HIPAA survival guide

How compliant is your organization?

WHITE PAPER

hexnode

TABLE OF CONTENTS

1

How vulnerable is the healthcare industry?

To answer that question, let's take a look at the statistics.

According to the US Department of Health and Human Services data breach portal, over 40 million records have been stolen in 2021 exposing a multitude of private details of the affected patients.

Details such as their social security number, patient records and financial data were exposed from a ransomware attack.

The healthcare industry has always been a popular target for cybercriminals. Unlike most other industries, a data breach within the healthcare industry does not only lead to the loss of critical data from systems and applications but also negatively impacts vulnerable people whose sensitive health information is held at ransom and exposed to unauthorized parties.

Health records continue to be a target for cybercriminals. The evolution of the cybersecurity threat landscape makes it harder for healthcare organizations to stay updated with the implementations they need to carry out to ensure all data falling under their purview stays protected from a wide range of threats and vulnerabilities.

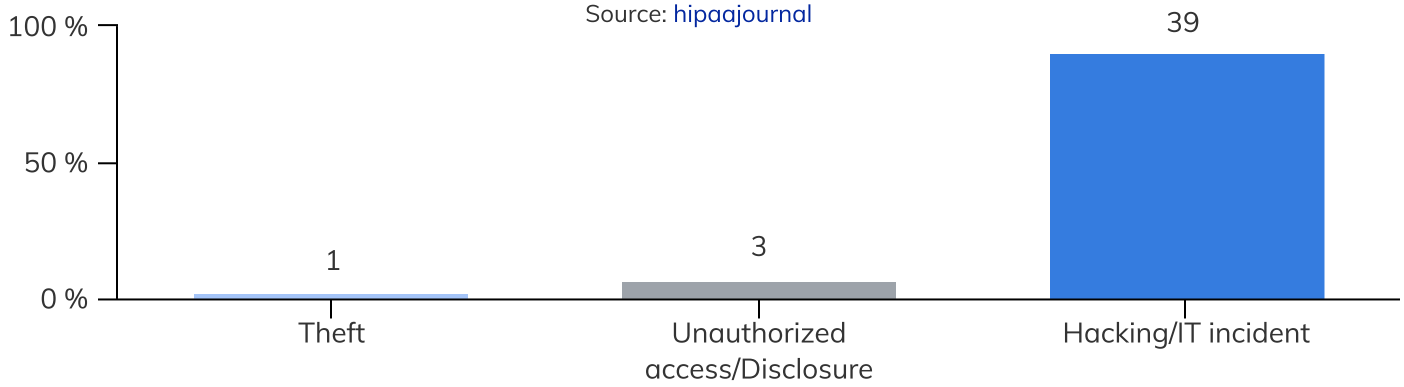
RECENT STATISTICS AND FIGURES

Monthly breach report – March 2022

The US Department of Health and Human Service’s Office for Civil Rights (OCR) reported 43 healthcare breaches of 500 or more records. The leading cause of those breaches was hacking.

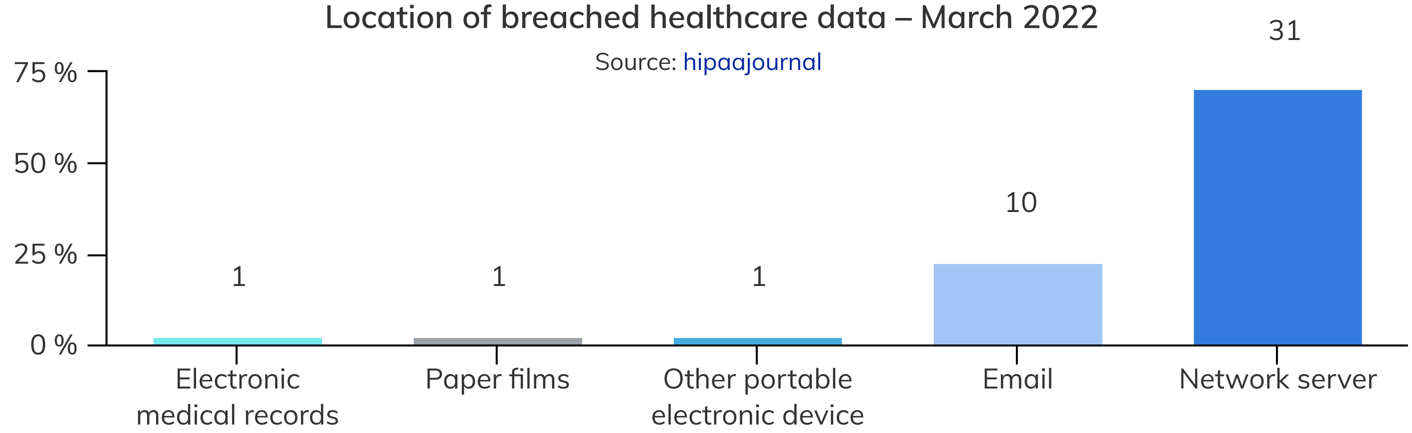
Cause of healthcare breaches – March 2022

