Your Role in Managing HIPAA Compliance

A GUIDE FOR IT PROFESSIONALS

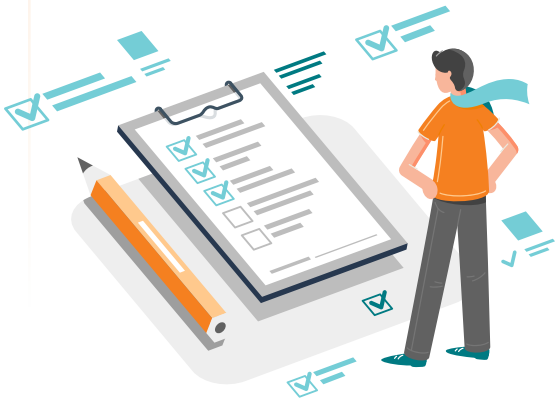
COMPLIANCE MANAGER GRC™
Governance, Risk & Compliance for All

Whitepaper

INTRODUCTION

Whether you are an IT professional working in an IT department or for a Managed Service Provider (MSP), your role is governed by regulations. The Health Insurance Portability and Accountability Act (HIPAA) Security Rule that protects electronic data went into effect in 2005, but small and midsize healthcare organizations are still struggling to comply with the law. They are confused and fear the Security Rule because they don't have the IT knowledge or tools to properly meet the requirements to secure data. Worse, when the Security Rule was written there weren't a lot of medical records – most were paper – and the rule was written before the sophisticated threats that hackers are now using to hurt healthcare organizations. That's why they need you.

This whitepaper covers everything you need to know about your role in managing HIPAA compliance, and how to work with the executives and employees of the Covered Entities and Business Associates – whether you work within the IT department of these organizations, or they represent your clients as an MSP.



Beyond HIPAA, state data breach laws and contracts protect Personally Identifiable Information (PII) including social security numbers, driver's license numbers and financial information that may also be included in an electronic medical record.

WHAT DATA NEEDS IT PROTECTION UNDER HIPAA

The HIPAA Security Rule and Privacy Rule both have IT requirements associated with it, which is why you need to know what kind of data is covered.

HIPAA refers to Protected Health Information (PHI), which includes any written, spoken, or electronic information that is identifiable to a specific patient and contains information about their treatment, diagnosis, or payment for healthcare services.

HIPAA also refers separately to Electronic patient data, (ePHI), which includes electronic medical records, exported PDF files, spreadsheets, emails, medical images, document images, and voice messages.

Organizations that ignore HIPAA do so at their own peril. And if you work within the IT department of one of these organizations – or have them as your clients – the executives need to be made aware that they are running the risk of serious penalties, loss of reputation, and even business closure if they fail an audit or suffer a data breach. And, as the IT person ultimately responsible for data security and privacy, you will likely get dragged into the blame game.

Medical records are targeted by cybercriminals more than other types of data because they contain valuable information that has a long shelf life. Unlike credit card numbers that are quickly cancelled if compromised, medical records include personal and health information that can be used for many years.

HIPAA COMPLIANCE IS SMART CYBERSECURITY: NUMBERS THAT MATTER

With data breaches reaching an all-time high, HIPAA compliance is more than a legal requirement; it is a best practice. Reading about large data breaches of millions of records often makes small medical practices and clinics think that they are too small to be targeted by hackers and regulators. This is a myth considering the number of data breach reports and HIPAA penalties that have affected small practices, including single-doctor practices. This is why compliance must be taken seriously, not only by large enterprises, but also by small and midsize organizations, which often lack the infrastructure to prevent a smaller, though equally crippling, breach and the resources to recover from the resulting setback to the business.

Healthcare data breaches are more costly than other types of breaches. According to the IBM Cost of Data Breach Report, the average total cost of a data breach in the healthcare industry is $6.45 million, 60 percent higher than the global average of all industries combined. The cost per breached healthcare record is $429, almost double the cost for any other industry in the United States.[1]

