AVERTIUM®

EBOOK

YOUR GUIDE TO HIPAA COMPLIANCE

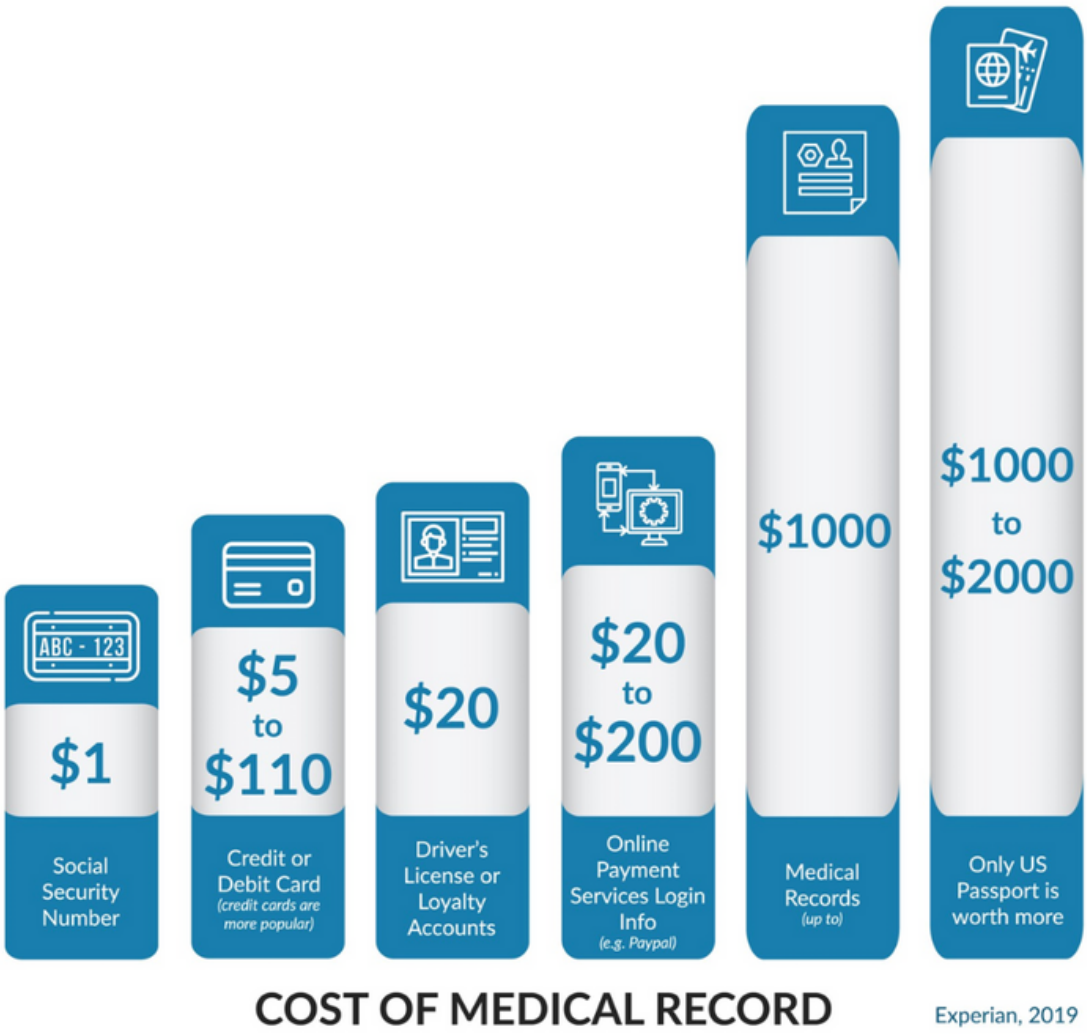
CONTENT

INTRODUCTION TO HIPAA COMPLIANCE

When the Health Insurance Portability and Accountability Act (HIPAA) was signed into law in August of 1996, the intent was to provide an improved method of allowing employees to retain healthcare coverage between jobs, combat waste and fraud in healthcare, and encourage the use of medical savings accounts by offering tax cuts.

The explosive growth of the internet, the digitization of patient medical records, and the resulting vulnerability of these records set a change of course in motion. HIPAA is better known today for setting standards to protect the personal information of patients collected as part of providing healthcare services.