Source: hipaajournal



Location of breached healthcare data – March 2022

Source: hipaajournal

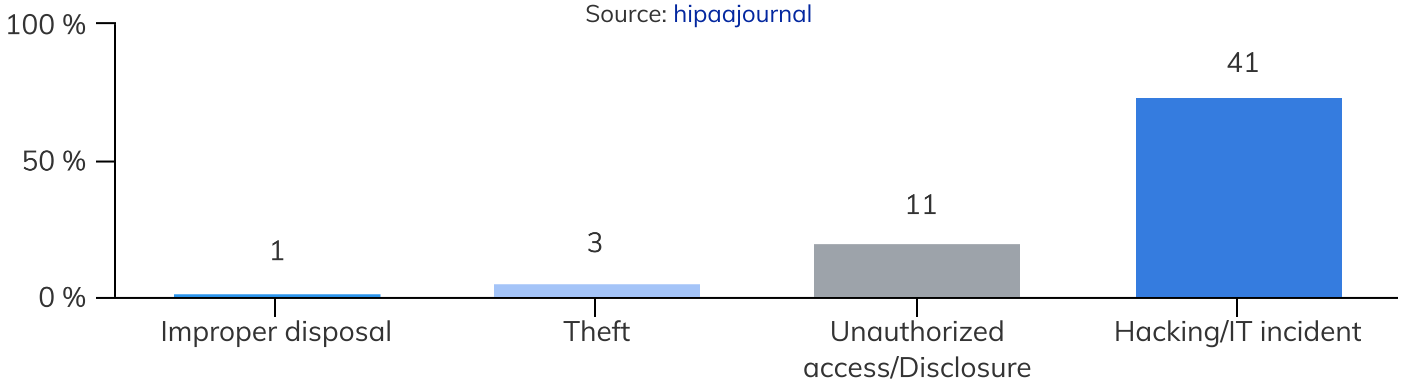


Monthly breach report – April 2022

April recorded a 30.2% increase in reported data breaches in the past four months. 56 data breaches out of 500 or more records was reported by the OCR in April 2022. The average breach size recorded this month was 38,575 records and the median breach size was 6,546 records.

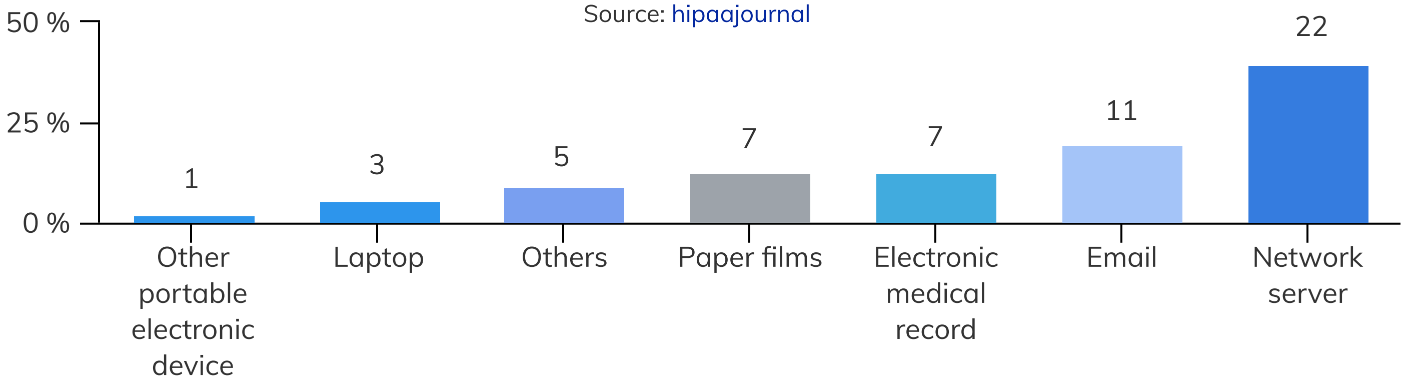
Cause of healthcare breaches – April 2022

