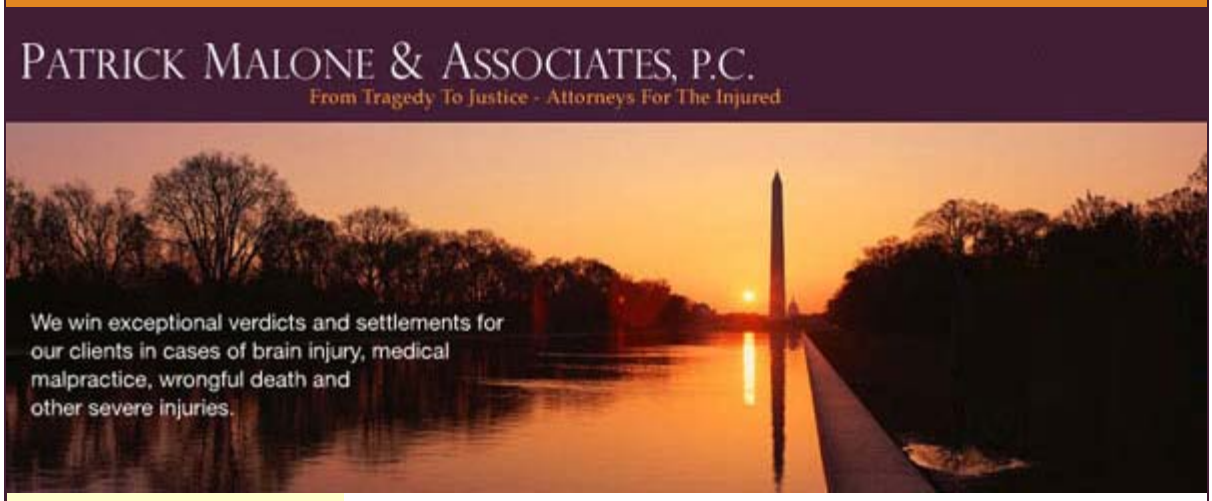
Getting the Best Medical Care: a Newsletter from Patrick Malone



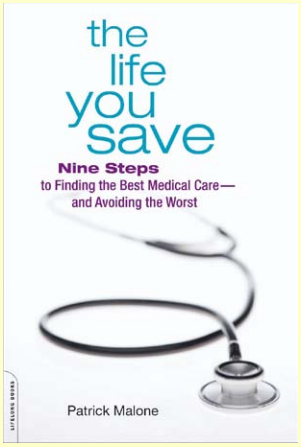
In This Issue

Quick Links

Our firm's website

Read an excerpt from Patrick Malone's book:

The Life You Save: Nine Steps to Finding the Best Medical Care -- and Avoiding the Worst



Secure Health Records: A Matter of Privacy *and* Safety

As our medical and insurance records increasingly are stored online by companies that lack adequate security, our lives are vulnerable to prying eyes whose attentions we don't welcome.

Health care organizations are attractive targets because they maintain tons of information easily sold on the black market and because their security measures aren't up to the standards of other industries.

Health outfits have gotten a wake-up call in recent months, thanks to data breaches of an estimated 80 million customers of health insurer Anthem and of 11 million Premera members.

The concerns are about privacy protection and ID theft. -- and even the safety of your own health care. This month, we examine the developing state of digital medical records, and what to do if yours have fallen, or might fall, into the wrong hands.

What's at Risk

To a hacker, health data is more valuable than credit card information. Health information has a life-long shelf life. Health care files often contain not only patient names, addresses, phone numbers and medical information ranging from the ordinary to the sensitive, but also dates of birth, Social Security numbers, bank account information and anything else the provider or underwriter has collected over the relationship.

You can change your bank account and credit card numbers fairly easily, but not your Social Security number.

Stolen data leads to stolen IDs, and the establishment, for example, of fraudulent lines of credit and medical insurance fraud. If your medical insurance information is used to obtain care for someone else, it not only messes with your credit rating, but your health profile, which poses a risk to your physical, not just financial, health.

Learn More

Read our Patient Safety Blog, which has news and practical advice from the frontlines of medicine for how to become a smarter, healthier patient.

Join our Mailing List

And, according to a recent story in the Washington Post, that kind of crime often isn't caught as quickly as financial fraud. What if you end up in an emergency room, unconscious, and the hospital has access to what seems to be your medical history that actually is someone else pretending to be you?

What if information about your medical condition goes viral? What if a potential employer, suitor, your mother, finds out online that you have or had a mental disorder or venereal disease?

Even a broken leg is no one else's business if you don't want it to be (although it's more difficult to hide if you're limping around on crutches), but some things are inherently more private, and once they're made public on the Internet, you can never hide them again.

Even if you think privacy is a quaint idea in the age of the Internet, it's critical to a productive doctor-patient relationship. Getting the best medical care depends on trust and honesty, so if you're hiding information to protect your privacy, you're not allowing practitioners to give you the best care.

Who's Peeking Into Your File?

The Washington Post reported that since 2009, data for more than 120 million people has been compromised in more than 1,100 separate breaches at organizations handling protected health data.