Selling patient healthcare data on the black market has become a lucrative business. Medical record data is worth over 4,500% more on the black market than credit card data. This is mainly due to the nature of the data: A credit card number can be easily changed, while medical record information such as birthdate is persistent. A medical record also contains a significant amount of valuable information, often including credit card numbers, social security numbers, and insurance and policy numbers.



Related Resource: [Why Pen Tests are key to a Robust Incident Response Plan]

THE COST OF A HEALTHCARE DATA BREACH

According to an IBM study, a breach of medical records costs (in USD) increased by 12.3% in the last year of approximately $164 per record in 2022, as compared to $161 in 2021. This equates the total cost of a breach to be over $4 million in 2022. Following an 11-year trend, healthcare organizations have the highest costs associated with data breaches at almost double the cost of the 2nd highest industry (finance).

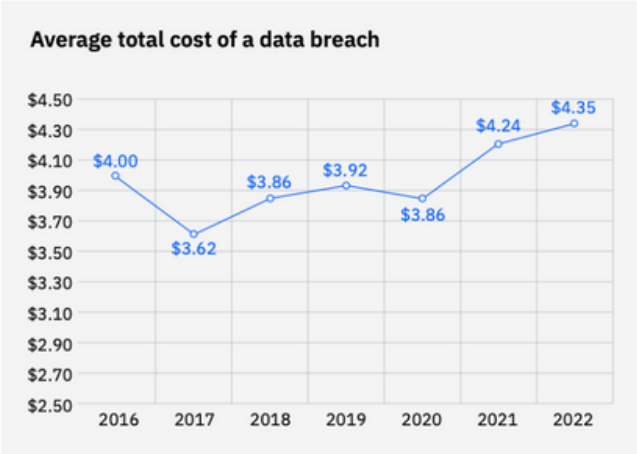


Figure 1: Measured in USD Millions – IBM

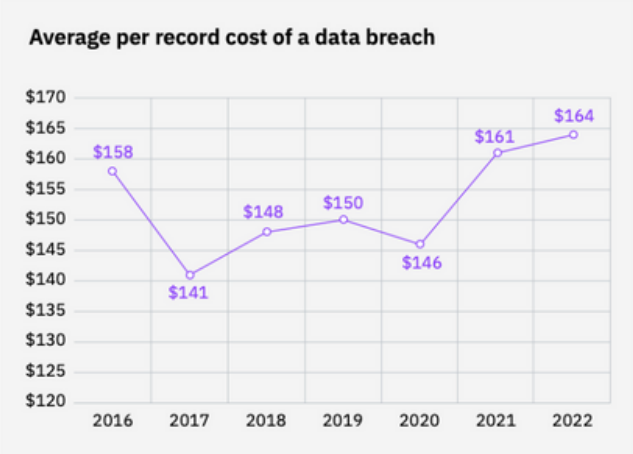


Figure 1: Measured in USD – IBM

HIPAA FINES

Another factor in healthcare data breach costs to consider is fines imposed by the Office for Civil Rights (OCR) at the US Department of Health and Human Services (HHS) which oversees HIPAA compliance. To encourage covered entities and business associates to secure patient data, penalties for HIPAA violations have increased dramatically over recent years.

HHS distinguishes among the nature of fines and applies annual limits according to four penalty tiers: No Knowledge, Reasonable Knowledge, Willful Neglect – Corrected, and Willful Neglect – Not Corrected.

2022 HIPAA Penalty Structure

Penalty Tier	Culpability	Minimum Penalty per Violation – Inflation Adjusted	Max Penalty per Violation – Inflation Adjusted	Maximum Penalty Per Year (cap) – Inflation Adjusted
Tier 1	Lack of Knowledge	$127	$63,973	$1,919,173
Tier 2	Reasonable Cause	$1,280	$63,973	$1,919,173
Tier 3	Willful Neglect	$12,794	$63,973	$1,919,173
Tier 4	Willful Neglect (not corrected within 30 days)	$63,973	$1,919,173	$1,919,173

Source: OCR

The fine range above takes into consideration the inflation rates for 2022. HIPAA will publish an adjusted 2023 penalty table this year with a multiplier of 1.07745.