Source: hipaajournal



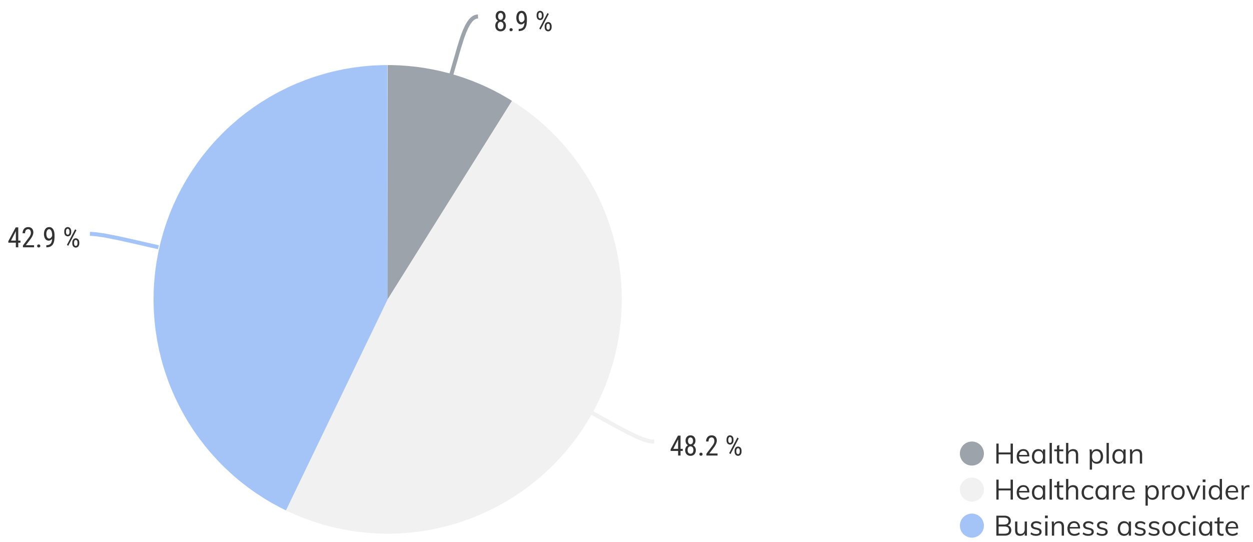
Location of breached healthcare data – April 2022

Source: hipaajournal



Data breaches by entity type

Source: hipaajournal



2

What is HIPAA? How does it help in ensuring protection of ePHI

HIPAA incorporates the requirements of other legislative acts such as the Public Health Service Act, the Employee Retirement Income Security Act, and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

HIPAA was introduced in 1996 by the United States Congress to ensure people out of work could still be covered by healthcare benefits. It also sets the guidelines Covered Entities need to implement to protect sensitive healthcare information. Healthcare organizations are always under the threat of hackers selling sensitive data to make a substantial amount of money.

HIPAA was responsible for introducing various standards for safeguarding the protected healthcare information and ensuring the safe transfer of healthcare data between Covered Entities and Business Associates. It helped reduce the sheer amount of paperwork by automating several processes within organizational workflows.

RULES OF HIPAA

The rules of HIPAA define the various security measures organizations need to take up to ensure data security and to have an adequate responsive framework when data breaches occur. These include:

- **Privacy Rule** – it defines what constitutes a Protected Health Information, and the responsibilities Covered Entities and Business Associates hold in protecting the patient data they handle. It also mandates that only a minimum amount of data should be handed over to third parties to complete the task they are assigned to.
- **Security Rule** – it sets the guideline on the minimum physical, technical and administrative safeguards Covered Entities need to implement to protect electronic Protected Health Information (ePHI).
- **Breach Notification Rule** – it documents the procedures that should be followed after a breach has occurred to ensure the breach does not cause further damage to affected patients.
- **Enforcement Rule** – it consists of the fines and other penalties that can be imposed on a Covered Entity in the event of a data breach.
- **Omnibus Rule** – it addresses privacy on multiple areas such as the length of time in which patient records need to be maintained to the requirements of encryption needed to protect the Protected Health Information.

