HEALTHCARE IT TRANSFORMATION:
How Has Ransomware Shifted the Landscape of Healthcare Data Security?

By Karly Rowe, Experian Health

Healthcare IT transformation

Exchanging information across the healthcare ecosystem and achieving interoperability are goals and challenges healthcare organizations share. Regulations such as the Affordable Care Act and Meaningful Use put forth incentives and requirements to drive adoption of electronic medical records and facilitate the exchange of information. And while healthcare's transition from paper to electronic medical records brings IT efficiencies and benefits to care coordination and patient engagement, it also presents new challenges and risks in managing and protecting patient's digital medical identities.

The challenges of protecting digital medical identities

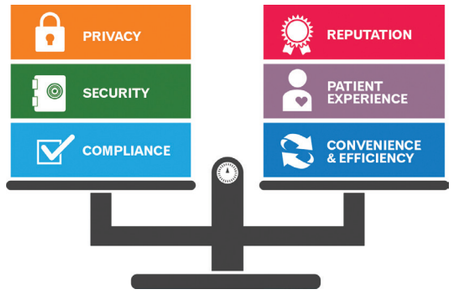
Healthcare organizations are continually challenged with balancing security with the patient experience and convenience.

While the healthcare industry focuses on integrating electronic medical records into various systems and processes, criminals see a ripe opportunity to steal medical identities from vulnerable, unprotected systems. In comparison to other industries, such as financial services or retail, healthcare lacks the sophisticated data security tools; making it an easier target with more lucrative data. With medical identities valued at 20-50 times more than financial identities (according to the Federal Bureau of Investigation), criminal attacks are now the leading cause of healthcare breaches. Statistics from the Identity Theft Resource Center show more than 112M records were compromised in 2015, up from 8.3M in 2014. Accompanied by the fact that detecting an intrusion can take a year or more, healthcare breaches continue to fuel medical identity theft which is the fastest growing type of identity theft— increasing at a rate of 22% annually.

As healthcare organizations drive large volumes of sensitive personal health information to data storage platforms, the complexity of protecting patient information increases as the number of users and devices accessing it grows. For physicians embracing 'bring your own device' strategies and patients demanding information at their fingertips, healthcare organizations struggle to implement security protocols without hindering the patient experience.

After watching some of the largest healthcare enterprises fall victim to attacks in 2015, the reprieve that many hoped for in 2016 is no longer in sight. 2016 has ushered in a new wave of ransomware attacks, which have forced healthcare organizations to completely shut down operations for days at a time. The healthcare industry is now recognizing 2015's attacks as merely the beginning of a new era in healthcare. Data security has become—and will remain—a top priority for the healthcare industry.

Healthcare organizations have come to realize that data security measures must extend beyond their own organization to include vendors and patients, both of whom are accessing sensitive information within their network. The industry is now taking a closer look at the security policies and the business associate agreements they have in place with vendors



to ensure that those relationships aren't creating additional vulnerabilities for criminals to exploit. Furthermore, healthcare organizations are acknowledging that there isn't a silver bullet, or a single solution, which can address all of their security challenges. This shift in thinking is ushering in new multi-layered, multi-solution security strategies to provide more comprehensive protection.

As important as a healthcare organization's security strategy, is its communication to patients. The number of healthcare organizations plagued by negative headlines has led to heightened patient sensitivity about sharing their personal information. 64% of patients cite privacy issues as a key concern for accessing health information online and another 21% admit to withholding information from doctors out of concern of data security. These behaviors have significant care implications and directly oppose the goals of interoperability, for which electronic medical records were intended to help achieve. Healthcare organizations need to be proactive and transparent about the measures they are taking to keep patient data safe, with a focus on building a stronger level of trust with their patients.

Experian Health's role

Experian Health is an industry leader in offering revenue cycle management, identity management, population wellness, and data and analytics solutions. Driven by real-time data and advanced analytics, our solutions help clients improve operational efficiency, financial responsibility and care coordination in today's value-based environment. Healthcare providers, labs, pharmacies and other risk-bearing entities leverage Experian Health's products and services to better understand their financial performance, make smarter business decisions, enhance their bottom line, protect patient identities and strengthen the patient payment and care experience.

Matching, managing, and protecting consumer identities is at the core of Experian's expertise. We have more than 40 years of experience delivering these capabilities across many industries, including healthcare, financial services, state and local government agencies, and retail. Drawing on our experience and leveraging our breadth and depth of data sources, robust analytics, and deep-rooted healthcare expertise, we deliver solutions to address healthcare's business challenges. We partner and integrate with leading health information services vendors to deliver identity verification for healthcare portals.

Experian Health Precise ID® with Digital Risk Score enables healthcare organizations to verify patient identities before providing patients access to healthcare portals with sensitive health information. Our solution provides multilayered identity verification by evaluating identity, device, and online risk factors in one, comprehensive platform and in less than one second. It provides continuous medical identity protection during enrollment and ongoing portal access requests without burdening patients with lengthy processes. Precise ID with Digital Risk Score ensures the right patients are given access to sensitive health information, allowing healthcare organization to reassure patients that their medical identities are protected and build a trusting relationship.

As the industry continues to evolve into a more digital environment, healthcare organizations need to adapt by developing and implementing more robust security strategies. Through relationships with vendors, such as Experian Health, healthcare organizations can better protect their patient's sensitive information.

www.experianhealth.com

Increasing volume of PHI on data storage platforms

Fluidity and persistence of data on computers, mobile devices and internet

Medical identities are more lucrative than financial identities

It can take up to one or two years before medical identity theft is detected.