A service of the California HealthCare Foundation

iHealthBeat
Reporting Technology's Impact on Health Care

Tuesday, October 14, 2008

PHR Privacy Questions Get Tougher When Criminal Justice System Involved

by Dennis Melamed

The Kabuki we see in the transition to electronic health records obscures two obvious and fundamental issues:

- The nature of the confidentiality privilege for electronic records maintained by patients instead of doctors; and
- The right to avoid self-incrimination when medical records contain information that might result in criminal prosecutions.

Both issues deal with the legal rights patients have in their medical records. To be clear, this is not the same as the patient rights granted under HIPAA or the types of private sector commitments to not abusing use of medical records. We seem to have a grasp on these finer points.

Instead, there seems to be little enthusiasm for dealing with the more mundane non-health related issues that arise when patient data meets the court system and the criminal code. These more concrete and practical issues are the real posers.

Privilege To Be Served (With a Subpoena)

Let's start with the "simpler" issue. In June, the Markle Foundation announced that many of the industry's heavy hitters and consumer groups had reached an agreement on a code of patient rights and behavior in regard to personal health records as part of its Connecting forHealth initiative. It's important to remember that these records are maintained by the patient.

This common framework -- from a patient confidentiality perspective -- focused on how the private sector had agreed to be on the side of the angels in managing patients' information.

Don't misunderstand me. That's a good thing and everyone in that initiative deserves to be applauded.

However, no one seems to have considered the legal ramifications of having a patient maintain his or her own records when lawsuits or criminal proceedings occur. When asked, the heavy hitters in the Connecting for Health initiative said they had not considered it. They were focused on the private sector and non-judicial aspects of EHRs.

The default assumption seems to be to leave it up to judges to decide what to do.

This is a grave oversight when we consider the hundreds of thousands of court cases in which lawyers seek information from the opposing side and are limited in their ability to fish for information.

All states recognize, in one fashion or another, a physician-patient privilege when it comes to medical information.

But what happens when the patient holds a separate set of records? What confidentiality right can a patient claim when an insurer or an employer or soon-to-be ex-spouse seeks records from the patient directly? There is no doctor to claim privilege.

In a paper-based world, the individual can simply deny having the records or destroy them.

In a world where the information is stored electronically, no such easy answer exists. The consumer's PHR contractor has the information. And even if a health care organization is the one maintaining the PHR, where is the doctor-patient relationship implied?

While patients' PHRs might not be official, they will certainly be of use to those seeking official records. If they are not official, we still cannot assume they are inaccurate. If we do that, then we have to wonder about the value of the PHRs in the first place -- at least a little bit. In any case, the "official" status is of little consequence because the PHRs are likely to contain useful information for legal purposes of discovery.

This is no trifling matter. Since the HIPAA Privacy Rule went into effect in 2003, many state courts have addressed the legality of attempts by defense attorneys to informally speak with plaintiffs' doctors in a large number of malpractice and child custody cases.

These so-called "ex parte" communications are not prohibited by HIPAA. However, some states, such as Tennessee, have banned them entirely, concluding that the convenience for the legal system does not outweigh a patient's right to confidentiality.

Other states allow such information communications, but only with patient authorization.

These state actions only address medical records held by doctors and thus have some form of confidentiality privilege to overcome.

PHRs Not So Lucky

If it hasn't happened already, it won't be long before attorneys go for the PHRs and avoid the hassles and complications of going through doctors. When that happens, we all can be sure to hear patients wonder what happened to patient privacy.

Congress has not addressed this issue. But then again, no one else has either.

An easy starting point might be a federal law that grants PHRs with the same patient privilege that exists in the states in which the patient receives treatment.

Of course, the law being the law, it might not be so simple because some states have constitutional rights to privacy; others have the privilege established by case law; and still others base the patient privilege on contract law. That discussion is for another day -- except for one point.

Because patients' rights to confidentiality are based on different premises, it is reasonable to assume that judges will take different routes in making decisions on PHRs. And we can be sure that not all PHR roads will necessarily lead to patient confidentiality.

The differences among the states raise the second issue that is studiously ignored in the discussion over EHRs.

The Right to Self-Incrimination

We've paid a lot of attention to the complexities surrounding laws focused on privacy and data security. The creation of the Health Information Security and Privacy Collaboration to iron out inconsistencies among the states over privacy and security is a testament to those challenges.

The efforts have largely focused on conventional privacy laws, such as HIPAA and states' versions of medical privacy laws.

That focus is too narrow. The state and federal legal requirements to report health data are numerous and varied. Significantly, many laws involve criminal activities, not civil violations.

I can already hear the response to this line of reasoning: Health care providers are safe in sharing patient data with other doctors for treatment and billing.

That's true. It's also not the only consideration.

One of the more immediate and foreseeable problems deals with issues surrounding the age of sexual

consent and the sharing of reproductive information.

For the past 16 months or so, I've asked people much smarter than me about the following scenario:

- Parents have a 16-year-old daughter and live in a state like New Jersey where the age of consent is 16.
- For whatever reason, the daughter has visited Planned Parenthood and received some prescriptions for contraceptives.
- Later in the year, the daughter visits an uncle in Virginia where the age of consent is 18.
- She is involved in an accident in Virginia, and the emergency physicians on the scene want her records from New Jersey.
- When the Virginia physicians see the records, they notice the contraception prescriptions.
- Because the age of consent in Virginia is 18, does the Virginia physician assume that child abuse has occurred because the contraceptives suggest sexual activity? Are they then required to report it to Virginia criminal law enforcement authorities?
- Does that mean that the parents who rush to visit their daughter are arrested for child abuse or negligent care once they step foot in Virginia?

So far, all of the people smarter than me have only pregnant pauses to offer.

This example is not as hypothetical as it may seem. In September 2006, the Indiana Medicaid fraud agency unsuccessfully sought the patient records of Planned Parenthood of Indiana in an investigation claiming that the organization failed to report child sexual abuse. In that case, the child abuse was defined as a minor having sex before age 14.

In 2003, the Kansas attorney general issued an opinion that any sexual intercourse with a minor was sexual abuse as a matter of law regardless of whether it was consensual or with a peer. It was challenged in court.

State and federal laws may force doctors to violate the physician-patient privilege. We are likely to run into analogous problems in other areas wherever there is no uniform federal law, such as domestic violence and substance abuse to name but two.

What can we deduce from these gaping holes in our approach to EHRs?

We already know that privacy laws are piecemeal. We aren't going to do anything about that. But we have failed to realize that many other laws that interact with the health care system are also piecemeal.

We are only asking for trouble when we pretend a multi-trillion dollar industry operates in a self-contained legal and societal environment.

So at the end of the day, we can continue to make the transition into EHRs in a vacuum and risk being sucked into a vortex of unintended -- but easily anticipated -- lawsuits in other areas.

Or we can start a practical discussion of how EHRs will interact with other laws outside the narrow confines of medical confidentiality.

Patients will take little comfort in knowing that their medical records stewards did not sell their data to marketers when they their rights in court have been compromised.

Readers are invited to send feedback to: **ihb@chcf.org**