New Florida Law Gets Serious About Offsite Storage of Patient Information

On May 8, 2023, Florida Gov. Ron DeSantis signed new restrictions into law for health care providers that utilize resources outside the U.S. While the majority of the new law affects the real estate industry in Florida, it also includes key updates to the Florida Electronic Health Records Exchange Act relating to the maintenance of patient information outside the U.S. and Canada (the Offsite Restrictions) and, in so doing, has the potential to impact various actors in the Florida health care industry. For health care providers and vendors, it is important to understand the Offsite Restrictions to achieve compliance before July 1, 2023.

What Do the Offsite Restrictions Prohibit?

As stated above, SB 264 includes an amendment to the Florida Electronic Health Records Exchange Act that tracks the general concern of the legislation — keeping Florida residents protected from foreign entities.

However, if you are one of the specifically listed "health care providers," the Offsite Restrictions will prohibit you from physically maintaining patient information in any location other than the continental U.S. and its territories or Canada. The Offsite Restrictions are intended to apply to both the physical and virtual storage of patient information, including maintenance through a third-party or subcontracted computing facility or cloud-based vendor.

The Offsite Restrictions specifically focus on health care providers that utilize "certified electronic health record technology" (CEHRT) to maintain patient information. Because CEHRT is federally defined and certified under the guidance of the United States Department of Health and Human Services, the application of the Offsite Restrictions should be fairly straightforward from a technology standpoint. However, the new law concludes by providing that the Offsite Restrictions apply to all "qualified electronic health records," which is a broader term not limited to CEHRT and therefore raises the possibility that the Offsite Restrictions could be interpreted to apply to electronic health record technology beyond CEHRT.

To track compliance with the new law, providers will be required to attest under penalty of perjury that they are complying and intend to remain in compliance with the Offsite Restrictions when submitting an initial or renewal application for a license from the Florida Agency for Health Care Administration (AHCA). The law also provides that failure to comply with the Offsite Restrictions could result in AHCA disciplinary action.

Will the Offsite Restrictions Apply to Health Care Vendors?

As noted above, the new law specifically identifies the governed parties as health care providers that utilize CEHRT to store patient information offsite in a physical or virtual environment. However, this application includes offsite storage using "a third-party or subcontracted computing facility or an entity providing cloud computing services." Given the breadth of this definition, health care vendors providing or otherwise utilizing offsite storage may be required to certify compliance with the Offsite Restrictions via contract to ensure that their provider partners can certify compliance under Florida law.

Next Steps

Health care providers and their third-party vendors should read the Offsite Restrictions as affecting all health care professionals. As such, health care providers likely will require that any third party who manages their patient information offsite affirm that the physical location of such information is either in the U.S. or Canada.

From a vendor's standpoint, the first step should be to check where the patient information handled by the organization is physically maintained. If the information is maintained outside of the U.S. or Canada, the vendor should transition any noncompliant information to an appropriate U.S. or Canada-based location. By being proactive, a health care vendor can ensure they maintain existing business relationships with health care providers racing to beat the law's effective date.

However, ensuring compliance may prove tricky if a health care provider or its vendors use the cloud. Because cloud-based services function by using individual servers at data centers and server farms around the world, it may be difficult to confirm compliance with the Offsite Restrictions. Covered parties should reach out to their cloud-based providers as soon as possible to ensure that patient information is not physically stored outside of the U.S. or Canada. If the cloud provider cannot ensure that all patient information is stored in a U.S. or Canada-based location, the parties must be prepared to quickly pivot to a cloud provider that can offer a compliant storage location.

Moving forward, health care providers will likely want to negotiate commitments in their vendor agreements that patient information is stored in a manner that is compliant with the Offsite Restrictions, which will likely result in many vendors having to closely examine both the structure of their internal storage facilities and also their cloud-based storage arrangements.

Finally, it is important that health care providers and vendors continue to check for updates from the AHCA on how the Offsite Restrictions will be enforced and reach out to legal professionals to understand how and to whom the law applies once the July 1 effective date passes.

The Chambliss Health Care team will continue to monitor these developments. Please contact Doug Griswold, Mark Cunningham, or your relationship attorney if you have questions or need additional information.