These numbers don't include the cost associated with losing patient trust. In fact, the lost business cost of a data breach was nearly $1.6 million (38% of the global average of $4.24 million) – each compromised customer record was worth an average of $180.

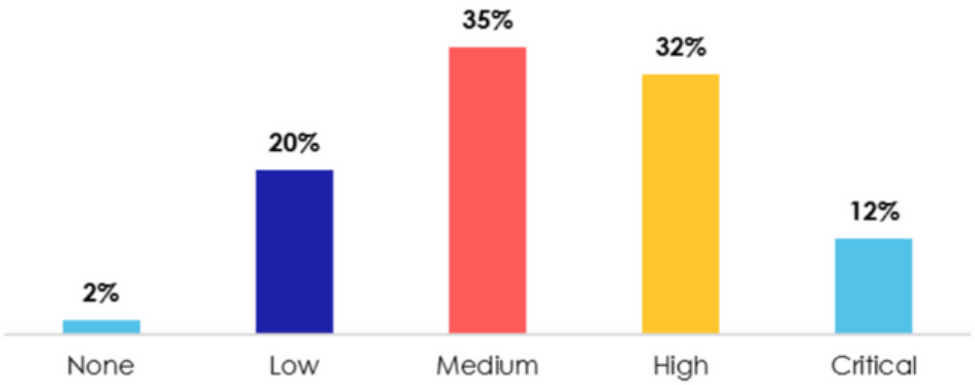
The Department of Health and Human Services maintains the HHS Wall of Shame breach portal that posts all HIPAA data breaches affecting more than 500 individuals per breach. As this demonstrates, a breach can cost an organization not only in penalties and fines, but also severely damage reputation.

Even an alleged breach or frivolous complaint can result in an investigation of your organization by the OCR. From both a legal and brand image standpoint, it's always better to go the extra mile to ensure you comply with any regulation that may be applicable to your organization.

THE THREAT IS REAL

The high value of healthcare records has effectively placed a target on protected health information (PHI). According to the 2021 HIMSS Cybersecurity Survey Final Report, 67% of respondents indicated that their healthcare organizations have suffered significant security incidents in the past twelve months. Depending on the size of the healthcare organization, incidents that qualify as significant attacks range from online scam artists to irresponsible insider activities.

Figure 3: Severity Levels of the Most Significant Security Incident in the Past 12 Months



While attacks on hospitals make for eye-catching headlines, significant breaches and security incidents continue to plague US healthcare businesses and practices of all types and sizes.

YOU'RE NOT ALONE

Regardless of security maturity level, companies often feel as if they are alone in their lack of creating and enforcing effective security measures. But headlines regularly reflect that even large healthcare enterprises are being breached, costing them millions in fines, security upgrades, and settlements. While there is, unfortunately, no shortage of instances on this topic, we've included a few notable significant breaches:

- **February 2014 – Anthem Inc. →** Health insurer Anthem Inc. suffered a massive cyberattack that affected 78.8 million individuals. Separate investigations by both the insurance commissioners' examination team and a third-party security firm determined the breach began when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content. While the commission did not impose fines, it required Anthem to make significant investments in security enhancements to the tune of $260 million.

- **March 2019 – UCLA Health →** Due to a data breach in May 2015, UCLA Health reached a $7.5 million settlement in a class-action lawsuit with the 4.5 million former and current patients affected by a May 2015 health data breach. The information stolen as the result of a year-long hack of the network included names, dates of birth, Social Security numbers, Medicaid or health plan identification numbers, and some medical data. The plaintiffs argued the health system failed to report the breach in a timely fashion. Under HIPAA, providers are required to notify patients within 60 days of breach discovery. UCLA Health also agreed to update its cybersecurity practices and policies.

- **December 2019 – Banner Health →** Healthcare provider Banner Health, the largest single employer in Arizona, was breached in 2016 and in 2023 paid $1,250,000 to OCR and agreed to Implement a corrective action plan. Threat actors accessed the private health data of nearly 3 million individuals over a period of approximately two weeks. Banner Health operates 28 hospitals and specialized facilities in six states, employing more than 50,000 people.