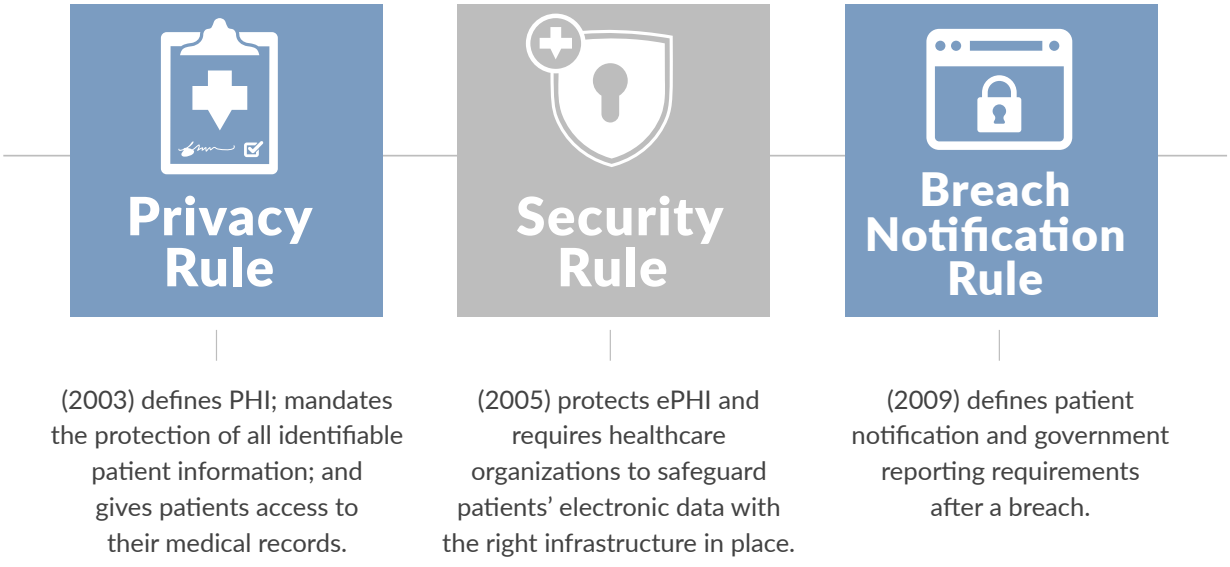
The high costs of breaches are not just fines issued by regulators. Lawsuits, credit monitoring, loss of business, corrective action plans and increased marketing costs to recover the organization's reputation, all add up quickly.

This white paper walks you through HIPAA's evolution, why it matters, and how you can leverage your experience and specialized tools to help healthcare organizations and the businesses that serve them remain secure and HIPAA compliant.

A BRIEF HISTORY OF HIPAA

Initially signed into law to improve portability and accountability of health insurance coverage for employees moving between jobs and to eliminate health insurance fraud, HIPAA has evolved into the regulation that protects patient privacy and a patient's right to access their health information.

HIPAA is separated into three rules:



In 2013, the HIPAA Omnibus Final Rule made changes to the original rules.

HIPAA is enforced by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). All 50 state attorneys general can enforce HIPAA. Failure to comply with HIPAA guidelines has resulted in significant financial penalties and expensive damage to reputations. The U.S. Department of Justice prosecutes criminal violations of HIPAA.

Complying with HIPAA is also tied to financial incentives for healthcare providers that bill Medicare, through the Merit-based Incentive Payment System (MIPS). This ties HIPAA to Medicare payments, meaning that failure to comply can be considered Medicare fraud.

