Published on *The National Law Review* https://natlawreview.com

Florida Electronic Health Records Exchange Act Amended – Health Records Maintained by Qualifying Health Care Providers Must Be Stored in the U.S., U.S. Territories, and Canada Only

Article By:

Julia B. Jacobson

John E. Wyand

Kimberly J. Donovan

Gicel Tomimbang

On May 8, 2023, Governor Ron DeSantis of Florida signed CS/CS/SB 264, amending a suite of Florida statutes to impose heightened requirements on business activities involving foreign interests. As related to the health care industry, CS/CS/SB 264 amended the Florida Electronic Health Records Exchange Act (Act) to, among other things, require "health care providers" that utilize "certified health record technology" to manage health records in an electronic interoperable and digital format to ensure that in addition to maintaining such records in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA), the health records must be stored only in environments physically maintained in the U.S., its territories or Canada, effective July 1, 2023. CS/CS/SB 264 also amended Florida licensure requirements for qualifying health care providers, obligating licensees to comply with the amended requirements of the Act, particularly as related to the security and storage of personal medical information outside of U.S. and Canadian jurisdictions, in order to obtain and maintain a license in Florida.

Key Takeaways and Recommendations

- Qualifying health care providers must comply with both HIPAA and Florida state requirements for transfers of health care data. Although HIPAA does not impose specific requirements regarding where health data must be stored, the amendments to the Act require qualifying health care providers in Florida to only store health records in the U.S., its territories, or Canada. As such, effective July 1, 2023, qualifying health care providers in Florida have heightened health data record storage obligations.

- Qualifying health care providers must submit a signed affidavit attesting under penalty of

perjury that the provider is in compliance with the health records storage requirements of the Act when they submit their initial and renewal license application. Non-compliant qualifying health care providers may be subject to disciplinary action by the Agency for Health Care Administration, the Florida state agency that regulates health care licenses in Florida.

- The applicability of the Act does not depend on where the patient who is the data subject resides, but on whether the entity is a qualifying health care provider under Florida law. The Act applies to HIPAA covered entities and business associates that are also qualifying health care providers in Florida under the Act. It also applies to traditionally non-HIPAA covered entities and business associates, such as acupuncturists. Therefore, the requirements of the Act apply to a broader group of entities that collect health data than HIPAA.

- The Act does not directly impose obligations on parties that are not qualifying health care providers under Florida law, such as third-party vendors that provide cloud computing services and other health technology vendors, but effectively prohibits offshoring of data in health records. To comply with these obligations, qualifying health care providers will most likely contractually flow down the requirement to store health records only in the U.S. and Canada to their third-party vendors via business associate agreements and data processing agreements.

- Recent enforcement and regulatory trends suggest the Act is likely the first of many legal and regulatory restrictions that will apply to transfers of sensitive data (e.g., health data) to foreign jurisdictions. Therefore, third-party vendors providing cloud computing services and other health technologies to qualifying health care providers should be prepared to offer its customers U.S.- or Canada-based data processing, maintenance, and storage options to accommodate legal and regulatory developments.

HIPAA and the Act. The most prominent law applicable to the processing and maintenance of health data is HIPAA, which only applies to qualifying covered entities and business associates and sets forth data privacy and security requirements for safeguarding health data that is "protected health information" (PHI). Covered entities and business associates comprise only a fraction of the universe of entities that process and maintain health data. Likewise, PHI is only a fraction of the universe of health data collected from individuals. HIPAA does not restrict processing and maintenance of PHI to the U.S. and does not enumerate geographic restrictions on data, provided covered entities and their business associates have appropriate agreements, including business associate agreements, and HIPAA-required data privacy and security safeguards in place. Further, HIPAA does not preempt stricter, non-conflicting state laws, meaning that states may opt to implement stricter requirements to protect their constituents.

Here, Florida amended the Act to impose more specific requirements regarding the storage of "health records." The Act broadly defines "health record" as any information recorded in any form or medium, which relates to the past, present, or future health of an individual for the primary purpose of providing health care and health-related services. The Act does not define "health care" or "health-related services," and the broad definition of "health record" presumably includes data within a health record that qualifies as PHI. As such, the Act imposes enhanced data processing and maintenance requirements on health care providers in Florida.

