NDoc Connect Blog

This year's diagnosis for the healthcare industry? Data breaches

You might have a fleeting moment of worry when you type in your credit card information to make an order on Amazon, or figure that most cyber attacks involve financial institutions or government agencies anyway. But as recent reports show, healthcare is actually the most-targeted industry for data breaches - and the threat is only growing.

A survey conducted by 451 Research in April revealed that 63 percent of healthcare industry professionals reported that they had experienced a data breach - a larger share than any other industry. And the 2016 Data Breach Industry Forecast published at the end of last year by Experian predicted that healthcare will be one of the most at-risk industries for cyber attacks in 2016. In addition, it found that a whopping 91 percent of all healthcare organizations experienced at least one data breach in the last two years.

With the rise of the adoption of electronic medical records, that means the healthcare industry needs to take a harder look at how it's storing, sending and securing patient information.

Don't let the wrong hands get on your agency's data.

High-value information

So while you may think that cyber crooks only want credit card numbers, there's another type of data that is worth a pretty penny: patient health information. Medical records are now worth nearly 10 times more than credit card numbers on the black market, according to Experian. Health records are attractive to hackers because they change much less frequently than credit cards, and because financial information is usually found in the same networks that store the health information, giving hackers an easy two-for-one deal,a paper by the Escal Institute of Advanced Technologies noted. Medical records are also frequently stolen to commit insurance fraud, according to Reuters.

This year's diagnosis for the healthcare industry? Data breaches

Targets big and small

Last year, several major healthcare companies had their data swindled and held for ransom. In March 2015, Premera Blue Cross suffered a cyber attack that exposed the medical and financial data of 11 million customers, making the incident the largest-ever breach of patient medical data, reported Reuters. And the very same day Premera was attacked, Anthem Inc announced that it had also been targeted by an online attack that jeopardized the medical records of 79 million customers.

"Medical records are worth 10 times more than credit card numbers on the black market."

However, it's not just the big healthcare players that are the victims of cyber attacks. Bloomberg reported that in 2012, the Surgeons of Lake County, a small medical center in Illinois, had its emails and electronic medical records stolen by hackers and held for ransom.

Since EHRs rely in part on self-reported patient information to improve care, the rising incidence of data breaches is especially worrying. The Escal Institute of Advanced Technologies cited a 2015 Protected Health Information Data Breach Report by Verizon that found that "people may even be withholding information from their health care providers because they are concerned about the confidentiality of their records."

Comprehensive coverage essential

Armed with the knowledge of the growing threats to healthcare information security that loom large over the industry, agencies of all types and sizes need to re-evalute their networks and EHR systems to ensure that their data is encrypted and secure. In interview with CSO Online, Tina Stewart, vice president of marketing at Vormetric, which sponsored the 451 Research report, recommended that agencies have comprehensive security measures and make sure that they do not rely on federal regulatory compliance to keep their systems secure.

"Lots of investment is going into network and endpoint protection," she said. "However, healthcare organizations should prioritize protecting critical information once perimeters have been breached. It's not that we don't need network and endpoint defenses, but priorities should shift to include data security."