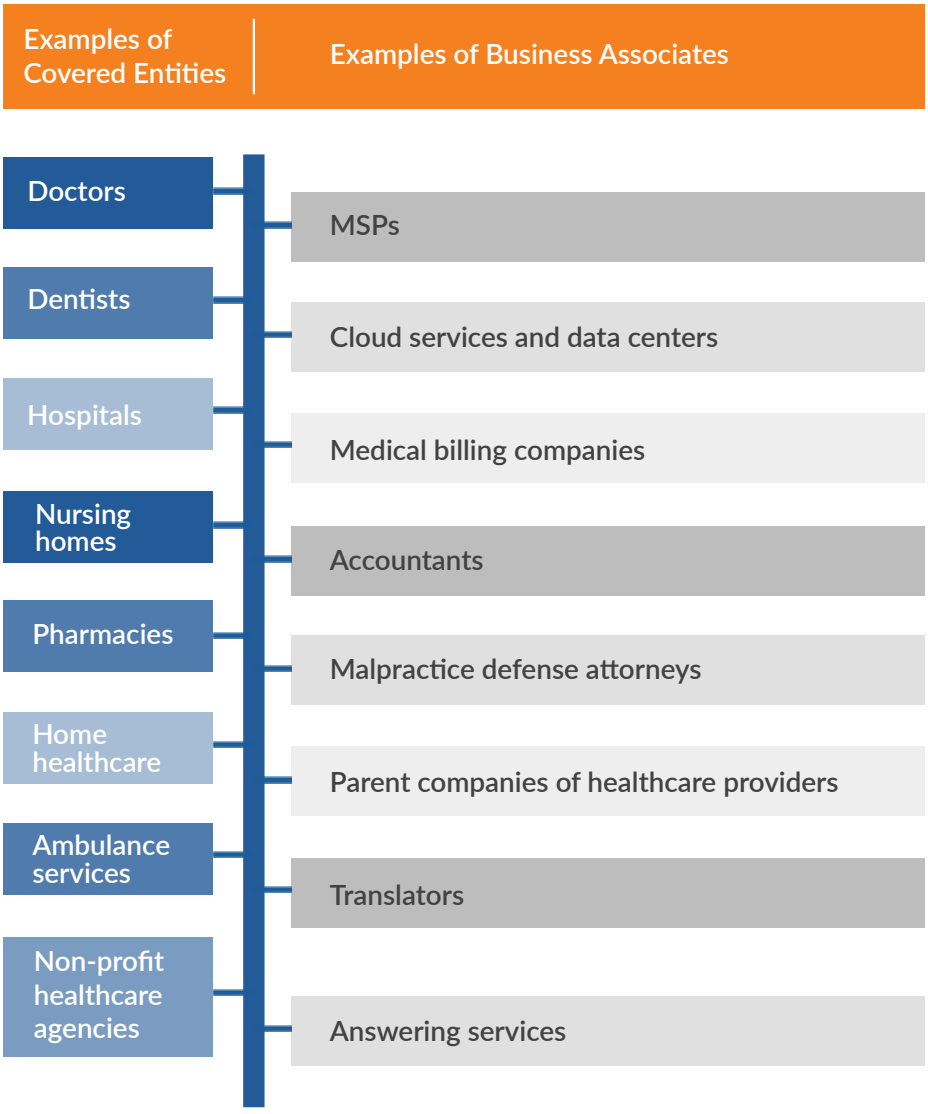
Compliance is not a one and done exercise. Like your health, which can change without warning, an organization can be compliant one day and the next day develop hidden risks and compliance violations.

WHO IS COVERED BY HIPAA?

HIPAA does not apply to medical records everywhere. It applies to Covered Entities — healthcare providers that bill Medicare, Medicaid and health plans, and those health plans that pay for care. It also applies to Business Associates — vendors that support healthcare providers and health plans and come in contact with PHI or the systems that store or process it. Business Associates must sign Business Associate Agreements (BAAs) and implement a program to comply with the HIPAA Security Rule.

Cash-only and free medical organizations do not have to comply with HIPAA. However, state data breach laws and professional license requirements require these organizations to secure their patient information at the same level as HIPAA.

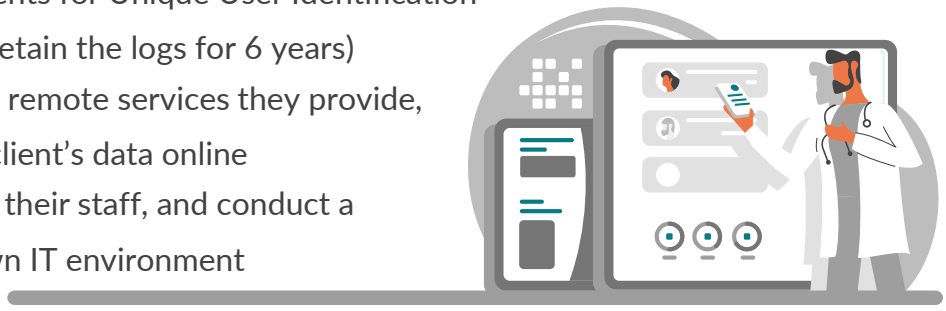
The federal government expects Covered Entities and their Business Associates to be fully compliant with the rules. Further, if Business Associates work with downstream vendors to support their clients, those vendors too must comply with HIPAA. Simply put, any entity involved in creation, storage and use of patient's health information falls under HIPAA requirements.