- **April 2022 – OneTouchPoint →** Mailing and printer vendor, OneTouchPoint discovered encrypted files on their systems as a sign of a cyber attack. Initially, the business stated that “only” 1.1 million accounts were accessed, but the latest updates have shown that 2.65 million accounts were compromised in the attack.

WHO MUST BE HIPAA COMPLIANT

Any organization that stores, processes, or transmits protected health information (PHI) is subject to HIPAA regulations, including covered entities as well as their business associates, consultants, and vendors.

Covered Entities

HIPAA regulation defines three types of covered entities: health plans, health care clearinghouses, and health care providers.

Health plans are organizations that provide medical care or pay the cost of providing medical care. This includes health maintenance organizations (HMOs), preferred provider organizations (PPOs), Medicare, Medicaid, company health plans, etc.

Healthcare clearinghouses include any organization that receives data from one healthcare entity in one format (either standard or nonstandard), convert it to another format (nonstandard or standard), and provides it to another entity. Examples include billing services, community health information systems, and any other organization that provides “ services to one or both organizations.

Healthcare providers include anyone who provides healthcare services. This includes everything from preventative care to rehabilitation to pharmaceutical care. Examples include individuals such as doctors, pharmacists, hospice workers, and lab technicians as well as entities such as hospitals, physician practices, walk-in clinics, and nursing homes.

Related Resource: HIPAA Privacy During a COVID-19 Outbreak Re-Occurrence

Business Associates

Business associates are any organization that has a vendor or subcontractor relationship with a covered entity and handles protected health information as part of that relationship. If an organization has access to health information in a digital or physical form or access to systems that generate or store this information, they may be considered a business associate under HIPAA.

THE HIPAA RULES

By enacting the HIPAA law, Congress mandated the establishment of Federal standards to ensure the confidentiality and privacy of PHI. HIPAA is comprised of the Privacy Rule, the Security Rule, and the Breach Notification Rule which collectively mandate how patient privacy should be ensured and how sensitive health data should be protected.

HIPAA Privacy Rule

Established in 2003, the HIPAA Privacy Rule identifies the ways that PHI moves through and is stored within an organization, as well as potential ways by which this information could be revealed to unauthorized parties.

The Privacy Rule requires a comprehensive set of policies and procedures key to an organization s compliance. These set guidelines about how PHI can be disclosed and what is required in a notice of privacy practices.

This is important because it dictates how healthcare providers and support staff interact with you and other providers responsible for your care. For example, the Privacy Rule requires healthcare providers to discretely check patients in for an appointment, ensures only the necessary information for care is provided to other caregivers, and makes sure medical information is shared only with authorized individuals such as approved friends, family, or personal representatives.

A covered entity's workforce members must be thoroughly trained on those policies to ensure they understand how to interact with patients and their sensitive data.

Privacy Officer

HIPAA requires that businesses subject to HIPAA assign at least one person as a Privacy Officer or outsources these duties on a temporary or permanent basis.

The Privacy Officer is tasked with developing and enforcing a HIPAA-compliant privacy program that must include overseeing recurring employee privacy training, conducting risk assessments, and developing HIPAA-compliant policies and procedures as necessary.

Protected Health Information

Key to HIPAA enforcement is determining what qualifies as protected health information. The Privacy Rule defines PHI as "any information held by a covered entity that concerns health status, the provision of healthcare, or payment for healthcare that can be linked to an individual."

According to HHS, protected health information is data, including demographic information, which relates to:

- The individual's past, present, or future physical or mental health or condition
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual

The HIPAA Privacy Rule defines 18 “identifiers”, any combination of which makes healthcare data PHI. This is information that can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

Some modes of these types of PHI are obvious, like the contents of a person’s medical record, lab test results, or medical bills.

However, protected health information also includes:

- Conversations between a patient and their provider about their treatment
- Any medical information stored by the patient’s health insurance provider
- The patient’s billing information

If your organization handles any of these types of information in any form, you may be subject to HIPAA regulations.

Healthcare Information Not Covered by HIPAA – There are some restrictions on data covered by HIPAA:

- HIPAA does not apply to employment or education records
- HIPAA no longer applies to data stripped of all identifiers that can tie the information to an individual, referred to as de-identified PHI

HIPAA Security Rule

The HIPAA Security Rule was enacted in 2005 and applies to health plans, healthcare clearinghouses, and to any healthcare provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the “covered entities”) and to their business associates.

