New Jersey Law Journal

VOL. CXCVIII - NO.3 - INDEX 227 OCTOBER 19, 2009 ESTABLISHED 1878

COMMENTARY

Electronic Health Records And the End of Anonymity

By Grayson Barber

The American Recovery and Reinvestment Act, better known as the federal stimulus package, dedicates $19 billion to the development of electronic health records, and $0 to the protection of individual privacy.

Privacy and security regulations in the HIPAA essentially stopped providing meaningful privacy protection in 2002. When that statute was enacted in 1996, your health-care provider had to get your permission before disclosing your medical information to business associates and others.

Under the Bush administration, however, the federal Department of Health and Human Services changed the rules, and your authorization is no longer required. Health-care providers are free to disclose your health information for treatment, payment or "health-care operations." Those privacy statements you sign are not consent forms; they're reservations of rights.

The last vestiges of privacy in the form of "practical obscurity" will disappear as the paper records in your doctor's office are converted to digital form. This may be a good thing, depending on how you look at it. Every doctor you visit will be able to get a record of every treatment you ever received, quickly and efficiently. If you are treated for a sexually transmitted disease, mental illness, or even hemorrhoids, your ability to "isolate" different kinds of medical care will be gone. For example, you may not feel it's necessary for your dermatologist to know you take lithium for depression, but the choice will not be yours.

Microsoft, one of America's most successful corporations, is angling to get some of that stimulus money by developing different kinds of databases to house the new digital health records. Individual patients like you and me might prefer to purchase its "HealthVault" in which to store our own X-rays and charts. But once you disclose your digital record, the data can be replicated endlessly, so you don't really have control over those records. It may be more sensible therefore to entrust the records to a big provider like a regional health information organization. Even then, you'll want to know your records are being protected from hackers, or mislaid in a laptop.

With the latest security measures, every big database still has a dark side: It becomes a surveillance system. Electronic health records, stored together, will provide law enforcement with a convenient opportunity to monitor your prescription drug use. As hospitals can identify undocumented immigrants, they will similarly be able to identify citizens with outstanding warrants.

This means, obviously, we need to put some parameters around the use of electronic health records. We can decide to use them for improving the quality of medical care, for measuring error rates in hospitals and for infectious disease detection systems. We can use them to market pharmaceuticals and deny insurance coverage. We can identify patients who abuse prescription painkillers, and teenagers who take birth control pills. Matching them against law enforcement records, we could intercept, at the hospital door, parents who are behind in their child support payments.

When people lose a sense of trust, when they don't feel their medical records are private, they try to protect themselves. They ask doctors to change diagnoses, to "dysthymia," say, lest they should be tainted by "depression." They pay out of pocket to hide medical tests, lest their insurers re-disclose their information to their business partners. Many avoid medical help altogether, lest they receive a diagnosis that carries a stigma, like HIV or addiction. This torpedoes the benefit of using digital medical records for public health statistics, because it skews the data.

Moreover, computer scientists have shown that anonymous data can be re-identified easily. A few years ago, AOL released thousands of records from which "personal identifiers" had been removed. The *New York Times* carried a front-page story shortly thereafter, with intimate details about the people to whom the data belonged. In fact, 87 percent of Americans can be uniquely identified, using date of birth, gender and ZIP code.

The stimulus plan for electronic health records does provide much bet-

Barber, a solo in Princeton, concentrates on privacy matters.

ter privacy protections than HIPAA. It prohibits the unauthorized sale of medical records, limits marketing and mandates data encryption. Best of all, it contains breach notification provisions: if there is a data spill, you will find out if your medical records have been inadvertently disclosed.

Unfortunately, for you there is no remedy.

New Jersey should recognize a private right of action for individuals who are harmed when their health records are improperly disclosed. We should also make it a crime to re-identify medical records or de-anonymize them. The loophole for marketing should be closed to make it clear that Microsoft is not a "business partner" with our health-care providers.

In short, we must protect our digital records from re-disclosure. Computers cannot do this without the force of law. ■