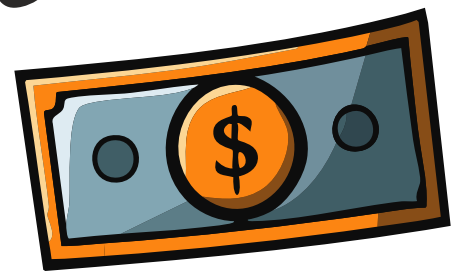
HOW SELECTING A HITRUST Certified VENDOR COULD SAVE YOU MILLIONS |



Data breaches are dangerous and incredibly costly. Learn more about how a HITRUST-certified vendor can mean the difference between secure PHI and successful ransomware attack.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

Introduction

According to The HIPAA Journal, there were **721** **healthcare data breaches** involving 500 or more patient records in 2024 - more than double the number of similar breaches a decade later, in 2014. Even more troubling, the 10 largest healthcare data breaches in 2024 exposed the personal health information, or PHI, of 137 million individuals.

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, the following definition of health information: **"Health information means any information, whether oral or recorded in any form or medium, that–**

(A) is created or received by a health care 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 health care to an individual, or the past, present, or future payment for the delivery of health care to an individual."

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

In short, any health information that can be tied to an individual is considered PHI. The following are a few common examples:

Administrative and personal details about an individual patient

Clinical, diagnostic, treatment, and prescriptive information

Payment, insurance, and health plan information

Notes, conversations, documents, test results, and references—regardless of medium—about any topic related to a person's health

PHI is valuable data to criminals and hackers who can use this information for any number of criminal acts, from ransoming private individual medical data and identity theft to accessing payment and billing systems, allowing for the theft of financial data.

Understand How Breaches Happen

When it comes to ransomware attacks, healthcare is disproportionately affected, with ransomware attacks targeting hospitals. In October 2020, the FBI, the Cybersecurity and Infrastructure Security Agency, and the Department of Health and Human Services issued a statement advising healthcare organizations to be especially vigilant of ransomware attacks.

In the years following this warning, we have seen a number of large-scale ransomware attacks on healthcare systems and hospitals, with some occurring across multiple states. These attacks are very common and have been known to shut down IT systems of entire medical centers for weeks on end.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

While PHI breaches from hacking and criminal activity can result in serious consequences, many PHI breaches are due to insider or vendor wrongdoing or error and loss or theft of devices and documents that contain PHI.

As an example of this, the **most significant breach in 2024** was one caused by unauthorized access to email addresses. Bad actors were able to gain access to the email accounts of two Kaiser Permanente employees; this security breach exposed the medical information of...

13.4 *million* individuals

In one of the largest breaches of 2020, Health Share of Oregon had to notify over 654,000 patients about a potential breach of their PHI. What's worse is that this breach was caused not by an employee of the healthcare organization itself, nor a clever hacker who outsmarted the organization's IT and cybersecurity measures. Instead, this breach was the result of one of the healthcare organization's vendors—a laptop of an employee of Health Share of Oregon's transportation vendor, GridWorks, was stolen.

While this incident of laptop theft might not have been the employee's fault, this particular data breach speaks to how important it is that vendors take the same cybersecurity precautions as the healthcare organizations they serve. To put oneself in the shoes of a hacker, if healthcare organizations are arming themselves against cybersecurity threats, it makes sense to instead target vendors that work with these organizations due to their potential for having a lowered guard and less-sophisticated security software.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

These are just a few of the hundreds of breaches that occurred in the past five years, with many more likely going unreported or yet to be disclosed to the public. You can find more examples of prominent data breaches here.

SafeGuarding Patient Data in the Era of AI

While ransomware, hacking, and unauthorized access remain ongoing threats, a new vulnerability has emerged in recent years: artificial intelligence (AI).

Automation and AI are transforming healthcare in countless ways, from assisting in diagnosis on the clinical side to streamlining patient billing processes on the administrative end. With these advances comes a heightened responsibility to protect sensitive patient data from emerging cyber threats.

AI is improving the speed and accuracy of healthcare billing, but as this technology becomes more prevalent, it also becomes more and more alluring to cyber criminals. AI systems aggregate and analyze vast amounts of data, which means any breach could expose sensitive patient information, including medical records, billing details, and insurance information.

The risk is amplified by the complexity of healthcare data and the expanding attack surface created by interconnected systems. This aggregated data is vulnerable in the same ways other PHI is vulnerable—through phishing, ransomware, insider threats, and simple user error or oversight.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

Healthcare providers must adopt a proactive mindset toward cybersecurity, ensuring they stay ahead of these evolving threats rather than taking a wait-and-see approach. The implementation of AI and automation should always be accompanied by more robust data protection practices.

The Consequences of Data Breaches

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

In 2022, the Federal Trade Commission received over *27,000* **reports of medical identity theft**. The survey estimated that the total value of out-of-pocket expenses incurred by victims of medical identity theft was *$12.3 billion*.