This rule provides guidance on how entities store, transmit, and protect electronic PHI (ePHI), requiring appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of data. To this end, the Security Rule requires a periodic risk assessment of an organization's technical and non-technical safeguards be conducted.

Because the Security Rule is specific to the electronic behavior with which an organization handles PHI, this rule focuses on the implementation and administration of standards as they relate to information technology infrastructure and cybersecurity posture.

While electronic medical records (EMR) enable convenient and speedy sharing of information amongst authorized providers and support staff, accessibility raises the importance of ensuring proper controls are in place around those records and systems to prevent breaches that can result from hacks, ransomware attacks, malware attacks, and shoddy workplace controls such as poor passwords or lack of proper encryption.

Mobile Devices

Mobile devices such as laptops, iPads, and smartphones add complexity to compliance. These devices potentially contain hundreds or even thousands of patient records and can easily be lost or stolen. The Security Rule establishes standards for how covered entities and business associates may use or disclose ePHI through certain types of technology while protecting the security of the ePHI. This rule requires an analysis of the risk the technology poses to the ePHI and the implementation of reasonable and appropriate administrative, technical, and physical safeguards to address such risks.

The OCR and the Office of the National Coordinator for Health Information Technology (ONC) issued guidance on the use of mobile devices and tips for securing ePHI on mobile devices. These offices recommend the following to protect and secure health information when using a mobile device:

- Use a password or other user authentication
- Install and enable encryption
- Install and activate remote wiping and/or remote disabling
- Disable and do not install or use file-sharing applications
- Install and enable a firewall
- Install and enable security software
- Keep your security software up to date
- Research mobile applications before downloading
- Maintain physical control
- Use adequate security to send or receive health information over public Wi-Fi networks
- Wipe the device before disposal or reuse

Security Officer

In addition to a privacy officer required by the Privacy Rule, HIPAA requires that a covered entity or business associate organization assign at least one person as a security officer. For smaller organizations, the same person can fill both roles or the business may outsource the duties on a temporary or permanent basis.

While both compliance officers are responsible for developing security policies, implementing procedures, training, and performing risk assessments, the security officer's focus is compliance with the administrative, physical, and technical safeguards set forth in the Security Rule.

Related Resource: What you need to know about Telemedicine, HIPAA Compliance and the Pandemic

HIPAA Breach Notification Rule

The Breach Notification Rule of 2009 requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information. The HHS defines a breach as the impermissible use or disclosure under the Privacy Rule that compromises the security and privacy of said PHI.

Notification requirements are governed by the number of records. Breaches of 500 or more individuals require immediate notification to the Secretary and a media outlet. Any breach requires notification of the affected individuals.

Following a breach, covered entities must provide notification to affected individuals, the Secretary, and, in certain cases, the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

HITECH

Also adopted in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed. This act provided a vehicle to help and encourage covered entities to computerize patient medical information. HITECH also led to the Meaningful Use incentive program that provided financial incentives to covered entities to move to electronic medical records as well as the Breach Notification Rule. This Act encouraged the use of electronic patient portals, which provide patients a way to view their records and make appointments electronically through a secure portal.

The Final Omnibus Rule

Omnibus Rule was passed in 2013, introducing a few new requirements, but most notably clarifying the vagueness of several areas in the existing rules. The rule also combined HIPAA and HIPAA HITECH under one rule. “Workforce” Notable changes included how to render ePHI unreadable, the definition of who would be considered members, the use of mobile devices in relation to PHI, and managing the use of patient information regarding marketing. One of the biggest changes from the Omnibus Rule was the stipulation that, in addition to covered entities, business associates and subcontractors would also be held responsible for breaches of PHI and business associates must comply with HIPAA.

GETTING STARTED: HIPAA RISK ASSESSMENT

According to the HHS, “Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule.” Therefore, the law requires an annual risk assessment to be completed by all organizations covered by HIPAA.

HHS states the risk analysis process includes, but is not limited to, the following activities:

- Evaluate the likelihood and impact of potential risks to ePHI
- Implement appropriate security measures to address the risks identified in the risk analysis
- Document the chosen security measures and, where required, the rationale for adopting those measures
- Maintain continuous, reasonable, and appropriate security protections.