"That's a third of the U.S. population -- this really should be a wake-up call," Dr. Deborah Peel, executive director of Patient Privacy Rights (PPR), told The Post.

Often, as in the case of Anthem and Premera, such breaches aren't discovered or disclosed until weeks or months after they occur.

Hackers seldom turn their data ore into gold quickly -- usually they sell the data they've collected; they themselves don't assume the IDs of the people they've ripped off. But sometimes your credit rating can be ruined before you're even aware of it.

Large-scale hacking isn't always responsible for breaches of medical data. Often, private information is compromised when someone employed by a health-care organization is careless with a laptop or the disposal of paperwork. But, as The Post pointed out, "hacking-related incidents disclosed this year have dramatically driven up the number of people exposed by breaches in this sector."

Providers and health insurers must abide by the Health Insurance Portability and Accountability Act (HIPAA). It's a federal law that protects the privacy and security of patient records, and is largely the reason you must sign release-of-information forms whenever you see the doctor. No one may review your records if you don't give permission. Of course, you can't receive care or insurance coverage if you don't allow these providers to see your information.

With the increasing specialization of medical care and referrals to other practitioners, hospitals and labs, a lot of parties are legitimately entitled to see your records. The more cooks in the soup, the more likely it is that one of them isn't paying careful enough attention; the

more likely it is that some outfit hasn't updated its technology.

Quality Control Is Lacking

When medical data breaches are discovered, the federal Office for Civil Rights investigates. It's a division of the Department of Health and Human Services that reviews thousands of complaints every year with a staff of only a couple hundred people.

The investigative news organization ProPublica.org recently interviewed its director, Jocelyn Samuels, who said in regard to the Anthem/Premera situations that they illustrate "... both the increasing risks that exist in the cybersecurity space and the need for covered entities [anyone subject to HIPAA's requirements] to continue to update and evaluate their risk analyses to ensure that their risk management plans adequately anticipate all of the kinds of threats they may face."

Technology has changed so much since HIPAA was passed that it's difficult for public and commercial interests to stay current. But that's their job. Samuels claimed that application of HIPAA has expanded with the growth of electronic health records, and that it's a priority for her department to provide "adequate guidance" as the willingness and capability to share information across all kinds of platforms rapidly grows.

That's pretty soft; essentially, the feds are saying they'll try to protect you, but criminals usually are a step ahead of the forces meant to thwart them, and mismanaged companies only enable their data-stealing efforts.

Health-care organizations must make data security a priority of information management. They must regularly assess and address the risks to their data. They should recognize and respond quickly to incursions into their "secure" information to reduce the harm to the people they affect. But as the Anthem/Premera breaches demonstrate, that doesn't always happen.

One cybersecurity expert told The Post, "The medical industry is years and years behind other industries when it comes to security."

And as Peel told The Post, government, like industry, isn't keeping up with the demands of security. "HIPAA required security be addressed, but it wasn't spelled it out exactly how, so there was no culture of using ironclad security," she said. "We have systems that are engineered as though this data is not sensitive and valuable."

And even when the "system" identifies a breach, the entity that allowed it to happen often suffers no consequences. (See our blog, "Few Consequences Result When health Data Is Breached.") So what's the incentive to clean up its act?

How to Protect Your Health Information

As the Patient Privacy Rights organization declares, no one should have to choose between privacy and health. Learn more about health privacy from the PPR, and consult its FAQ page for more detailed

information about who can access your information.

Individual states have different approaches to enforcing medical records security, and sometimes their consumer affairs and/or health departments can assist in your efforts to protect yours. Find your state's consumer agency here and health agency here.

In an effort to streamline the delivery of medical services and to ensure all providers have common, accurate patient records, some states are implementing a data-sharing system. California's Open Portal is such a program. According to Andy Krakov, of the California Health Care Foundation,"The value of open data is its potential to put needed data in the hands of those who can do something with it, such as coders, journalists, advocacy organizations and policymakers. Government alone can't be responsible for reaching all the people who can develop apps, visualizations, ways to improve health care. The long-term benefit is to raise awareness -- and data has great potential for exposing what needs to be fixed."

That's certainly possible, but many privacy watchdogs are concerned that Open Portal isn't as secure as it needs to be. Individual consumers whose states encourage their participation in such programs (usually through their health insurers) must carefully consider the benefits and risks before they opt in. In some cases, you must opt out, so review your health insurer information carefully about any such programs.

Recent Health Care Blog Posts

Here are some recent posts on our patient safety blog that might interest you.

- Thinking about surgery for aches in joints and bones? First, read this piece about the conflicts of interest that are rife in the orthopedic industry. We have a list of the top five overused and often worthless orthopedic procedures: knee arthroplasty, vertebroplasty, and more.
- Huckabee the Huckster: Promoting Bogus Diabetes Treatment for Political Gain.
- The "paleo diet " -- why eating like a caveman doesn't make a lot of sense.

Past issues of this newsletter:

We're now in year SIX! Here is a quick index of past issues of our newsletter, most recent first.

Here's to a healthful 2015!

Sincerely,

Patrick Malone
Patrick Malone & Associates