Healthcare IT News

Security: Healthcare's Fixer-Upper

The alarming state of affairs, how the industry's slack security is bad for business, and what some are doing to step it up

June 4, 2014 | Healthcare IT News - Healthcare's all about the patients, right? Earning their trust so they return for annual checkups, delivering high-quality care while respecting their medical privacy at the highest level.

But far too often, there's a disconnect – the idea that the care ends when the patient exits the building or a diagnosis is made, the idea that clinical deals with clinical and information technology deals with IT. But, that's not often the case in this digital age. Lines are blurred, and what happens in one area can have serious implications for another – especially when it comes to patient privacy.

Healthcare organizations are charged with safekeeping some of the most personal and sensitive information on individuals who come to receive care. That bout of depression you had in your early 20s, the sexually transmitted infection you were treated for last year, blood tests of every ilk, cancer diagnoses, medical procedures, HIV statuses, psychiatric disorders, every medication you've ever been prescribed, administered vaccinations, Social Security numbers, dates of birth, demographics, where you live, insurance details, even payment information. Healthcare organizations are gold mines of data. Valuable data. And, traditionally, protecting said data hasn't been the industry's strong suit.

"Protecting data hasn't been the industry's strong suit."

Since 2009, when the HIPAA breach notification requirements took effect, nearly 1,000 large data breaches – those involving 500 individuals or more – have been reported to the Department of Health and Human Services, affecting almost 32 million people.

In addition to the breaches reported by covered entities and business associates themselves, the Office for Civil Rights, the HHS division responsible for enforcing HIPAA, has received nearly 95,000 privacy and security complaints over the handling of health data since 2003.

That's a number meriting a reevaluation of how healthcare does privacy and security.

Complex nature of data breaches

Of course, the reasons behind why many organizations have reported egregious privacy and security failings are not always one dimensional. Oftentimes, data breaches are the result of mistakes by well-intentioned people governed by poor policies and paltry staff training, and sometimes it's the other way around.

Frequently, it's a matter of unencrypted devices being stolen or lost, but there's low probability the data has actually been compromised.

And sometimes, as Lynn Sessions, partner at BakerHostetler, who focuses on healthcare privacy, hears from her clients, it's a matter of a single unencrypted device slipping through the cracks of an entity with otherwise strong encryption policies: "We are encrypting 99.9 percent of our 'fill in the blank' devices, but this one slipped between the cracks because it fell outside of the normal procurement process, or it was a biomedical device or it was used by the marketing department because they use Apple computers versus PCs," said Sessions. "Organizations have loopholes," and therein lies the breach potential.

And lastly, IT departments are just plain swamped, dealing with myriad projects and limited staff, time and budget to handle them. They can't be superheroes all the time. Providers are getting to the breaking point. Sometimes, projects have to be put on the back burner, and in many cases it turns out to be privacy and security. But listen up, IT folks: this just may end up costing you more in the end.

"IT departments are swamped, dealing with myriad projects and limited staff, time and budget to handle them."

Paying a pretty penny

Be certain of one thing: Data breaches come at a premium.

To date, OCR has levied more than $25.1 million in monetary fines against healthcare organizations found to have violated HIPAA privacy and security rules.

Sure, not all groups are slapped with federal penalties, but don't let that ease any worries; the associated costs can often end up trumping government fines.

You have to consider the legal fees, internal investigations, credit monitoring provisions, outsourcing hotline support in addition to the external investigations. And these dollar signs can sure pile up.

A March report by the privacy research firm Ponemon Institute, for instance, pegged the cost of healthcare data breaches at a towering $5.6 billion annually, industry-wide.

Drilling into the numbers further, healthcare organizations can anticipate handing over $2 million on average over a two-year period. (The lowest two-year costs were pegged at $10,000.) That's even a 17 percent decrease from costs seen since last year, Ponemon officials noted, which can be partly attributed to the slight downtick in the number of HIPAA breaches reported by organizations compared to 2012.

So, your organization had a HIPAA breach, didn't get hit with a federal fine and came out relatively unscathed with associated costs. Not too bad, right? Not necessarily.