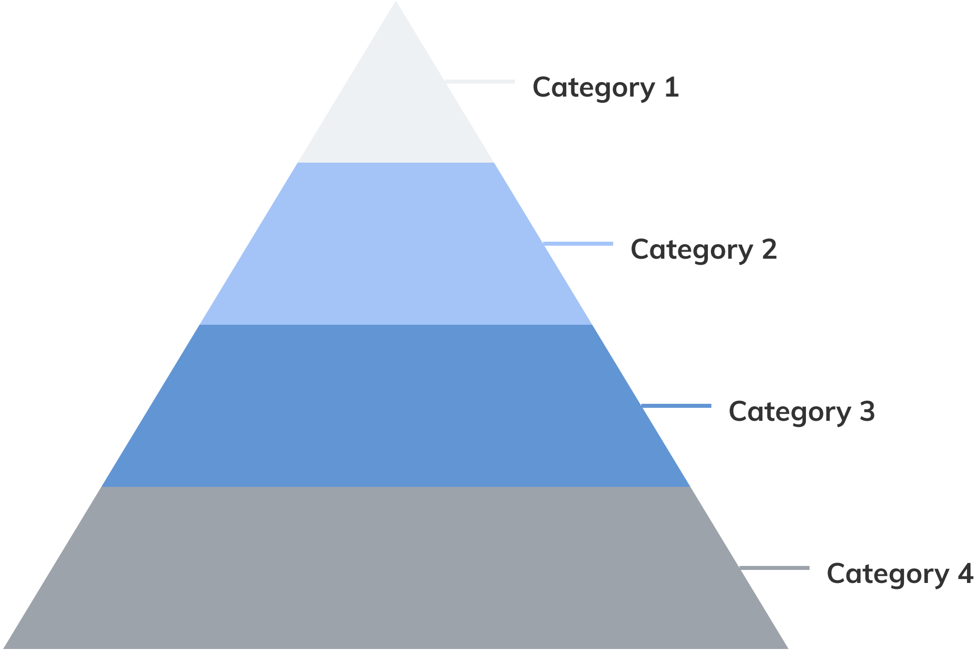
ARE HIPAA TRAININGS REQUIRED?

Employee training is mentioned within the Administrative Requirement of the HIPAA Privacy Rule and the Administrative Safeguard of the HIPAA Security Rule. The main purpose behind these training sessions is to make employees aware of the responsibilities they hold in safeguarding data and being aware of the multiple safeguards taken up by the organization.

Employees should be properly communicated on about the consequences of the data breaches and the financial implications it could have over on the organization.

WHAT ARE THE HIPAA VIOLATIONS?

Cost of HIPAA violations is high. The HIPAA violation structure can be broken down into multiple levels.



- **Category 1:** the Covered Entity was unaware of the violation and thus could not have taken steps to avoid it. They will be advised to take more care to follow the HIPAA rules.

  Potential fines: *minimum fine of $100 per violation up to $50,000*

- **Category 2:** this consists of violation that the covered entity should ideally be aware of but could not have implemented the measures needed to avoid it.

  Potential fines: *minimum fine of $1,000 per violation up to $50,000*

- **Category 3:** violation occurred due to the willful neglect of the HIPAA rules. Attempts have been made to rectify the violation.

  Potential fines: *minimum fine of $10,000 per violation up to $50,000*

- **Category 4:** violation occurred due to the willful neglect of the HIPAA rules. No attempts have been made to rectify the violation.

  Potential fines: *minimum fine of $50,000 per violation, maximum $1,50,000*

3

How to get your organization HIPAA ready

HIPAA compliance can be a complex and exhausting process that even the biggest organizations may face troubles with. Many businesses are still in the process of finding the right policies to stay in compliance with HIPAA guidelines.

This section focuses on the processes and safeguards one must take into consideration to become HIPAA compliant.

The HIPAA security rule requires Covered Entities and Business Associates to implement multiple processes and measures to improve the overall security of the organization and ensure the complete protection of electronic Protected Health Information (ePHI).

The safeguards are split into three. These include:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

ADMINISTRATIVE SAFEGUARDS

This is the overarching term that involves all the processes, procedures and policies involved in ensuring the confidentiality, integrity and availability of ePHI and to protect the data from any data breaches or disclosure.

The administrative safeguards defined within the HIPAA security rule include:

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plan evaluation
- Business associate contracts and agreements

The administrative safeguards consist of over half of HIPAA security requirements. In order to check whether your organization is compliant with the administrative safeguards, you will have to evaluate your existing security controls and do a proper risk analysis.

