MINTZ

“Access Denied” – Understand How Your Electronic Health Records Are Controlled

September 25, 2014 | Blog |

VIEWPOINT TOPICS

- Health Care

RELATED PRACTICES

RELATED INDUSTRIES

Written by: **Rachel Irving Pitts**

Earlier this week, my colleague **Dianne Bourque** commented on a small medical practice’s inability to access its patients’ medical records one July day after its EHR vendor blocked the practice from pulling the data stored in the EHR. In the **Boston Globe article**, the EHR vendor compared the situation to an electric company turning off the power after months of nonpayment. As technology advances, we abandon “outdated” ways of doing things - our cordless phones won’t work when our power is shut off, and a doctor who has switched to an EHR can’t grab the paper chart off the stacks when its EHR shuts down. A main purpose of the push for providers to adopt EHR is to streamline patient care – a doctor at the hospital doesn’t have to wait for the primary care provider’s chart with the relevant medical history to be delivered or faxed, but just uploads the relevant data set with the patient’s history so they can diagnose and treat the patient. But that all goes out the window if your EHR goes dark, and you can’t get to the records.

Mintz Levin isn't involved in the case discussed in the Boston Globe, but we routinely advise on EHR and business associate relationship issues. Our best advice for providers looking to avoid a situation like the one covered in the article is to focus on HIPAA privacy and security rule compliance and “meaningful-use” requirements when contracting with an EHR vendor, but not lose sight of other practical aspects of the relationship. Your EHR vendor relationship should not rule your patient relationship.

A few things to consider in your contracts:

- Be sure your EHR vendor agreements specify who owns the data and make sure that a data “black-out” is not a remedy the vendor can use if there is a contract dispute.
- Remember that data backup is a HIPAA compliance requirement. Covered entities must maintain retrievable, exact copies of ePHI, so inability to provide care following data “black-out” may reveal HIPAA compliance failures.
- Specify that the data must be returned to the provider if the agreement is terminated by either party for any reason. Providers have medical record retention obligations under state law whether or not their EHR vendor is still in business.
- Clearly delineate each party’s obligations in your agreements – who, what, when, and how.

These are just a few of many issues you will need to consider when negotiating and entering into EHR vendor contracts. The small practice in Maine provides a cautionary tale and a reason to review your existing agreements to see if they need more clarity. A common mantra of health care reform (including the push for EHRs) is the **triple aim**: improved patient experience, improved population health, and reduced per capita costs. But a break-down in the new and improved system doesn’t advance any of these aims. At the end of the day, patient safety is paramount to all of the parties – and where technology has its limits, the parties should understand in advance where the data will be.

Authors