In addition to HIPAA, there's also the state and regional fines that can get you rethinking how privacy and security is done.

Managed care giant Health Net will tell you a little something about those. The Woodland Hills, Calif.-based health insurance company learned its business associate IBM had lost nine unencrypted server drives in January 2011. The servers contained the Social Security numbers, names, addresses and health information of Health Net employees, members and providers.

They may have dodged federal fines, but that didn't deter two state attorneys general offices from filing suit against the company. Ultimately, Health Net was required to hand over $625,000 in fines and damages to the Connecticut attorney general and the state insurance commissioner. What's more, a year later, the company also announced a settlement with Vermont's attorney general, to the tune of $55,000.

Identify theft

In the realm of patient privacy and security, it's judicious to consider the medical identity theft and fraud landscape. The more laissez-faire healthcare organizations are in protecting patient data, the higher the chance of fraud.

"In 2010 if you received a data breach notification, there was a better than 1 in 10 chance you'd also be the victim of fraud. In 2012, the correlation jumped to 1 in 4."

"To give you an example, in 2010 if you received a data breach notification, there was a better than one in 10 chance that you would also be a victim of fraud. In 2012, the correlation jumped to one in four," said Al Pascual, senior fraud and security analyst for Javelin Research, in an interview with *Healthcare IT News* last year, discussing a fraud case study report.

The report examined a HIPAA oversight by a contracted Utah Department of Health employee that turned into one of the largest HIPAA breaches ever reported, affecting 780,000 people. Due to a server's weak default password and failure to manage the department's IT assets appropriately, hackers exploited the vulnerability, snatching up Social Security numbers, medical diagnostic codes and dates of birth.

From this incident, Javelin Research estimated some 122,000 cases of fraud would occur, with the total cost pegged at a whopping $406 million and representing some 20 hours to resolve each fraud case per person.

Moreover, the value of something like a Social Security number has an "indefinite shelf life," added Pascual. "These people are going to be at risk indefinitely," he said.

"Having that much information, storing it all in one place, leaving it unencrypted, hiding it behind weak or default passwords, that would be wholly unacceptable in the financial industry," added Pascual.

"Storing that much information in one place, leaving it unencrypted, hiding it behind weak or default passwords – that would be totally unacceptable in the financial industry."

Trust and patient health

Then there's the issue of trust and how patients respond following the compromise of their protected health information. This patient response can signify serious long-term consequences for their health and wellbeing, as privacy advocates point out.

"People refuse to see doctors for sensitive conditions because they know the information won't stay private. I'm talking about cancer, depression, sexually transmitted diseases," said Deborah Peel, MD, founder of Patient Privacy Rights, a non-profit consumer privacy watchdog organization, in a 2013 Health Privacy Summit video. "That's a tragedy when people who have very treatable, serious medical illnesses won't get care."

A 2014 Harvard School of Public Health study assessing the privacy perceptions of U.S. adults pertaining to their health data found more than 12 percent of some 1,500 respondents withheld information from care providers over medical security concerns.

Applying this percentage to the national population represents a potential 38.2 million people withholding medical information from providers. What's more, this number doesn't even consider people who altogether forgo medical treatment due to data security concerns.

Findings underscored "the need for enhanced and sustained measures to ensure the confidentiality, integrity and availability of PHI," researchers wrote. This particularly holds true when considering sensitive data like sexually transmitted infections, mental health disorders and drug misuse.

The consequences of patients withholding information or forgoing treatment are numerous, ranging from less severe – perhaps missed opportunities for smoking cessation counseling due to nondisclosure – to serious medical care consequences and compromising surveillance system data quality. "Patients with infectious, notifiable conditions who withhold all or part of necessary medical information (including relevant travel or social history) may inadvertently put the lives of others at increased risk.

Furthermore, non-disclosure, under-information or misinformation may jeopardize the data quality of healthcare surveillance systems," researchers concluded.

Might the some 6,500 HIV positive patients who had their statuses accidentally sent in an email to 800 employees of the Palm Beach County Health Department think twice about going back?