To businesses, the impact of healthcare violations and **PHI breaches includes potentially significant fines and penalties and loss of consumer trust**, with the largest settlement amount for HIPAA violations coming in at a staggering *$16 million.*

Victims of identity theft paid

$18,660 on average

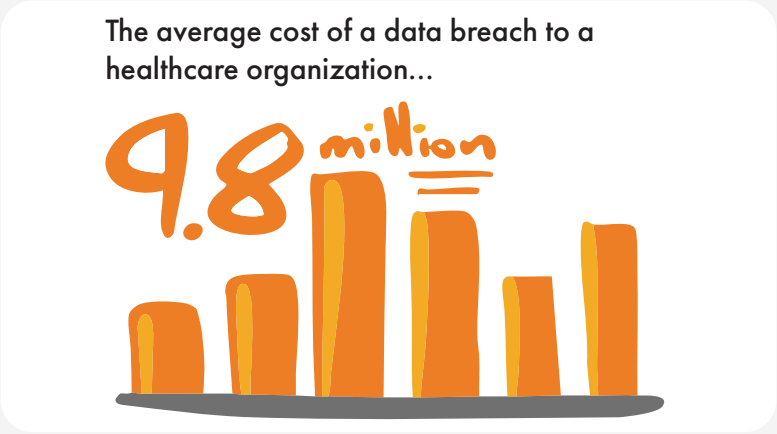
2013 Survey on Medical Identity Theft by the Ponemon Institute

In 2018, after exposing the personal data of 79 million individuals...

Anthem Inc. was ordered to pay the OCR $16 million in addition to a $115 million settlement for a class action lawsuit filed by the consumers whose data was exposed in the breach.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

On top of these fines and penalties, the cost to alert thousands—or, in some cases, millions—of patients of a breach, provide remediation options from credit monitoring, and resolve legal matters is extremely high.



The Ponemon Institute and IBM Security 2024 analysis of the cost of healthcare data breaches

Healthcare has been the costliest industry for data breaches since 2011, with business disruptions, remediation, and customer service driving much of the cost.

The overall cost of a data breach **increased significantly in 2024**, driven partly by a nearly 11% **rise in expenses** related to lost business and post-breach response compared to the previous year. Lost business costs encompass revenue lost from system downtime, as well as expenses associated with customer loss and reputational damage.

Another significant expense incurred by businesses due to data breaches includes the costs of coming up with and implementing information security, business continuity, and incident response plans to prevent future breaches. This cost includes documentation, employee training, hiring a Chief of Information Security Officer (CISO), and more.

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

MailMyStatements 165 Caprice Ct, Castle Rock, CO. 80109 | 866 943 7287 | sales@mailmystatements.com

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

How HITRUST-Certified Vendors Protect Against Data Breaches

While data breaches, HIPAA violations, and PHI risks are inevitable challenges that the healthcare industry must contend with, there is a powerful framework available to healthcare organizations that can help manage the complex security landscape that this industry presents—that framework is the Health Information Trust Alliance (HITRUST).

HITRUST was founded in 2007 through a collaborative effort of healthcare, business, technology, and information security leaders. The aim of this collaboration was to help organizations effectively address and efficiently manage the complex **security, privacy, and regulatory factors** that affect health information systems and exchanges that handle PHI and ultimately safeguard 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, and those internal and external factors, whether malicious or not, that threaten PHI. HITRUST creates the solid foundation the healthcare industry needs, one that is critical to the prevention and mitigation of various data breaches involving PHI that will continue.

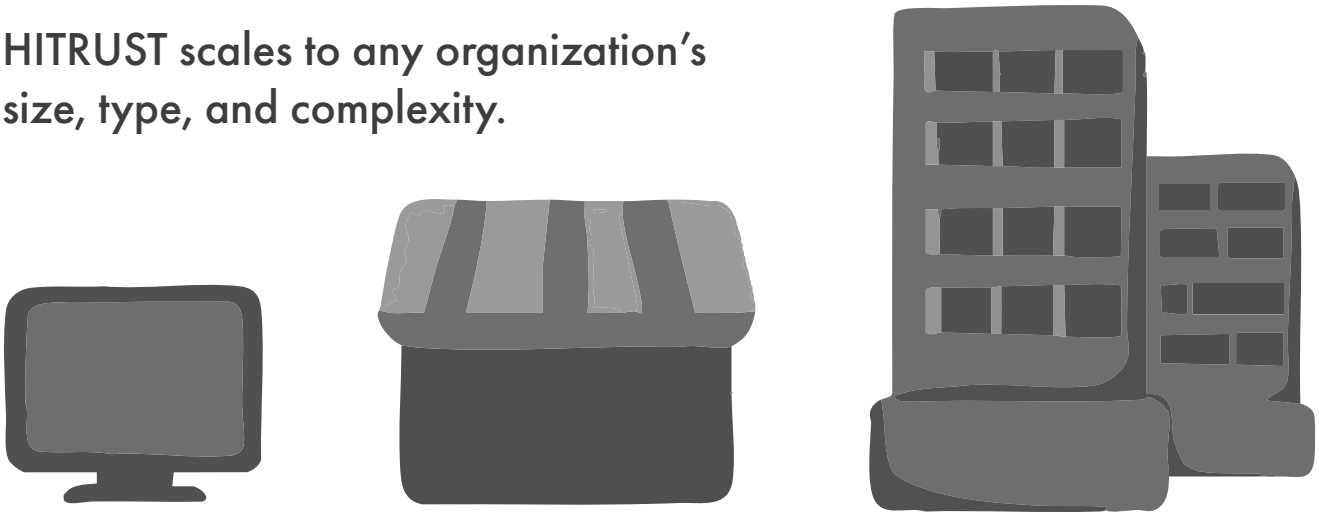
The HITRUST CSF provides the organizational structure necessary to clarify, manage, utilize, and cross-reference the compliance and authoritative sources that govern healthcare. Following a risk-based approach, this comprehensive framework effectively incorporates and manages existing state, federal,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

