Why You Should Select a HITRUST Certified Vendor For Your Medical Practice

An inside look at how data breaches can affect your patient's trust.

There are over 6.1 million healthcare data breach victims in 2018, costing hundreds of millions and compromising Protected Health Information, or PHI, for numerous patients worldwide. Research shows that with the proper execution of a HITRUST framework, a majority of these reported breaches would have been prevented or swiftly remedied by implementing adaptable and scalable safeguards, preventative measures, and corrective systems -- saving countless dollars, hours, and headaches from malicious attacks and human errors.

The high cost of data breaches in the Healthcare Industry

The Breach Barometer Report from Protenus showed that at least 3,143,642 patients were exposed in data breaches during Q2, 2018. With over 140 data breaches during this period involving healthcare organizations, it's clear that Protected Health Information (PHI) is constantly at risk.

PHI, also known as personal health information or private health information, is a vulnerable target due to the large amount of sensitive data connected to it.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), also known as Public Law 104-191, contains in Section 1171 of Part C of Subtitle F, Administrative Simplification, a definition of health information as: "any information, whether oral or recorded in any form or medium, that – (A) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of healthcare to an individual, or the past, present, or future payment for the delivery of health care to an individual."

In short, any health information that can be tied to an individual is considered PHI, such as administrative and personal details; clinical, diagnostic, treatment, and prescriptive information; payment, insurance, and health plan information; notes, conversations, documents, test results, and references, regardless of medium, that are related to a person's health.

PHI is valuable data to criminals, hackers, and other nefarious elements. It can be used to conduct criminal acts such as ransoming private individual medical data, identity theft, accessing payment and billing systems, and stealing financial data.

The healthcare industry is disproportionately vulnerable, accounting for 45% of all ransomware attacks in 2017. These attacks are very common and have been known to shut down IT systems of entire medical centers for weeks on end.

While some high-profile PHI breaches are caused by hacking and criminal activities, even more of them are due to insider or vendor errors and loss of devices or documents that contain PHI.

Here are some examples of recent data breaches in the healthcare industry:

- A ransomware attack against the Fetal Diagnostic Institute of the Pacific in June 2018 potentially breached the data of 40,800 patients.
- In August 2018, three phishing hacks breached 20,000 Catawba Valley patient records through unauthorized access from an employee email account.
- The Centers for Medicare and Medicaid Services discovered a data breach in October 2018 that compromised the records of as many as 75,000 individuals.

These incidences are just the tip of the iceberg. There are many more breaches that have likely gone unreported or yet to be disclosed to the public.

HIPAA violations severely impact the healthcare industry on multiple levels. To consumers, medical identity theft can result in collection letters from creditors for expenses that thieves incurred in their name, out-of-pocket payments to healthcare providers or insurers to restore coverage, and increases in healthcare premiums.

The global average cost of data breaches has reached $3.86 million in 2018. IBM and the Ponemon Institute found that the cost healthcare data breach averages at $408 per record, the highest of any

industry for the eighth straight year. (It's nearly three times higher than the cross-industry average of $148 per record.)

For more data on the cost of data breaches, refer to the latest report issued by the Ponemon Institute.

The impact of healthcare violations and PHI breaches includes potentially significant fines and penalties, as well as the loss of patient trust. In August of 2016, the U.S. Department of Health and Human Services (HHS), Office of Civil Rights (OCR) announced one of the largest settlements for HIPAA violations involving PHI. Advocate Health Care Network paid a settlement amount of $5.55 million and adopted a corrective action plan for multiple HIPAA violations.

In addition to fines and penalties, it's extremely costly to alert thousands, if not millions, of patients of a breach, provide remediation options for credit monitoring, and repair legal matters.

Other significant expenses incurred by healthcare organizations due to data breaches include the business costs of implementing IT security, ensuring business continuity, and setting up incident response plans to prevent future breaches.

While fines and other costs are a significant consequence of violations, the loss of revenue due to a decrease in consumer confidence, trust, and loyalty can be devastating as well. These intangible measures can result in a decrease in sales, losing customers or patients to competitors, marketing challenges, and stagnation in growth. While there may be metrics by which to quantify these intangibles, their actual value is immeasurable.