THE IT VENDOR'S RESPONSIBILITY TOWARD HIPAA COMPLIANCE

If a Business Associate's network is compromised then, access to their clients is also compromised. Business Associates must:

- ☑ Sign BAAs and implement a compliance program, including a full set of policies and procedures
- ☑ Limit access to any PHI their technical team can reach at a client site
- ☑ Comply with HIPAA's requirements for Unique User Identification and logging all access to ePHI (retain the logs for 6 years)
- ☑ Protect the logins and access to remote services they provide, such as accessing a healthcare client's data online
- ☑ Provide basic HIPAA training to their staff, and conduct a security risk analysis of their own IT environment



These requirements include:

- ☑ **Physical security:**
  Ensuring only authorized personnel access their premises. Additionally, they must be vigilant about protecting your endpoints as well as storing, transferring and disposing PHI and ePHI data.
- ☑ **Policies & Procedures:**
  Having written HIPAA policies and documented procedures to ensure ePHI remains fully protected in accordance with each section of the Security Rule.
- ☑ **Storage:**
  Installing a strong backup system and testing the backups to ensure patient information is restorable.
- ☑ **Access control and safeguards:**
  Establishing strong access controls (e.g., user privileges, policies, or authentication) to ensure only authorized users with HIPAA training can access data.
- ☑ **Auditing:**
  Auditing clients' HIPAA operations with full reports and log files to identify security problems and ensure they do not reoccur.
- ☑ **Network security:**
  Ensuring their networks are fully secured and cannot be breached. This means preventing unauthorized users from accessing networks and having all checks and balances in place to protect data (including encryption).

At the outset, working with healthcare data might seem challenging but the potential opportunity is huge. The healthcare market is ever-growing and presents numerous lucrative job opportunities for IT professionals and revenue channels for a savvy MSP looking to ensure its healthcare clients stay ahead of the curve.

Kaseya's 2020 MSP Benchmark Survey, for example, found over 39% of American MSPs had difficulties with HIPAA compliance. At the same time, 52 percent of respondents did not offer assessment services.[2] Offering compliance-related services would benefit healthcare compliance clients as well as provide an additional revenue stream for the MSP.

NON-COMPLIANCE IS EASY, BUT COSTLY

In early 2021, Excellus Health Plan agreed to a settlement totaling $5.2-million after an investigation uncovered multiple HIPAA violations, including the failure to conduct an accurate and thorough organization-wide risk analysis.

Other notable penalties

Cottage Health paid over $9 million because their server was accessible on the internet. A security configuration setting within their operating system allowed access to ePHI files without asking for a username or password. They had not signed a BAA with their IT provider nor had they conducted a thorough and accurate security risk analysis. **Worse, their insurer refused to pay the $3 million federal fine, a $2 million state penalty and a $4.1 million lawsuit settlement** with patients because they said Cottage Health was not compliant with its cyber insurance policy.

Tennessee Medical Imaging (Touchstone) paid **$3 million for exposing over 300,000 patients' health information**, as one of their servers permitted uncontrolled access to patients' data. They had not signed a BAA with their IT support provider or third-party data center, nor had they conducted a thorough and accurate security risk analysis.

Medical Informatics Engineering (Indiana Medical Records Service) paid $100,000 because hackers used compromised user credentials and accessed ePHI for about 3.5 million patients. They had not conducted a thorough and accurate security risk analysis.

The complete list of penalties, which is quite lengthy, can be found on the HHS website.

Major healthcare organizations are aware of HIPAA and go to great effort to remain compliant. They have the staff and budget to stay up to date and protect themselves.

In contrast, smaller businesses tend to have fewer resources at their disposal and are less aware and up to date on the risks involved and substantial penalties for non-compliance.

In addition, a bigger enterprise is likely to recover more easily from a setback. A smaller company will feel the impact more acutely, and proportionately suffer greater financial damage and setback to its reputation.

More than being financially devastating, a HIPAA fine can ruin the trust between doctors and patients – often a real business crusher. HIPAA applies to medical data, but other laws protect confidential personal information, which is a goldmine for hackers. Patients' social security numbers, date of birth, driver's license information and other details can lead to easy identity theft and are sold at a premium by criminals on the Dark Web, breaking the trust between patients and their healthcare provider.