Related Resource: First HIPAA Risk Assessment? Here's how to be prepared

WHY YOU NEED A HIPAA RISK ASSESSMENT

A risk assessment identifies and documents your areas of risk associated with the creation, storage, transmission, and processing of ePHI in accordance with the HIPAA Privacy, Security, and Breach Notification Rules. The exercise also analyzes the use of administrative, physical, and technical controls to eliminate or manage vulnerabilities that could be exploited by internal or external threats.

Following a risk assessment, the organization must take action to correct any issues that may cause exposure of sensitive data.

The OCR levies fines even for potential breaches of PHI where an OCR audit identifies security weaknesses that could lead to a breach but have not yet been discovered or exploited by an attacker. These fines have been issued if an organization has failed to perform a risk assessment or if the risk assessment performed overlooked these vulnerabilities.

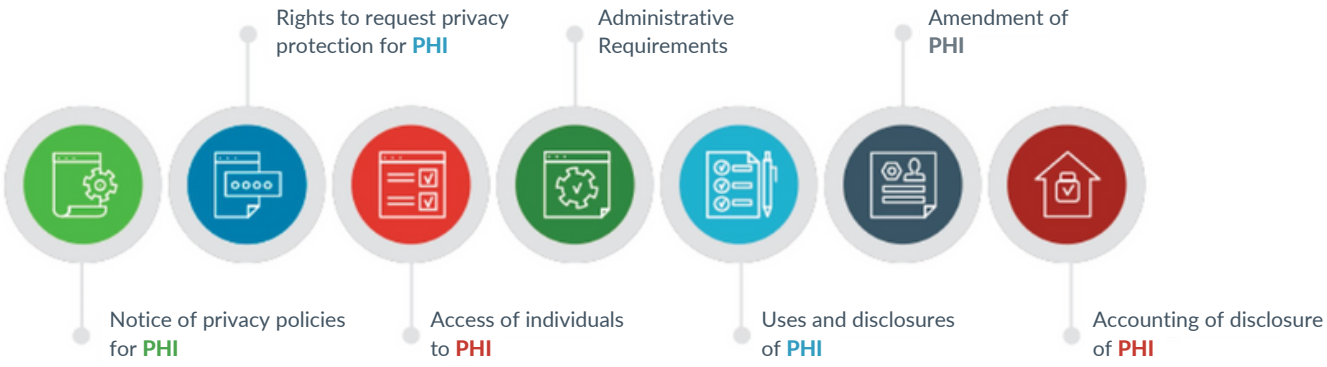
This is why it's important to conduct a thorough risk assessment performed by an informed and reputable professional.

Understanding HIPAA Risk Assessments

When conducting a HIPAA Risk Assessment, it's important to consider the requirements within the Privacy, Security, and Breach Notification Rules.

Privacy Rule Intent and Considerations

HIPAA specifies seven criteria for a risk assessment that complies with the requirements of the Privacy Rule. In order to comply with the Privacy Rule a risk assessment should investigate how the following are managed within an organization:



While performing a HIPAA risk assessment, it is important for the privacy officer to consider all uses of PHI within the organization and how both intentional and unintentional data flows may affect the privacy of patient information.

Related Resource: Does HIPAA apply to me?

Security Rule Intent and Considerations

The HIPAA Security Rule establishes a national set of security standards for protecting health information that is possessed or transmitted in electronic form. The Security Rule does not dictate how organizations implement their security controls but requires them to consider the following as it pertains to their business:

1. Size, complexity, and capabilities
2. Technical, hardware, and software infrastructure
3. Costs of security measures
4. The likelihood and potential impact of risks to ePHI

Affected entities range from the smallest provider to the largest multi-state health plan. Therefore, the Security Rule allows consideration in the most reasonable and appropriate application of security controls. This depends on the organization's size and resources.

That said, no matter how small the practice is, doing nothing is not an option.

Breach Notification Intent and Considerations

Covered entities and business associates must provide the required notifications only if the breach involved unsecured PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the organization shows there is a low likelihood that protected health information was compromised.