Security management process

This section requires Covered Entities and Business Associates to implement a strong security framework by performing risk analysis and other processes required for managing risks identified within its environment. The implementation specifications of a security management process include:

- Risk analysis
- Risk management
- Sanction policy
- Information system activity review

> ***" HIPAA administrative safeguards are crucial measures that covered entities must consider under the HIPAA Security Rule. "***

Assigned security responsibility

This section identifies the personnel who is responsible for ensuring the Covered Entity continues to stay compliant with the security rule.

Workforce security

This section requires Covered Entities to ensure that authorized members of their workforce are provided access to the ePHI when required. The processes taken up to delegate access should also be effective in preventing unauthorized employees from accessing sensitive information.

Employees requiring access to ePHI should be identified. It should also identify the time in which access should be granted and ensure enough measures are implemented to control workforce access to these resources. The three implementation specifications include:

- Authorization and/or supervision
- Workforce clearance procedure
- Termination procedures

Information access management

This section mandates organizations to incorporate strict access controls to prevent any unauthorized disclosure, modification or destruction of sensitive patient data. The three implementation specifications include:

- Isolating healthcare clearing house functions
- Access authorization
- Access establishment and modification

Security awareness and training

Security training for all the new and existing employees of the Covered Entity is a mandated requirement of the Security Rule. Training should also be given when operational or environmental changes affecting the ePHI take place. The changes could also be documented in the updated policies and procedures.

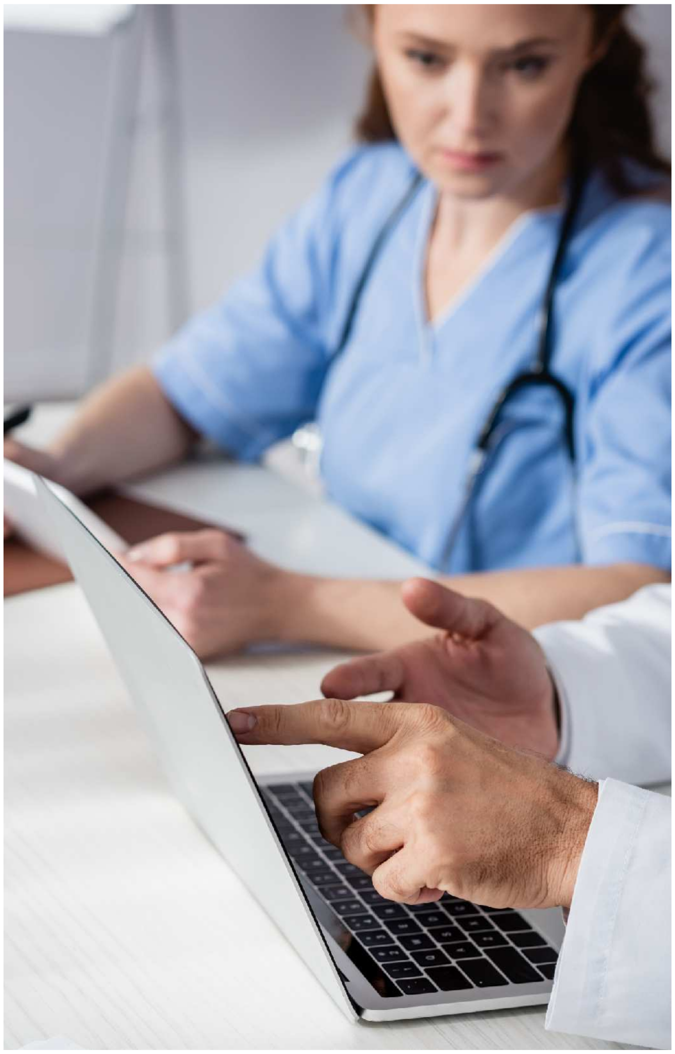
The four implementation specifications include:

- Security reminders
- Protection from malicious software
- Log-in monitoring
- Password management

Security incident procedures

Organizations must document policies and implement the required procedures to address information security incidents. The procedures should document how the incidents should be identified, the communication channels and the procedures employees should follow when reporting an information security incident.

This would include various implementations such as preserving the evidence, mitigating the situation that caused the incident, documenting its outcome and evaluating the security incidents as part of conducting the risk management process.



