Optometry Practice Sues EMR Vendor for Crash of EMR System and Total Loss of Patient Records

A recent New Jersey court case emphasizes the need for every health care provider using an electronic medical record (EMR) system to ensure, through independent due diligence, that the EMR system is fully HIPAA compliant and secure, including redundant backup, notwithstanding any contractual or other representations made by the EMR vendor. In Quality Eye Associates, LLC v. ECL Group, LLC et al., Civil No. 22-2489 (D.N.J. July 25, 2022), an optometry medical practice sued its EMR vendor after the software system crashed and the group "lost the vast majority of the EMR data from 2013 onwards." The EMR system contained patient records as well as billing and financial information.

Background

The practice and EMR vendor were parties to an agreement for the EMR software and other services provided by the vendor, under which the vendor "represented that the program was regulation compliant in that it was ensured to save, retain, and store Plaintiff's data and that Defendants were continuously updating the program to ensure it remained that way." The plaintiff optometry practice alleged in the lawsuit that, despite the defendant vendor's representations that the EMR software program was regulatory compliant and the information was therefore secure, the vendor knew this was not the case and "knew their (sic) programming was inadequate from February 2013 until the December 2020 server crash."

Motion to Dismiss

Before the court was the defendant EMR vendor's motion to dismiss all of the plaintiff's claims of breach of contract, negligence, and common law fraud and consumer fraud. The court ruled in favor of the defendant on the negligence and fraud claims, but ruled in favor of the plaintiff on the breach of contract claim. Therefore, the case is now proceeding on that claim.

Takeaways

Although the case is not yet concluded, it highlights the importance of fully implementing the requirements of the HIPAA Security Rule, which governs the security of electronic protected health information (ePHI). In addition to the court case, the parties likely will undergo scrutiny by the applicable professional licensing board(s), the U.S. Department of Health & Human Services, Office for Civil Rights (OCR, the HIPAA enforcement agency), and/or one or more state attorneys general. HIPAA and applicable licensing rules require health care providers to securely maintain electronic medical records, including by taking precautions to prevent corruption or loss of such data, performing periodic risk assessments to identify threats and vulnerabilities to ePHI and the systems that house it, and taking actions to address identified threats and vulnerabilities.

Other takeaways include:

- Loss of patient record and billing data can have a crippling effect on a health care provider, including disruption to ongoing patient care, disruption to business operations, and financial losses.
- EMR software contracts are typically highly-technical and lengthy; consideration should be given to consulting with legal counsel, including to review:

o The health care provider's rights with respect to the software, including management and disposition of the data therein upon termination or expiration of the agreement—how and when is the EMR data transferred to the health care provider, does the contract require that the data be provided in readable and usable format, and does the agreement make it clear that the provider owns the data?

o Does the contract clearly set forth the vendor's obligations with respect to HIPAA compliance, security, backup redundancy, software updates, and related matters?

o Does the contract permit the vendor to de-identify patient data and commercialize such de-identified data for its own benefit? If so, has the provider's legal counsel opined that such actions are HIPAA-compliant and legally permissible?

o Does the contract permit the vendor to subcontract any of its duties and obligations, and if so, has legal counsel reviewed the same?

o Does the contract permit any health care data to be maintained by the vendor outside the United States? Will this violate Medicare rules or other applicable law? What additional risks are created by permitting the data to be maintained in this way?

o Does a HIPAA business associate agreement accompany the vendor contract?

o Does the agreement require the vendor to maintain cyber/data breach insurance?

o Does the agreement require the vendor to indemnify the provider for cyber/data breaches?

o Is venue and jurisdiction for disputes and governing law in the state where the provider is located? Who pays legal fees?

- HIPAA Security Rule compliance requires more than written policies and procedures—full implementation of the requirements of the rule requires continuous and ongoing oversight and action.
- Breach or loss of ePHI implicates multiple laws and multiple governmental agencies—providers may face scrutiny and penalties from professional licensing boards, the federal OCR, and state attorneys general, among others. If affected patients reside in multiple states, scrutiny—and penalties—can extend across those states.

For more information or for assistance with your HIPAA compliance program, contact:

Lani M. Dornfeld, CHPC (Certified in Healthcare Privacy Compliance), Member, Healthcare Law, at 973-403-3136 or ldornfeld@bracheichler.com