A risk assessment ensures the organization has a process in place to properly report in the event a breach occurs based on the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification
2. The unauthorized person who used the PHI or to whom the disclosure was made
3. Whether the protected health information was acquired or viewed
4. The extent to which the risk to the protected health information has been mitigated

Performing a HIPAA Risk Assessment

The ONC and the OCR jointly provide resources for determining if your organization is compliant with HIPAA regulations. The Security Risk Assessment (SRA) Tool provides questions for small and medium-sized practices and business associates to help an organization identify the shortcomings in their security policy. Note, the SRA tool assumes a level of technical knowledge to be effective/helpful.

HHS also publishes an audit protocol that describes the requirements that must be met to comply with the Privacy and Security Rules.

The main difficulty in performing a HIPAA risk assessment in-house is the number and detail of the requirements that must be fulfilled for HIPAA compliance. While these tools can help with identifying shortcomings, it's important to note that they do not help with designing and tailoring a remediation strategy to meet an organization's specific needs.

PREPARING FOR YOUR FIRST HIPAA RISK ASSESSMENT

HIPAA compliance can be a daunting endeavor, especially if your organization has never faced this challenge. If you are facing your first assessment, there are a few things you should know.

Understand Your Security Environment

Prepare for the assessor's visit by gathering information, having the right people available for the engagement, and explaining to your staff what is happening and why it's important to collaborate.

Having the "right" people available depends on the company. Your assessor can tell you the types of positions/people who may be appropriate, but your understanding of your environment in designating these people is key.

Realize it's an Assessment, Not an Audit

Understanding the purpose of an assessment is important in moving forward: It is to help you understand where you truly stand and where your vulnerabilities lie so you can fix them.

This is your chance to discover weaknesses and get clarification from a healthcare and security compliance expert. Your risk assessment is only as good as the information you provide. The more forthcoming and willing you are to work with your assessor, the more productive, accurate, and ultimately valuable your assessment will be.

A good healthcare security consultant works with you as a partner. Be honest and share. Remember, an assessment is a learning exercise. Take this opportunity to understand what your security posture is and where the vulnerabilities are, and to get a plan in place to remediate those problem areas.

Know Where You Stand on Documentation

HIPAA is a legislation that relies heavily on documentation. Therefore, all processes should be documented in a policy and procedure. In addition, all documentation should be straightforward and easily accessible/centrally located.

Conversely, if a process is documented, the organization should be following it in practice. Documenting a process but not adhering to it will be discovered.

Be Patient

Organizations must work diligently toward healthcare compliance. While a HIPAA risk assessment can provide a baseline, very few organizations achieve an acceptable level of compliance with their first attempt. A comprehensive healthcare compliance program provides a roadmap for achieving and maintaining HIPAA compliance long-term.

HIPAA ENCRYPTION STANDARD

HIPAA currently classifies the encryption standard of data at rest (being stored in persistent storage) and in transit (flowing from one point to another) as an addressable implementation specification, not a required implementation.

Does this mean an organization must encrypt their ePHI data?

According to Deven McGraw, former Deputy Director of Health Information Privacy at the Department of HHS, an addressable specification does not mean it is optional.

Simply put, if you encrypt your ePHI data, you're compliant with the HIPAA encryption standard and therefore covered by the Safe Harbor Rule in case of a breach.

Related Resource: 10 Ways Using SIEM Technology can automate fulfilling HIPAA Regulations

Encryption Lessons Learned

MD Anderson Cancer Center at the University of Texas was fined $4.3 million concerning data breaches that resulted in the loss of the health information of 33,500 patients.

These fines relate to incidents in 2012 and 2013, during which MD Anderson suffered three distinct breaches of protected health information. The incidents included the theft of a laptop from an employee's home and the loss of two different USB thumb drives, all containing unencrypted personal health data.

Failure to encrypt mobile devices also recently landed the University of Rochester Medical Center (URMC) in hot water as well. In November of 2019, URMC agreed to pay $3 million to the OCR and to take substantial corrective action to settle potential violations after the university filed breach reports in 2013 and 2017 following its discovery that PHI had been impermissibly disclosed through the loss of an unencrypted flash drive and theft of an unencrypted laptop, respectively.

With more than 26,000 employees, URMC is one of the largest health systems in New York State and includes healthcare components such as the School of Medicine and Dentistry and Strong Memorial Hospital.