In 2017, there were 477 reported PHI breaches, affecting 5.6 million patient records. This is a startling number and justification for PHI data security to be a top priority for any organization that creates, accesses, exchanges, or handles PHI in any manner.

While data breaches and HIPAA violations are risks that healthcare organizations have to contend with, they can take better control and manage the complex security landscape of this industry with the HITRUST framework.

Managing Security Risk with HITRUST Framework

HITRUST was founded in 2007 as a collaborative effort among healthcare, business, technology, and information security leaders.

It aims to help organizations effectively address and efficiently manage the complex mix of security, privacy, and regulatory factors that affect health information systems and exchanges that handle PHI -- with the ultimate goal of safeguarding PHI. To accomplish this, the HITRUST Common Security Framework (CSF) was developed.

Through its many programs, methodologies, and services, the HITRUST CSF creates a new playing field for those who create, utilize, manage, or store PHI. It addresses and manages the internal and external factors, whether malicious or not, that threaten PHI.

HITRUST creates the solid foundation the healthcare industry needs to prevent and mitigate the various data breaches involving PHI that will continue to occur.

HITRUST CSF provides the organizational structure necessary to clarify, manage, utilize, and cross-reference the compliance and authoritative sources that govern healthcare. Following a risk-based approach, this comprehensive framework effectively incorporates and manages existing state, federal, international, and industry-specific standards, including ISO, NIST, HITECH, HIPAA, PCI, and COBIT.

How does HITRUST work?

Through a prescriptive set of controls, the CSF harmonizes and synchronizes the multitude of healthcare and healthcare-related authorities, standards, and regulations – allowing organizations to manage risk and solve compliance issues more effectively through assessment and assurance methodology programs and healthy controls available in the framework.

In addition, HITRUST CSF can be scaled to any organization's size, type, and complexity. From national hospital networks and chains to business associates and vendors that service healthcare entities, each

organization can customize, manage, and organize compliance standards as they apply to the organization.

Developed by industry leaders and experts across the healthcare industry spectrum that has a vested interest in maintaining the highest level of healthcare information security, HITRUST has become a standard for safeguarding and defending PHI from internal and external threats. As the most widely-recognized healthcare information cybersecurity leader, HITRUST operates the most active cyber center in the healthcare industry.

The HITRUST Cyber Threat Intelligence and Incident Coordination Center (C^3) uses a community defense and proactive alerting approach to handle the vulnerabilities faced by healthcare organizations and protect PHI against the threat of cyber criminals.

Partnerships with HHS and the Department of Homeland Security (DHS) contribute to the strength and efficacy of C3 -- further emphasizing the importance of healthcare information security.

HITRUST is a federally recognized Cyber Information Sharing and Analysis Organization (ISAO) that has information-sharing agreements with the HHS and DHS, which helps augment its efforts to reduce risk, exposure, and the threat to PHI.

In addition, HITRUST has partnered with the DHS Automated Indicator Sharing (AIS) Program. Through its Cyber Threat Xchange (CTX), HITRUST has integrated with AIS and can exchange cyber threat indicators with users, allowing organizations to reduce cyber risk through relevant and timely cyber threat information (CTI).

The integration and support of bidirectional CTI with DHS AIS now grants healthcare organizations that use HITRUST the chance to receive and send real-time CTI. This real-time exchange of information between the government and private sector changes the healthcare security landscape for organizations that utilize HITRUST CTX and allows them to address, respond to, and mitigate threats more effectively. This integration has also strengthened the defense of the nation's overall network security infrastructure.

Other cybersecurity programs HITRUST has implemented include a partnership with HHS for monthly healthcare industry cyber threat briefings. These briefings allow organizations to communicate CTI more

efficiently through the distribution of relevant, actionable, and educational threat information so they can better identify, mitigate, and respond to cyber threats quickly, effectively, and efficiently.

Capitalizing on their cybersecurity programs, HITRUST has established CyberRX: Health Industry Cyber Threat Exercise. Through another partnership with HHS, CyberRX is a series of industry-wide exercises that aim to mobilize and prepare healthcare organizations to respond to cyber threats utilizing innovative approaches, ideas, methods, and tactics.