HOW TO BE A TRUSTED TECHNOLOGY ADVISOR

As an IT professional working in an IT department or for an MSP, if you provide HIPAA compliance services people view you as more than a technician. You are a trusted partner who helps them protect their reputations and financial resources. Fulfilling this crucial responsibility means ensuring your organization or clients never have to fret over data security and compliance, as mandated under HIPAA. And, as a side benefit, your business will be better protected as well.

Let's look at how you can set this in motion.

Ask the right questions

Being a trusted advisor means having all critical information at hand. This begins with asking the right questions. **The very first question you should ask is:**

> ***Have you fully implemented a documented program that aligns with all the requirements in the HIPAA Privacy, Security and Breach Notification Rules?***

Other questions to continue the conversation include:

- ☑ Do you have a documented HIPAA compliance program with implemented policies and procedures?
- ☑ Do you have recent reports from network scans to prove your security controls have been implemented properly and are still working?
- ☑ Do you have recent reports showing where all your PHI and PII are across your network?
- ☑ Are your employees aware of the penalties that result from security violations?
- ☑ Are internal penalties in place for employees who violate security procedures?
- ☑ Do all of your users know what to do in the event of security incidents or issues?
- ☑ Is a process in place to document, track and address security issues or incidents?
- ☑ Is anyone tasked with checking all security logs, reports and records?
- ☑ Have you appointed a security official to ensure policies and procedures are followed?
- ☑ Do you have a thorough and accurate risk analysis that will survive an audit or data breach investigation?

Training is a Must for Your Staff and Your Clients

While technical tools can help prevent many types of incidents, end-user training is critical to help avoid mistakes, e-mail fraud attacks, ransomware, and accidental loss of data.

The right knowledge remains core to a systemic approach to ensure HIPAA compliance. In addition to offering the appropriate technical services, you can help with the necessary knowledge to make the best of the solutions.

For example, end users with access to healthcare data must understand the proper use of passwords, their complexity, and the importance of implementing multi-factor authentication.

End users should be trained to recognize and avoid phishing emails that could result in a ransomware attack, which could be very expensive and is a reportable breach under HIPAA.

Establish Administrative Safeguards

Establishing yourself as a trusted advisor requires that you have administrative safeguards – the written procedures and policies that help prevent security violations or breaches. You also need comprehensive contingency plans and a facility security plan. **A minimal checklist of administrative safeguards includes:**

Performing a thorough and accurate security risk analysis

Developing a risk management plan and mitigating the identified risks

Designating a security official responsible to oversee policies and continuously update them

Defining how access reports, audit logs and incident tracking are handled

Document Everything

Regulators demand written reports and other documents validating that a HIPAA compliance program has been fully implemented. Simply taking the correct steps isn't enough. You need recent documented Evidence of Compliance if you are going to survive an audit or a data breach investigation. The documents should be able to prove the steps taken to identify and mitigate security risks.

As a trusted advisor, you can support your organization or clients by providing current Evidence of Compliance for them to have in case they are audited or investigated. This can help prevent fines for Willful Neglect – knowing you must comply but not having the evidence to prove you did so.

You Could be Your Organization's or Clients' Best Defense in the Case of an Audit

Most smaller healthcare organizations do not have internal IT departments, so MSPs should emphasize their professional experience and credentials, much like their clients do when advertising for patients.

According to Mike Semel of Semel Consulting, "When it comes to surviving a HIPAA audit or data breach investigation, you need a professional. Like the specialists that doctors refer patients to every day, and the tests that they order to see what is happening under a patient's skin, your technology must be evaluated by someone with the proper skills and experience, who must look deep into your network to identify its strengths and weaknesses. Make sure they understand the HIPAA compliance requirements you face.

According to Mike Semel of Semel Consulting, "When it comes to surviving a HIPAA audit or data breach investigation, you need a professional. Like the specialists that doctors refer patients to every day. Your technology must be evaluated by someone with the proper skills and experience, who look deep into your network to identify strengths and weaknesses."

Most larger organizations have internal IT departments that can benefit from an independent risk analysis to get an independent assessment of cybersecurity and compliance, without the risk of fines when gaps are identified.

How to Implement the HIPAA Security Rule Requirements

The Security Rule can be confusing because it designates some items as “required” and others as “addressable.” It states:

> ***In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification:***
>
> - Implement the addressable implementation specifications
> - Implement one or more alternative security measures to accomplish the same purpose
> - Not implement either an addressable implementation specification or an alternative

In recent years, regulators have changed the way they enforce requirements, considering the changes to technology and the ever-growing threats from sophisticated hackers. For example, Encryption is an example of addressable security control. The catch is that, to date, whenever an organization has lost unencrypted data, the incident proved that the alternative protection was not as effective in protecting data as encryption.