Regardless if there was a legitimate business reason for employees to take data home, the laptops and removable media should have been encrypted when not in use and to require a password for access.

Separately, it should be noted that the nature of these incidents also underscores the importance of organizations carefully considering their remote work and mobile device management policies.

Complying with HIPAA Encryption Standards

Encrypting ePHI at rest and in transit may require a change in culture but it serves two purposes: The organization will be compliant with the HIPAA encryption standard and covered by the Safe Harbor provision in the event of a breach. This is because the Breach Notification Rule only applies to unsecured protected health information. Therefore, by encrypting ePHI it becomes secure protected health information.

The best method to ensure you following these steps:

1. Implement encryption on all devices that contain or have access to ePHI
2. Implement encryption for the transmission of ePHI when using unsecure methods such as email and removable media (USB flash drives, external hard drives, etc.)
3. Implement encryption for ePHI data at rest and in transit
4. Stay up to date with current federal and state legislation regarding breach notification requirements including encrypted data
5. Know and follow your corporate policies and procedures

When it comes to HIPAA, "addressable" does not mean "optional". While the encryption standard is classified as an addressable implementation, HIPAA fully expects it to be done.

LOG MONITORING REQUIREMENT

Because healthcare data contains so much personal – and valuable – information, the HIPAA Security Rule requires covered entities to record audit logs and audit trails for regular review.

While HIPAA does not specify the types of data that should be collected, a wider range of information collected provides for more thorough investigation should a security incident occur. That stated, the organization should carefully assess what types of data to store in logs to limit this to relevant information only.

Managed Security Services Providers

Shrinking IT budgets and ever-increasing security threats put many healthcare organizations in a bind. A cost-effective solution to accurately and consistently monitor logs is the use of a managed security service provider (MSSP) to fulfill the log monitoring requirement for covered entities and business associates.

An MSSP can accelerate and simplify HIPAA compliance management:

- Discover IP-enabled assets
- Identify vulnerabilities as a result of missing or unpatched software, a step required under the HIPAA Security Rule
- Correlate security events
- Detect threats already in the network and understand the objectives of those threats
- Help remediate alerts while monitoring and reporting on security controls required for HIPAA compliance
- Assure that all aspects of the company's security and compliance needs are being addressed

GETTING HELP WITH HIPAA COMPLIANCE

Technological advancements related to the creation, storage, and transmission of ePHI often out-pace an organization's ability to ensure the necessary controls are in place to protect patients' information. Most organizations do not have the time, resources, or skill set to ensure their compliance with the HIPAA rules.

HIPAA allows experts external to the organization to complete work on behalf of a covered entity or business associate in order to be compliant.

What to Look for in a Partner

HIPAA compliance and healthcare security consultant firms can provide much-needed expertise and relief, becoming a trusted extension of internal operations. It's important to choose a reputable firm with an extensive history of helping companies to achieve and maintain compliance.

When assessing a consultant or consulting firm, you should look for the following traits:

- Possess a deep understanding of HIPAA to accurately attest to the posture of your organization
- Be willing to spend time getting to know the organization, paying special attention to processes and characteristics specific to the business
- Provide a roadmap to remediation following the completed risk assessment and gap analysis to clarify the discrepancies between your systems and the desired or optimal healthcare security practice or configuration
- Be configured to act as a long-term partner to assist in achieving and maintaining compliance

HIPAA TODAY

HIPAA continues to evolve as new technologies and new breaches occur. The OCR is holding healthcare companies responsible for these breaches to increase and maintain accountability.

Many HIPAA requirements don't specifically state what a company must do. This gives each company some flexibility to do what is best for the organization. While there are no specific mandates, HHS states many times in the rules that a company must do appropriate " to protect PHI.

ABOUT AVERTIUM

Avertium is a cyber fusion company with a programmatic approach to measurable cyber maturity outcomes. Organizations turn to Avertium for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive approach to cybersecurity.

That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. Show no weakness.®

Looking for you next read? Take a look at one of our latest content:

"CASE STUDY: INTERNOVA TRAVEL GROUP"

Have questions? Give us a call.
877-707-7997

www.avertium.com

Arizona • Tennessee