NEUDESIC
an IBM Company

Meeting the Security Challenge:

How Healthcare Organizations are Stepping Up Data Privacy

By Lori Clark

Security is an imperative for every industry and company—and in the healthcare industry it is especially critical.

In addition to the same security concerns every industry has about information and data privacy, the healthcare industry also has enhanced regulatory and ethical requirements related to the privacy of healthcare information.

According to some sources, about 30% of the world's data volume is being generated by the healthcare industry.[1] This data includes information that is particularly vulnerable to security breaches such as Personal Health Information (PHI), Personally Identifiable Information (PII), and patients' financial information. For decades, there has been an attempt to consolidate all of these sources of personal information through efforts like statewide Health Information Exchanges (HIEs), that would make it easier for patients and their various healthcare providers to have all of the patients' information in one shared location. By sharing patient information with other healthcare organizations, however, patients' personal information and data becomes extremely vulnerable–and extremely valuable–for those wishing to profit from its acquisition.

[1]Wiederrecht, G., Darwish S., Callaway A., The Convergence of Healthcare and Technology. RBC Capital Markets. https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion#content-panel (Accessed July 22, 2022)

What is the current state of security in the healthcare industry?

Right now, the healthcare industry is a unique combination of cutting-edge technology and aging legacy systems like spreadsheets and manual data input.

While patients are embracing technology like health apps and demanding easier access to their personal health information, healthcare organizations are being pushed to up their own technology game.

As technology advances, however, so do the security concerns that span all industries—the threats of hackers and those with ill intentions trying to gain access to entire networks of information illegally. Connecting networks of data creates better access for healthcare organizations and patients, yes, but it also creates the opportunity for hackers to gain that same access to valuable information. Healthcare organizations have been experiencing escalated costs related to data breaches. In 2020 alone, healthcare data breaches cost $13.2 billion, which is over double the amount of the annual data breach cost of $6.2 billion in 2017. In response to these breaches, regulators are increasing pressure on healthcare organizations to improve security and compliance–but they aren't providing the funding for the healthcare organizations to do so.

The healthcare industry is also facing the challenge of every healthcare organization having different security protocols and processes. With various degrees of security measures in place, healthcare organizations lose the ability to effectively secure and manage their data widely. A prime example of this is the HIEs and the security situations they create by trying to consolidate patient information. The HIEs bring patient information together so that patients, providers, and payers can interact with the information directly and share it between cooperating and competing organizations. In doing so, however, the patients' information is now at the discretion of many organizations who may or may not be as secure and compliant as the organization that originally gathered the patient information, which could then compromise how secure the data remains.

So, how can healthcare organizations prepare for future security risks and threats?

To protect their patients' vulnerable information, healthcare organizations must invest in technology and processes that bolster the security of that information.

In addition to increasing their own security maturity, healthcare organizations must enhance regulations that enforce security and compliance standards to resolve the issues of when patient data is shared.

The Neudesic Care Management Platform helps healthcare organizations meet their security challenges and protects patient information from future security threats. Built on Microsoft Cloud for Healthcare, Neudesic's Care Management Platform incorporates security best practices to protect information. It uses a rich security model to protect the data integrity and privacy of users while promoting efficient data access and collaboration.

The platform is ideally suited to strengthen and improve healthcare ecosystems and promotes sharing patient information securely. It combines business units, role-based security, row-based security, and column-based security to define the overall access to information, while also meeting the healthcare industry's compliance and regulatory requirements.

A platform built for better outcomes

Neudesic's Care Management Platform is already improving patient care and business outcomes for healthcare organizations. The platform is helping increase security and building confidence in healthcare providers, payers, and patients by:

Reducing risk by 70% through improved case management and elimination of information gaps.

Reducing payment errors and missed payments by more than 90% through batch generation.

Reducing process overhead by 30% by streamlining processes and eliminating data re-entry.

Information security is an ever-present threat to all industries. For healthcare organizations, the Neudesic Care Management Platform is helping secure vital patient data and improve healthcare delivery.

About Neudesic

Neudesic is the trusted technology partner in business innovation, delivering impactful business results to clients through digital modernization and evolution. Our consultants bring business and technology expertise together, offering a wide range of cloud and data-driven solutions, including custom application development, data and artificial intelligence, and comprehensive managed services. Founded in 2002, Neudesic is headquartered in Irvine, California.

To learn more about Neudesic, please visit:
www.neudesic.com