This is why encryption is the only reasonable and viable way to meet HIPAA requirements that ePHI always be protected.

Ultimately, it is best to consider all addressable items as required.

LEVERAGE TECHNOLOGY TO ENSURE HIPAA COMPLIANCE

Ensuring HIPAA compliance is more than a one-and-done exercise. It requires repeated monitoring of all the administrative, physical and technical controls to ensure consistent security and compliance efforts.

An IT Security Risk Analysis is the First Step in HIPAA Compliance

Regardless of how a healthcare organization handles its HIPAA compliance, an IT security risk analysis is essential. Not having an 'accurate and thorough' HIPAA Security Risk Analysis is the most-cited root cause for HIPAA data breaches.

Many vendors offer self-help tools and questionnaires for healthcare organizations to use to perform their own risk analysis. Some vendors call providers and complete a questionnaire over the phone or through a web portal. That's like your doctor just asking you questions instead of doing blood tests and medical imaging to determine your health needs.

The only way to conduct a thorough and accurate IT security risk analysis – the standard that is not met in many multimillion-dollar penalties – is with the right technical assessment tools operated by trained IT professionals.

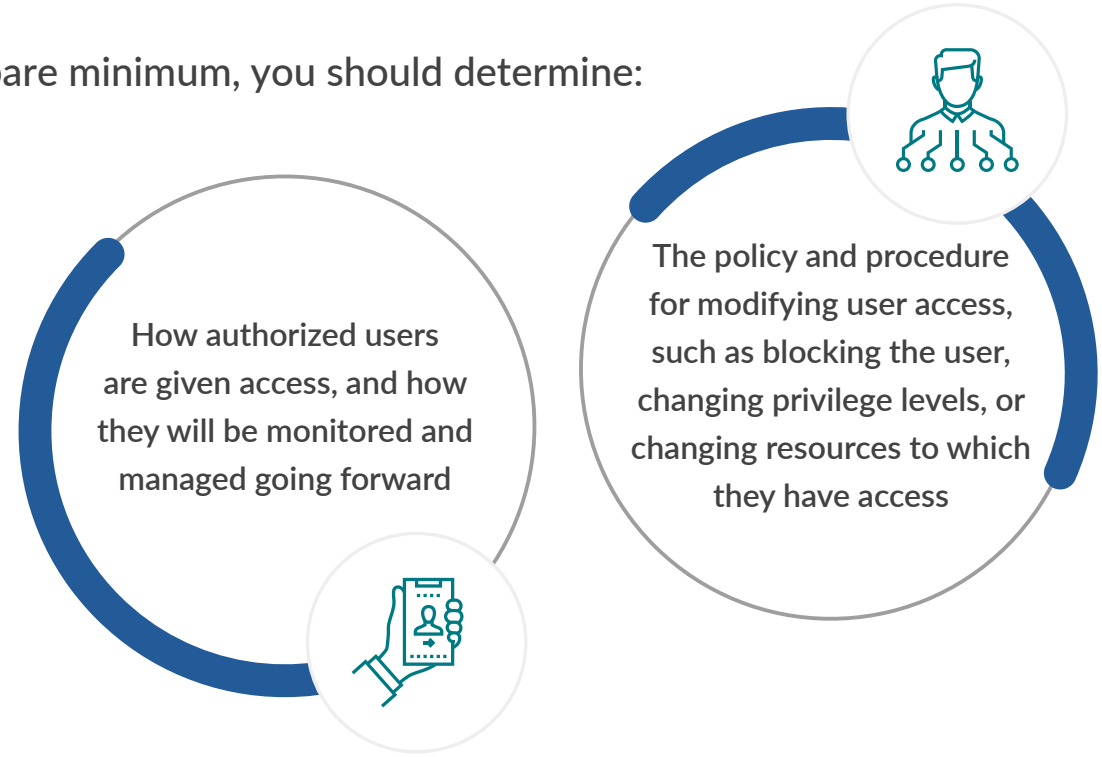
The risk analysis should cover:

An "under the skin" analysis by a trained IT professional
of vulnerabilities, risks and system threats to ePHI
A plan for protecting and securing ePHI regardless of location

Access Safeguards and Controls Require a New Approach

The crux of HIPAA compliance is ensuring that ePHI and the systems that store it can be accessed by only those with the proper authority. Written policies and procedures for information access management are key to locking down unauthorized access to ePHI and other confidential data and to survive a HIPAA audit or data breach investigation.