Contingency planning

This section establishes the processes in place to ensure access to ePHI can be retrieved when Covered Entities experience any disruption to their business operations. The disruption could be a result of natural disasters or occurrence of any information security incidents. The goal is to ensure ePHI is available whenever required. The five implementation specifications include:

- Data backup
- Data recovery
- Emergency mode operation plan
- Testing and revision procedures
- Applications and data criticality analysis

> ***" The contingency plan must have procedures for responding to an emergency that disrupts devices and systems containing ePHI. "***

Evaluation

Conducting an evaluation on a periodic basis helps Covered Entities to check whether the processes and measures they implement continue to be effective in protecting sensitive information. The evaluation should be done on both technical and administrative controls. Evaluation helps Covered Entities implement the right security measures to help them align with the standards put forth in the security rule.

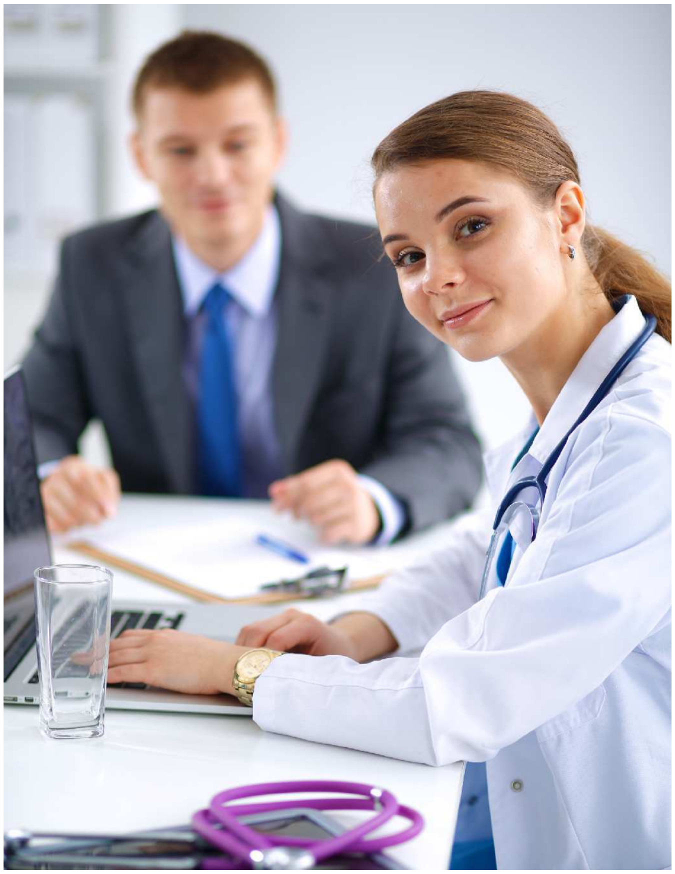
The baseline level of security should be compliant with the security rule. Further implementations should be based on the changes in your business and operational environment. The evaluation should be conducted on a scheduled basis. It should include reviews of both technical and administrative controls of the security program.

Business associate contracts and other agreements

This standard requires Covered Entities to only permit Business Associates to create, receive, maintain, electronic protected health information only if the Covered Entity is completely satisfied that the Business Associate appropriately safeguards the information.

The standard also highlights situations in which a Business Associate contract is not required. This standard consists of just one implementation specification, namely - the 'Written contract or other arrangements' specification.

" The HIPAA Privacy Rule requires that a covered entity must obtain satisfactory assurances from its business associate that they will appropriately safeguard the ePHI it receives or creates on behalf of the covered entity. "



PHYSICAL SAFEGUARDS

One of the requirements of protecting sensitive patient health information is to implement the adequate number of physical safeguards on all equipment and facilities used to store the information. In order to be completely compliant with the physical safeguards, organizations should make sure they have:

- The right number of security controls in place
- Do a proper risk analysis

Physical safeguards consist of all the measures, policies and procedures Covered Entities take up to protect the information security systems, equipment and buildings from the threat of unauthorized entry, information disclosure and modification. When planning the measures for this standard, the Covered Entity must think about all the various ways in which physical access to ePHI can be done.

The physical safeguards defined within the HIPAA security rule include:

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

Facility access controls

Covered Entities should implement policies and procedures to limit physical access to the information systems and facilities that store the information systems. The standard further mandates organizations to identify the roles and responsibilities of the individual with access to the information.