BillingCycle Plus™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

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 compliance better. With assessment and assurance methodology programs and healthy controls available in the HITRUST CSF, organizations can identify risks and solve compliance issues.

One of the many benefits of this CSF is its scalability. From national hospital networks and chains to business associates and vendors that service and assist healthcare entities, each organization can customize, manage, and organize compliance standards as they apply to that organization and their handling of and interaction with PHI.

HITRUST scales to any organization's size, type, and complexity.



Developed by industry leaders and experts across the healthcare industry spectrum, HITRUST has become a standard for safeguarding and defending PHI from internal and external threats. A 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 (C3) uses a community defense and proactive alerting approach to dealing with the vulnerabilities facing healthcare and protecting PHI against the threat of cybercriminals. Partnerships with HHS and the Department of Homeland Security (DHS) contribute to the strength and efficacy of C3 and further emphasize the importance of healthcare information security.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

Through its efforts to reduce risk, exposure, and the threat to PHI, HITRUST is a federally recognized Cyber Information Sharing and Analysis Organization (ISAO) that has information-sharing agreements with the HHS and DHS. Advancing its protection efforts, HITRUST has partnered with the DHS Automated Indicator Sharing (AIS) Program. Through HITRUST's 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 permits healthcare organizations that use HITRUST 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 the opportunity to address, respond to, and mitigate threats more effectively. This move has had another important effect—it strengthens 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 better. Through relevant, actionable, and educational threat information shared in these briefings, the ability to identify, mitigate, and respond to cyber threats quickly, effectively, and efficiently increases.

Capitalizing on its 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 aims 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 health care. The results and findings of these exercises provide valuable information and insight that applies to CTI coordination, improving C3 efforts, and information sharing among and between health care organizations, government agencies, and HITRUST.

BillingCycle Plus™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

HITRUST is not only setting the standard for healthcare information security and compliance management; their data management tools can save organizations time and money, too. The adoption of AI and electronic health records (EHR) presents a myriad of logistical, security, organizational, and management factors. While the risk to and threat against PHI is a primary concern for organizations, the need for effective data handling measures, in general, is also a concern. The sheer amount of data related to PHI is massive.

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 indispensable to the healthcare industry.

HITRUST tools

performing assessments

organizing and managing audits

handling reporting

tracking compliance

The HITRUST CSF is as adaptable as it is robust. In addition to being scaled to size and type for different 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 keeps users current in their practices and procedures, as well as current with industry and regulatory movements and changes.

One of the most positive effects that HITRUST has had on the healthcare industry is creating a dialogue about healthcare information security and providing an educational platform upon which to build safe standards, establish best practices, address the demands of compliance and risk management, organize and manage data, and safely and more efficiently handle PHI.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

Through this, HITRUST is at the forefront of healthcare cybersecurity, healthcare information security education, and thought leadership. 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, all charged with addressing, identifying, organizing, and managing healthcare information security and privacy challenges.

> "Cyberspace can be a pretty bad neighborhood, with too few barriers standing between hackers and their targets. Healthcare providers recognize that data security is of vital importance to their business."
>
> —Fred Chang, Director of Darwin Deason Institute for Cyber Security Bobby B. Lyle Endowed Centennial Distinguished Chair in Cyber Security at the Lyle School of Engineering, SMU.

Going back to the breaches mentioned earlier, each instance could have been prevented, or at the very least, quickly and efficiently identified and safely remedied with the use and proper utilization of the HITRUST CSF and its programs. The Health Share of Oregon breach that was caused by an employee of their transit vendor could have potentially been avoided if proper physical IT security training was administered to the employee. While theft is sometimes unavoidable, simple steps, including keeping work laptops out of sight and in a locked car, can make all the difference.

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved

With endless features, programs, tools, and knowledge contained in the framework and associated systems, the enacted controls and measures offered by HITRUST can 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. Beyond this, partnering with a third-party medical billing vendor that is a HITRUST partner allows for further benefits beyond billing compliance and enhanced security.

Outsourcing has been found to 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. By implementing enterprise-level security compliance systems and processes via specialized and HITRUST compliant third-party organizations, healthcare organizations can prevent breaches before they occur, protecting valuable PHI while simultaneously improving their overall billing and collection procedures.

PROUDLY **HITRUST CERTIFIED** SINCE 2016

BillingCycle Plus ™ Is a registered TM of MailMyStatements © 2025 | All Rights Reserved