At a bare minimum, you should determine:



Functionality like single sign-on (SSO and multi-factor authentication (MFA can help keep the doors shut for any intruder. For example, MFA asks end users to validate their identity beyond a password – through a fingerprint, authenticator app, or code that only the authorized user would know.

Say No to Free Web Mail and Yes to Firewalls

Free web mail is tempting. It's easy to set up, and messages can be sent from almost any device. However, free web mail is a big HIPAA no-no. HIPAA demands email to be encrypted from end-to-end and backed by a vendor with which a BAA has been signed. Firewalls with active intrusion prevention systems are also required.

Think this isn't a big issue? Neither did Idaho State University (ISU. The OCR found that medical records for 17,500 patients at ISU were not secure because the ISU firewalls were disabled for close to a year. The fine? $400,000.[3]

The Importance of Encryption

HIPAA requires that ePHI be encrypted at rest (stored on a device) and in-transit (across a network, the internet, or in an email or text message).

HIPAA and various state data breach laws exempt encrypted data from being reported if lost or stolen.

You are in an ideal position to keep healthcare data safe with encryption, both at rest and in transit between end users, and to provide reports that substantiate a healthcare organization's decision not to report a lost or stolen encrypted device.

Develop a Security Incident Response Plan

Security breaches do not come with advanced notification. A Security Incident Response Plan (SIRP) documents steps to be taken in case of a security breach or any other security event. The plan needs to include the required steps to determine if an incident is a breach that requires patient notification and government reporting. State laws and contracts also need to be considered.

Implement the NIST Cybersecurity Framework (CSF)

In 2021, a new HIPAA law was passed providing relief from HIPAA audits and penalties for organizations that can prove they have implemented the NIST CSF for the previous 12 months. The NIST CSF includes 98 security controls that, if implemented and documented, can provide relief from regulators and protection against lawsuits and insurance claim denials.

HHS does not recommend a particular approach – "In order to maintain a flexible, scalable and technology neutral approach to the Security Rule, no single method is identified for addressing security incidents that will apply to all covered entities."

However, by leveraging the right technology and implementing the NIST CSF, you can help your organization or clients with plans to quickly determine that a breach has occurred and help your clients meet the strict deadlines associated with a breach.