Applicability. The Act applies to qualifying "health care providers" that use "certified electronic health record technology" (i.e., qualified electronic health information technology that meet the health

information technology certification criteria set forth by the Office of the National Coordinator for Health Information Technology). "Health care providers" include, among others, Florida-licensed providers regulated by the Agency for Health Care Administration such as, for example, hospitals, health care clinics, ambulatory surgical centers, nursing homes, assisted living facilities, residential treatment facilities, and hospices. It also includes "health care practitioners" (e.g., Florida-licensed physicians, acupuncturists, chiropractors, midwives, etc.); speech-language pathologists and audiologists; nursing homes and related health care facilities; certain mental health facilities and their clinical and nonclinical staff who provide inpatient and outpatient services; continuing care facilities; and Florida-licensed pharmacists. The list of qualifying health care providers in the Act include HIPAA covered entities (e.g., hospitals, health care clinics, and physicians), business associates (e.g., nursing homes and assisted living facilities), and non-HIPAA entities (e.g., acupuncturists). Therefore, the Act applies to more entities than HIPAA.

As described above, the Act does not define the scope of provision of health care or health-related services, and therefore, what constitutes such services could be interpreted broadly. Further, although the Act defines the bounds of "health record," it does not define "patient," suggesting that the Act would apply to all health records processed and maintained by qualifying health care providers, regardless of where the individual patient resides. Therefore, the assessment of the Act's application depends on the whether an entity is a qualifying health care provider, and not on the residence of the patient who is the data subject.

Licensing Requirements for Qualifying Health Care Providers. Qualifying health care providers must submit an affidavit attesting under penalty of perjury that the provider is in compliance with the Act's requirements to store health records only in U.S. and Canadian jurisdictions at the time they apply for and each time they renew their license. Non-compliant qualifying health care providers may be subject to disciplinary action by the Agency for Health Care Administration. This means that licensees should ensure that their vendors, particularly technology vendors that process data on their behalf, comply with the storage requirements of the Act.

Third-Party Vendors. Although the amended Act defines "certified electronic health record technology"[1] and "cloud computing",[2] it does not directly impose requirements on third-party vendors, such as providers of electronic health records software and cloud computing services. However, most health care providers rely on third-party vendors for electronic health records and technology management. The Act requires qualifying health care providers to store health records only in environments physically located in the U.S., its territories, and Canada. Therefore, in effect, the Act obligates qualifying health care providers to require its third-party vendors to store health records only in environments physically located in the covered jurisdictions, effectively prohibiting offshoring of such data. These requirements will most likely be reflected in the qualifying health care providers' contractual agreements with their service providers, such as business associate agreements and data processing agreements, meaning that qualifying health care providers will soon begin requiring more specific data storage commitments from its third-party vendors. Further, recent enforcement trends (see for example, U.S. v. Easy Healthcare) suggest heightened enforcement and regulatory scrutiny of transfers of sensitive data (e.g., health data) to foreign jurisdictions. Accordingly, third-party vendors, particularly those that provide data storage services to qualifying health care providers, should be prepared to offer U.S.- or Canada-based data processing, maintenance, and storage options to accommodate legal and regulatory developments.

Please reach out to the authors or your Squire Patton Boggs relationship attorney if you have any questions or would like further information on this and other topics.

[1] The Act defines “certified electronic health record technology” to mean a qualified electronic health record certified pursuant to Public Health Service Act § 3001(c)(5), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

[2] The Act defines “cloud computing” to mean the same as the definition provided by the National Institute of Standards and Technology (“NIST”). NIST Special Publication 800-145 defines “cloud computing” as “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 . . . composed of five essential characteristics, three service models, and four deployment models.” See NIST SP 800-145 at Section 2 (The NIST Definition of Cloud Computing), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

National Law Review, Volume XIII, Number 171