The exercises include and examine both broad and segment-specific scenarios targeting health information systems, medical devices, and other essential technology resources used in the healthcare industry. The results and findings of these exercises provide valuable information and insights to help coordinate CTI, thereby improving C3 efforts and information sharing among healthcare organizations, government agencies, and HITRUST.

HITRUST not only sets the standard for healthcare information security and compliance management, but it also saves organizations time and money through its data management tools.

The digitization of health records (known as EHR) presents a myriad of logistical, security, organizational, and management concerns. While the risk to and threat against PHI is a primary concern for organizations, the need for effective data handling measures is also a challenge.

The sheer amount of data related to PHI is massive. HITRUST offers tools that provide solutions to performing assessments, organizing and managing audits, handling reporting, and tracking compliance.

Through its comprehensive, flexible, and efficient risk-based approach to regulatory compliance and risk management, the HITRUST CSF incorporates these tools to take the burden off organizations when it comes to data management and handling. With an ever-growing information highway that gets more complex every day, the need for such tools is invaluable to the healthcare industry.

The HITRUST CSF is as adaptable as it is robust. In addition to being scaled to suit the size and type of various users, organizations, and entities, the framework also evolves and adapts to user input, changing conditions in the healthcare industry, and the regulatory environment. This flexibility helps users stay current in their practices, procedures, and changes in industry regulations.

One of the most positive effects that HITRUST has on the healthcare industry is creating a dialogue about healthcare information security and providing an educational platform for building security

standards, establishing best practices, addressing the demands of compliance and risk management, organizing and managing data, and safely handling PHI.

In addition, the HITRUST Academy offers the only training courses designed to educate healthcare security professionals about data and PHI protection specific to the healthcare industry. It has been an incredibly powerful influence in closing identified gaps in the field by sponsoring industry working groups, panels, and committees, which are charged with addressing, identifying, organizing, and managing healthcare information security and privacy challenges.

Through its various initiatives, HITRUST is at the forefront of healthcare cybersecurity, healthcare information security education, and thought leadership.

Going back to the data breaches mentioned earlier, they could have been prevented, or at the very least, quickly and efficiently identified and safely remedied if the HITRUST CSF and its programs were utilized. For example, controls set forth by the CSF could include a checklist for controlling network access and setting administration privileges to prevent unauthorized access to PHI.

With endless features, programs, tools, and knowledge contained in the framework and associated systems, the enacted controls and measures offered by HITRUST cover management and compliance matters and address the full spectrum of cybersecurity needs.

With HITRUST's educational resources and thought leadership initiatives, healthcare organizations, their business associates, and vendors can find prescriptive methodologies and standards to help protect, organize, and manage healthcare data and PHI.

Partnering with a HITRUST-certified third-party medical billing partner allows for further benefits beyond billing compliance and enhanced security.

It can also help reduce billing errors, save money while improving cash flow, and allow a hospital or practice to focus on their core competency -- developing and improving relationships with their patients and improving care.

Hospitals and other health facilities can prevent security breaches, protect valuable PHI while improving overall billing and collection procedures by implementing third-party enterprise-level security compliance systems that are HITRUST compliant.

Sources

https://www.beckershospitalreview.com/cybersecurity/6-1m-healthcare-data-breach-victims-in-2018-5-of-the-biggest-breaches-so-far.html

https://www.hipaajournal.com/q2-2018-healthcare-data-breach-report/

https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-accounted-45-all-ransomware-attacks-2017

https://www.healthcareitnews.com/news/3-phishing-hacks-breach-20000-catawba-valley-patient-records

https://www.healthcarefinancenews.com/news/cms-responds-data-breach-affecting-75000-federal-aca-portal

https://www.healthcareitnews.com/news/ransomware-attack-fetal-diagnostic-lab-breaches-40800-patient-records

https://www.ibm.com/account/reg/us-en/signup?formid=urx-33316

https://healthitsecurity.com/news/healthcare-data-breach-costs-remain-highest-among-industries

https://hitrustalliance.net/

https://hitrustalliance.net/content/uploads/2014/07/HiTrustC3Datasheet.pdf

https://www.us-cert.gov/ais

https://www.healthcare-informatics.com/news-item/cybersecurity/2017-breach-report-477-breaches-56m-patient-records-affected