Or what about the 2,300 patients whose medical records and clinical lab results could be Googled online for a period of four months last year, like what transpired at the New York-based Glens Falls Hospital. Cases like these are far from uncommon, not to mention their far-reaching consequences for patient and provider alike.

Advice and to-do lists

As anyone who's ever worked for IT security can attest to, the job is no walk in the park. It's hard work. It's never-ending, and new threats, compliance mandates, vulnerabilities and updates are constantly arising. With strong leadership and a culture of compliance and responsibility to match, however, many healthcare organizations have illustrated it can be done right, and well.

Beth Israel Deaconess Medical Center's Chief Information Officer John Halamka, MD, said for this kind of career, it's a matter of first understanding: "A CIO has limited authority but infinite accountability." You have to ask, "How do you reduce risk to the point where government regulators and, more importantly, patients will say, 'what you have done is reasonable,'" he said.

"Another fundamental piece to doing privacy and security right? Get your risk analysis done -- properly."

This involves thinking about how to encrypt every device, how to protect the data center from both internal and external attacks. "Much of what I have to do is meet with my business owners and ask, 'what are the risks? Reputational risks? Patient privacy breach risks? Data integrity risks? We're never going to be perfect," he added. "But we can put in place what I call a 'multilayer defense.'"

Another fundamental piece to doing privacy and security right? No surprise here: Get your risk analysis done – properly. *"This is the single most important document as part of the OCR investigation,"* said Sessions. "(OCR is) asking for the current one; they are asking for two, three, five years back. They want to see the evolution of what was going on from a risk analysis standpoint at your institution to see if you were appreciating the risk."

This includes safeguards your organization has put in place from technical, physical and administrative standpoints, explained Sessions. Things like staff training and education, penetration tests, cable locks or trackers for unencrypted devices all matter.

Encrypt, encrypt, encrypt

"Encrypt; encrypt; encrypt," said Sessions. It's a safe harbor for the HIPAA breach notification requirements, but that still fails to motivate some.

"(Physical theft and loss) is the biggest hands down problem in healthcare that we are seeing," said Suzanne Widup, senior analyst on the Verizon RISK team, discussing the 2014 annual Verizon breach report released in April. "It really surprises me that this is still such a big problem ... other industries seem to have gotten this fairly clearly."

According to OCR data, theft and loss of unencrypted laptops and devices account for the lion's share of HIPAA privacy and security breaches, nearing 60 percent. (Hacking accounts for some 7 percent, and unauthorized disclosure accounts for 16 percent).

"Theft and loss of unencrypted laptops and devices account for the lion's share of HIPAA privacy and security breaches."

"Pay attention to encryption, for any devices that can leave the office," said former OCR deputy director for health information privacy Susan McAndrew at HIMSS14 this past February.

Of course, the healthcare breach numbers are going to be slightly higher because the federal government has mandated specific HIPAA privacy and security breach notification requirements for organizations, but that has no bearing on the reality that these organizations still fail to implement basic encryption practices, Widup pointed out.

Admitted Hostetler's Sessions, it is a pricing concern. "At a time where reimbursements are going down and technology costs are going up with the advent of the electronic health record, there are competing priorities within a healthcare organization of where they can spend their money."

Full disk encryption costs are currently estimated to be around $232 per user, per year, on average, according to a 2011 Ponemon Institute report, a number representing the total cost of ownership. And that number could go as high as $399 per users, per year, the data suggest.

Kaiser Permanente Chief Security Officer and Technology Risk Officer Jim Doggett, however, said encryption presents a challenge not only because of costs but also because of the data itself. "The quantity of data is huge," he told *Healthcare IT News*.

The 38-hospital health system encrypts data on endpoint devices in addition to sensitive data in transit, said Doggett, who currently leads a 300-person technology risk management team, in charge of 273,000 desktop computers, 65,000 laptops, 21,700 smartphones and 21,000 servers. And don't forget the health data of some 9 million Kaiser members Doggett and his team are responsible for. "This kind of scale presents unique challenges, and calls for the rigor and vigilance of not only the technology teams but of every staff member across Kaiser Permanente," he added.