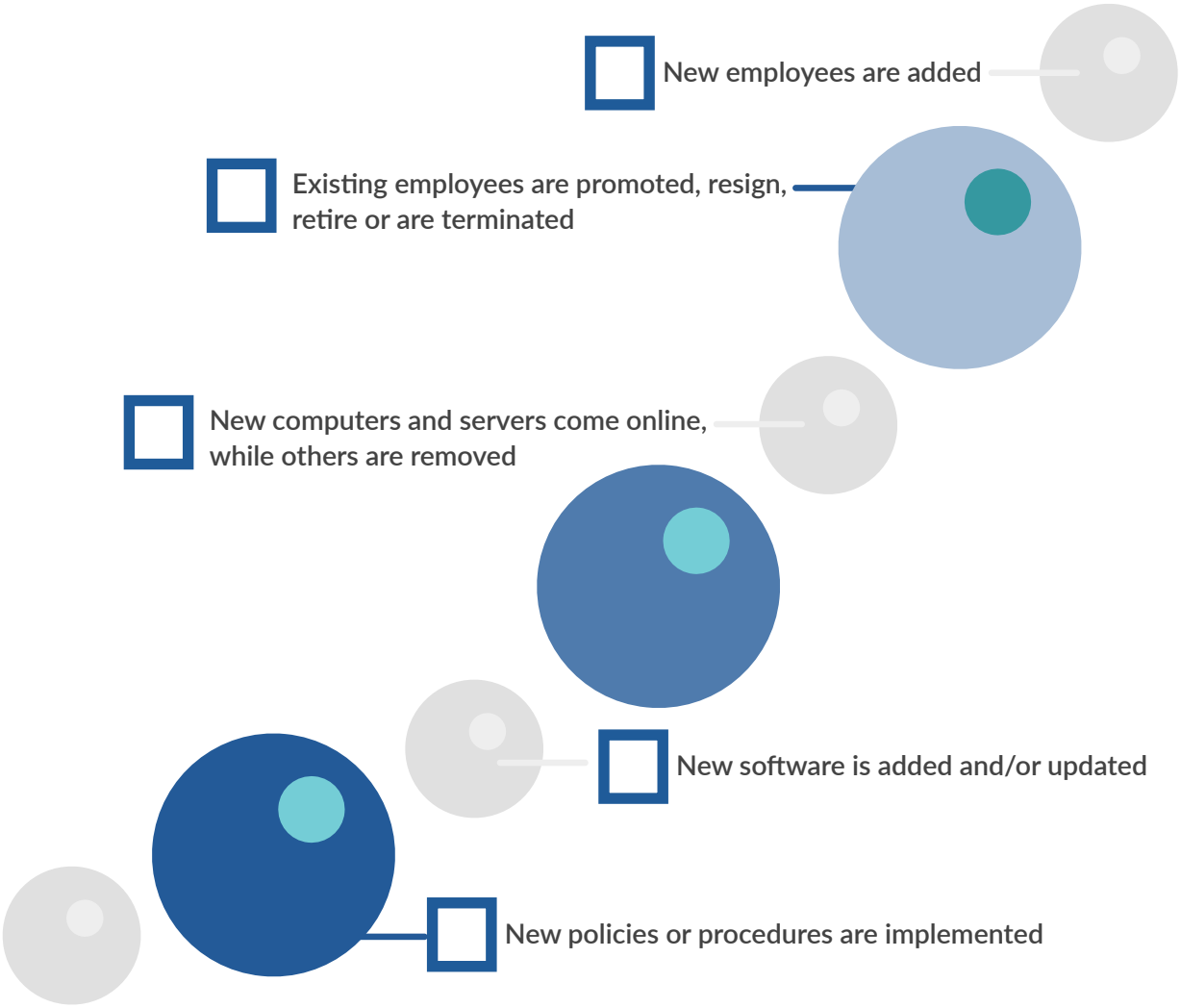
HIPAA-Mandated IT Risk Analyses Made Easy

While there are free check-list products and manual data collection tools available, Kaseya has developed a software solution purpose-built to help deliver and automate the kind of HIPAA assessment and HIPAA compliance services that will make you that trusted technology advisor.

Compliance Manager GRC is optimized to perform ongoing HIPAA compliance – including the critical Security Risk Analysis. It combines automatically collected network data with information gathered through observations, training sign-in sheets, and surveys to produce all of the documents necessary to deliver an IT security assessment that meet the HIPAA requirements.

An easy-to-deploy and affordable solution, it does the heavy lifting (including collating the necessary and affordable solution, documentation) to ensure your healthcare clients meet the HIPAA Security Rule annual assessment requirements.

But compliance is not a one-time, annual necessity. You can be compliant with the HIPAA regulations today, but quickly become out of compliance as the environment changes and evolves:



That's why you should implement a compliance process automation platform that will allow you to deliver ongoing Compliance-as-a-Service. This will also cement your position as a trusted technology advisor.

Compliance Manager GRC is a web-based platform that includes a workflow automation engine, taking the guesswork out of Compliance-as-a-Service. It is a role-based solution that allows stakeholders to participate in the process, while establishing you as the technical expert. With **Compliance Manager GRC** you can easily set up recurring HIPAA assessments at key intervals, and automatically produce updated management plans and Evidence of Compliance.

CONCLUSION

Because every state has a data breach rule, every organization is mandated to comply with at least one set of security or privacy guidelines, and at times more than one. HIPAA's requirements overlap with many of these state laws, and then takes things to the next level.

For most healthcare organizations and their vendors, ensuring compliance with HIPAA guidelines is tedious, confusing and downright frustrating.

You are in a unique position to assist with managing the entire compliance process – from assessing needs to ensuring every detail is in place, leveraging the technology at your disposal.

With this, you will bring not only peace of mind, but also a significant boost to your own standing in the company.

To learn how you can ensure HIPAA compliance isn't a thorn in your side:

Request a Compliance Manager GRC demo

or visit our website at:

https://www.compliancemanagergrc.com/

Sources

1. 2019 IBM Cost of a Data Breach Report
2. Kaseya 2020 MSP Benchmark Survey
3. U.S. Department of Health & Human Services website