any controlling person or entity of the licensee holds an interest in a foreign country of concern.

5. **Develop Annual Compliance Assessment and Certification/Recertification Process.** Most importantly, Florida licensees should develop initial and annual compliance assessments and recertification processes to ensure that all aspects of the Act are being met.

As always, Troutman Pepper's Privacy + Cyber and Health Science practices stand ready to assist with global privacy/security and health compliance, including developing and conducting applicability analysis and compliance assessments under the Act (and HIPAA), as needed.

Please contact Jim Koenig, Erin S. Whaley, Brent T. Hoard, and Emma E. Trivax or any member of our Privacy + Cyber and Health Sciences practices with questions.

---

[1] Fla. Stat. 408.051 et seq.

[2] Fla. Stat. 408.051(2)(d).

[3] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.,* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. *Special Publication 800-145*, National Institute of Standards and Technology, 2011.

[4] Fla. Stat. 408.051(2)(b).

[5] A “licensee” means an individual, corporation, partnership, firm, association, governmental entity, or other entity that is issued a permit, registration, certificate, or license by the agency. Fla. Stat. 408.803(9).

[6] Controlling interest” means the applicant or licensee; a person or entity that serves as an officer of, is on the board of directors of, or has a 5% or greater ownership interest in the applicant or licensee; or a person or entity that serves as an officer of, is on the board of directors of, or has a 5% or greater ownership interest in the management company or other entity, related or unrelated, with which the applicant or licensee contracts to manage the provider. The term does not include a voluntary board member. Fla. Stat. 408.803(7).

[7] “Interest” in an entity means any direct or indirect investment in or loan to the entity valued at 5% or more of the entity’s net worth or any form of direct or indirect control exerting similar or greater influence on the governance of the entity. Fla. Stat. 286.101(1).

[8] “Foreign country of concern” means The People’s Republic of China; The Russian Federation; The Islamic Republic of Iran; The Democratic People’s Republic of Korea; The Republic of Cuba; The Venezuelan regime of Nicolás Maduro; The Syrian Arab Republic; any agency of, or any other entity under the significant control of one of the above-listed foreign countries of concern. Fla. Stat. 692.201.

[9] *Id*.

RELATED INDUSTRIES + PRACTICES

- Health Care + Life Sciences
- Privacy + Cyber