PHOTO: THINKSTOCK

# BRACE FOR THE BREACH

The specter of a massive hack is haunting the healthcare industry. As it turns out, that might not necessarily be a bad thing for everyone involved. **Sarah Mahoney** explains

You don't have to be an IT wizard to know that the healthcare world is just a click or two away from a privacy apocalypse. Hack-a-phobia has moved center stage and consumers are well aware that something as simple as buying a frozen pizza from Target can set off Edward Snowden-grade drama. They're clamoring for "do-not-track" options and seizing control of their cookies. Their outrage is powerful enough to disrupt businesses, tarnish brands and land corporate higher-ups on the unemployment line—just ask the red-faced execs at Home Depot or JPMorgan Chase.

Healthcare, in the midst of a long and bumpy march toward electronic health records, cloud computing and defter data management, may be even more vulnerable than retail and financial businesses. Eset, a security software company, found that 40% of tech-savvy adults worry about the privacy of their health information. The more educated and affluent the consumer, the more likely they are to fret.

So what can everyone in the healthcare ecosystem—physicians, insurers and pharma companies alike—do to maintain confidence in their data-management skills and ensure the sanctity of patient information? Begin by acknowledging that breaches are inevitable.

"While companies need to do everything in their power to protect their data, they also need to assume breaches will occur," says Joseph Meadows, president of Think Patients, a healthcare marketing consultancy. "Any company that acts like a breach could never happen to them just isn't being realistic."

Meadows adds that the industry needs to acknowledge that healthcare breaches are a different animal than other security lapses. Bank accounts can be protected quickly via new debit cards and passwords; but once the cat is out of the bag that Dad needs Viagra, Mom just had liposuction and the kids are seeing behavioral therapists, there's no way that information can be called back.

"By its very nature, healthcare involves intimate, personal data," says Meadows. "It's almost sacred. That doesn't mean the information should not be collected and shared with responsible parties, because it must be in some cases. But sharing does create inherent risks."

Cloud computing adds to the danger, experts say. "As more transactions become wireless, personal medical information becomes abundantly digitized and activists and foreign nations are cyberhacking, we are in a perfect storm for data compromises," says Meg Alexander, a crisis and reputation strategist at Allidura Consumer, a PR company owned by Chandler Chicco.

**"The reality is that the implications of a data breach are far-reaching"**

—Meg Alexander, Allidura Consumer

## Protection: The best medicine

The best offense, of course, is a good defense, and companies need to be committed to making their data as safe as possible. For starters, limit the amount of information individuals are asked to share.

"Collecting data from patients and providers should be restricted to only what is needed for a particular program and use," Meadows says. "The decision to take possession of data should be balanced with both the need for that information and the value of the program compared to the risk of a data breach."

Additionally, all companies need to practice solid IT hygiene, by regularly updating software and investing in plenty of encryption, says Lysa Myers, a security researcher at Eset. She also recommends moving beyond passwords to "two-factor authentications, whether a biometric (like a fingerprint) or even an app on a smartphone."

Similarly, it's important to warn employees about "leaky data" and the risks of free Wi-Fi, a growing problem as workers increasingly log in from airports and Starbucks. "Public Wi-Fi can be an easy way for attackers to eavesdrop and snag your data in transit, if it is not properly secured," Myers says.

Healthcare entities should pay close attention to theft prevention, since that's where they're most vulnerable. A new study from software security firm Bitglass finds that loss or theft of employee mobile devices accounted for 68% of the healthcare breaches since 2010, while hacking was involved in just 23%.

Beyond that, it's essential to do scenario planning, if not all-out doomsday prep work. Ask yourself this: If a breach happens this afternoon, is your company ready? Too often, even healthcare companies that are adequately prepared for adverse regulatory or legal events, consider data privacy an afterthought, says Ben Atkins, digital and social lead at Chandler Chicco. He points out that there are forces for change, including the Federal Trade Commission's draft of rules that ask companies to assume "accountability for protecting user data, or face fines—just as Europe does already. And our industry has always maintained some level of standard due to HIPAA."

Plans should address all the complications that might arise even if the hack occurs via a partner or a vendor. "Companies should take responsibility for data, even when legally the data could be owned by a partner vendor and therefore they are accountable for a breach," Atkins says.

Perhaps most importantly, healthcare organizations must make sure their doomsday plans don't begin and end with IT. "While everyone thinks about IT with a data breach, the reality is that the implications are far-reaching. If a breach becomes public, it will impact the role of the operations and marketing officers," Alexander notes.

Of course, it's not easy to shift the mindset of company execs from "should we be worried?" to "quick! Let's make a plan!" In fact, some observers think industry readiness won't kick into high gear until a Target-sized nightmare strikes a well-known healthcare organization.

Stephen Cobb, also a security analyst at Eset, thinks it might take "a revelation or incident so far-reaching and egregious that just about everyone in the country sits up and takes notice," he writes in a recent blog post. "If that happens there will be headlines, accusations, letters to Congress, recriminations, investigations, jobs lost and eventually huge fines and damage awards. But unless attitudes change and numbers improve, and unless our government decides to get serious about reducing cybercrime, the outlook is stormy at best."

## Data = Solutions

Still, those fears aren't likely to slow healthcare's halting and complex march toward full digitization, whether in electronic patient records, pharmaceutical research or information-sharing among providers and insurers. Progress has been slow: In 2013, for example, only 6% of hospitals had met the Stage 2 Meaningful Use readiness standards the government has set for electronic health records.

Increasingly, that means all stakeholders are more tolerant of the potential dangers involved, says Raj Amin, co-founder of healthcare technology firm Mana Health. "Everyone understands that there are risks and the potential for breaches. Patients are smart, though, and they understand the exchange of data creates some value. The more we can express that value, the more willing they will be."

Amin expects patients to become more thoughtful about what they share. "They may decide not to disclose that they are HIV positive, for example," he continues. "But they see the benefit of consolidated electronic medical records."

**"Patients understand the exchange of data creates some value"**

— Raj Amin, Mana Health

Consumers and businesses alike are increasingly hungry for big-data advantages. In the wake of Apple's introduction of HealthKit, developers are providing many ways to track everything from diet to activity to health updates, via multiple devices. "One of the most common questions consumers have with such apps is 'how do I compare?'," Amin explains. "They know that there is value that can be unlocked for them when lots of data is pulled together in one place, just like when Netflix recommends a movie. We should soon be able to see that kind of innovation in healthcare."

Throughout the health ecosystem, there's agreement that big data is essential to fixing big, challenging problems. "You can't fix or improve what you can't measure, and in a modern society, that requires collecting data in a digital format," says Meadows. "Solving problems without data is going to be impossible. But caring for that data is a tremendous responsibility, and it must be taken seriously." ■