Encryption is also deployed enterprise-wide by the folks at Mayo Clinic. In addition to encrypting Mayo-issued laptops, tablets, flash drives, etc., any outgoing email unless it's going to a Mayo.edu address must be encrypted if it contains protected health information, said Barbara McCarthy, health information management services and privacy officer of Mayo Clinic in Florida.

Mayo also has a data loss protection application, McCarthy pointed out, which monitors outgoing emails and screens them for certain characteristics indicating disclosure of protected health information. If a disclosure occurs, a Mayo enterprise compliance officer addresses the issue in a direct email to the particular user who sent the information. The site privacy officer is copied along with other key stakeholders. "It's a tough email that goes out," said McCarthy, essentially saying, "Get it back, and don't do it again."

As Mayo Clinic's Mark Parkulo, MD, added: sure, encryption is huge and very much necessary, but an organization also has to concern itself with the policies and procedures portion of privacy and security – the employee education piece of the puzzle.

Importance of employee training

"Some of it is a real education issue," said Parkulo, vice chair of Mayo Clinic's Meaningful Use Coordinating Group, in an interview with *Healthcare IT News*. "A number of providers and other people don't understand that typical unencrypted email; you're not even sure exactly what locations it's going to, whether it could be intercepted or not."

These realities mean Mayo has to host "a lot" of education for providers throughout the year.

In terms of what this education looks like, Parkulo said first Mayo has standard education for employee orientation. On top of that, "then we try to get out multiple times per year, especially if there are issues through email, through grand rounds, through our websites." Sometimes even through the CEO of Mayo Clinic. "We try to get to people as many ways as possible."

"Compliance is everyone's job."

As McCarthy explained, Mayo has launched an effort at the enterprise level to converge on its HIPAA policy. "This is an all-out effort to get everything standardized across the enterprise with site-specific procedures," she said. "It's really been a great opportunity to refresh folks on what's really been in place."

Kaiser's Doggett agreed: getting to all those people is the important thing. "*Compliance is everyone's job,*" he said. "Our code of conduct, compliance policies, and compliance training curriculum make this expectation clear."

But be sure to go beyond the mere policies, Sessions cautioned. "(Healthcare) probably has more policies than they know what to do with," she said. "As far as the written policy, that's great. Connecting to the end users particularly on the security side I think is more difficult."

Beyond privacy: security is vital

On top of the privacy piece of the puzzle, there's also the security standpoint to consider – and it's far from one-dimensional.

Phil Lerner, chief information security officer of Beth Israel Deaconess Medical Center in Boston, said he has many competing priorities. "Continuous monitoring is a large priority of mine, so having a 360-degree view into whatever the technology may be," he told us. Then, there's supply chain security, "always digital forensics, mobile device forensics, incident response."

With threats like the Heartbleed vulnerability and cyberattacks on the industry only on the upswing – some 40 percent of healthcare organizations have reported a criminal data attack this year, according to Ponemon data – data security proves absolutely critical for organizations.

"What's newer at least in the few years as part of continuous monitoring is definitely threat feed analysis," added Lerner.

As the experiences of industry professionals have demonstrated, healthcare privacy and information security is not done in a vacuum. Whatever information technology departments or privacy officers do with the data from a technical and administrative standpoint, there also exist the corresponding clinical implications. It's simple cause and effect. Compromise the most personal of data, and you compromise the relationship between provider and patient.

"Past (security) incidents show us the industry has time and time again said: 'We care, but not a whole lot.'"

Past incidents show us the industry has time and again said, 'Come and trust us with your most personal information, but don't expect us to have a firewall to protect it; don't expect us not accidentally to post it publically online or encrypt it or monitor employees who are inappropriately accessing the data.' *They've said, 'we care – but not a whole lot.'*

Healthcare privacy and security needs a shakeup, an overhaul, a revamp of policies and system security.

It's not just a matter of professional obligation and responsibility. It's a matter of cost, reputation and the integrity of the patient-provider relationship. IT is waist deep in it all, for better or for worse. Now, here's to the better.

Erin McCann is Associate Editor at *Healthcare IT News. Her article above is posted at:*
http://www.healthcareitnews.com/news/security-healthcares-fixer-upper