Boston Business Journal

On the record

August 24, 2012

Opportunities and challenges abound as the health care sector finds new and innovative uses for patient-level data

Stephen Bernstein of McDermott Will & Emery said patientlevel data is generally kept under tight wraps.

The advent of patientprivacy regulations and new technologies intended to boost efficiency and record keeping among care givers has created huge opportunities — and potential liabilities — for the nation's health care system. Specifically, the passage of the Health Insurance Portability and Accountability Act of 1996 and its evolving requirements relative to the storage and protection of patient-level data have increasingly competitive advantage for hospitals, physicians groups, pharmacies and insurers who are adopting new and cutting edge tools to collect and analyze electronic medical records. Stephen W. Bernstein, who specializes in health care technology as global head of McDermott Will & Emery's Health Industry Advisory Practice Group, recently spoke with the Boston Business Journal about changes ahead in laws affecting how businesses handle patient data.

Let's start with the 1996 Health Insurance Portability and Accountability Act, or HIPAA. What is it?

HIPAA applies to five entities: health care providers, health plans, health care clearing houses, Medicare Part D providers, and business associates.

Why should businesses be paying attention to it now?

HIPAA provides a laundry list of situations where data can be moved — for payment, treatment, health care operations — without patient consent. Other situations involve important compliance considerations. An important statutory amendment called HITECH broadened HIPAA to cover business associates - any organization that is receiving protected patient health information and doing something on behalf of one of the four covered entities. So if a billing company is doing something on behalf of a health care provider, they're a business associate. We're waiting for regulations to be fi nalized.

What do businesses have to do?

Businesses serving the health care industry need to make sure they have written information-security plans in place, employees trained, and have a sense of what is happening with the data

they are holding. The big changes are for organizations not based in Massachusetts but working for companies here – they need to get up to speed with Massachusetts' privacy laws, which are stronger than HIPAA. They're liable for breaches if they don't handle data in a secure way.

How do you define privacy?

Privacy can fit into any of three categories: how data comes in, how it's used and how it goes back out.

What's the idea behind the push for medical record digitization in the president's Affordable Care Act and state cost-control law?

The idea is to improve access and improve quality while simultaneously reducing costs. The simplest way to reduce cost is to eliminate duplication. If a patient goes to one provider and then a specialist, there's no reason to order the same test. Health information technology can eliminate the need for that. The other component is measuring quality according to outcomes and to pay for results, and not because a test was administered. If hospitalizations can be avoided, that's a type of positive quality outcome.

Should patients be worried their data will be compromised?

It's important for patients to understand that their data is not floating loosely around the Internet. Their data typically moves in secure environments. It's available to clinicians who have a need to have it. Clinicians are being trained to handle it properly. There are situations where it goes astray, but at least where it goes astray, it's often trackable, whereas if someone picks up a paper record, you may have no idea it's missing.

It's becoming increasingly common for data to be accessed within a secure server as compared with data being sent outside of the system. Similarly, patients now have greater electronic access to their health records. Both PartnersHealth and Beth Israel Deaconess have special sites where patients can securely access portions of their records electronically.

What about doctors working at home with data?

Working remotely actually gives me much less pause than traveling with the data in your hands. Secure environments where clinicians "come to" the data remotely are safer than situations where the data is moving outside of a secure environment – particularly with paper records.