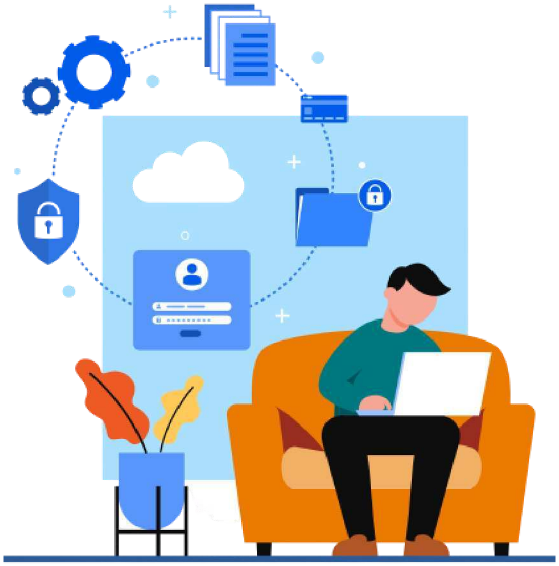
The documented procedures should also include the ways in which access to various entry points would be monitored and mention the interval with which these controls would be reviewed.

The four implementation specifications of this standard include:

- Contingency operations
- Facility security plan
- Access controls and validation procedures
- Maintenance records

Workstation use

This section requires Covered Entities to specify the functions of the computing devices. This minimizes the risk of improper use of devices. Ensuring proper usage of devices is important as it helps to limit the chances for breaches of confidentiality and other threats to occur.



Some of the requirements that constitute the proper usage of devices within the workplace include implementing a clear desk and clear screen policy and auto-locking devices after a set time period of inactivity.

Workstation security

Workstation security mandates organizations to implement adequate security controls to limit unauthorized users from accessing sensitive health information. They should be both physically and logically protected from unauthorized users. Some of the things that organizations have to ensure include:

- Making sure physical safeguards are implemented on systems harboring ePHI
- Identifying and classifying workstations that have access to ePHI
- Ensuring the currently implemented physical measures are effective in protecting the systems
- Ensure the documentation of the safeguards in the required policies and procedures

Device and media controls

This section requires organizations to document policies regarding the management and disposal of removable media that contains protected electronic health information, in and out of the facility and transfer of information between two facilities.

The four implementation specifications include:

- Disposal
- Media re-use
- Accountability
- Data backup and storage

> ***" The HIPAA Security rule states that Covered entities must implement device and media controls as a part of their physical safeguards. "***

TECHNICAL SAFEGUARDS

it refers to the technology and policies and procedures organizations use to protect ePHI and control the level of access employees and other interested parties can have to it.

The technical safeguards defined within the HIPAA security rule includes:

- Access Controls
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Access Controls

This section controls and defines the way in which users can read or modify the data present within the information systems. It provides users with rights needed to perform certain functions on systems, applications and files consisting of sensitive data.

Organizations can use a variety of tools and other technical controls to define the way in which access to these critical resources needs to be managed. The implementation specifications defined within this standard include:

- Unique User Identification
- Emergency Access Procedure
- Automatic Logoff
- Encryption and Decryption

> ***" Access controls should enable authorized users to access only the information necessary to perform assigned operations. "***

Audit Controls

This section requires organizations to have an adequate number of hardware, software and mechanisms in place to check the activity within the information systems housing the ePHI. This include evaluating and logging system activities and documenting system audit reports at regular intervals.

Integrity

Integrity is one of three triads of information security that checks the unauthorized modification or deletion of data. It requires Covered Entities to document policies and procedures to restrict sensitive data from being altered or destroyed.

Person or Entity Authentication

This section simply requires Covered Entities to properly verify the person or Covered Entity seeking access to the ePHI.

They could verify the identity of the individual through PINs, passwords, security tokens such as smart cards or biometrics.

Transmission Security

This section requires organizations to take up measures to prevent unauthorized access to data while being transmitted across networks.

The implementation specifications of this standard include the use of integrity controls such as implementing data loss prevention policies and configuring network settings and enabling encryption on user end devices.

" Covered entities must implement measures to secure unauthorized access to ePHI that is being transmitted over an electronic communications network. "

ROLE OF UEM IN HELPING COMPANIES BECOME HIPAA COMPLIANT

Access to sensitive data isn't just confined to the premises of your organization anymore. With remote work giving employees the flexibility to work from anywhere, the risk of critical health data falling into the hands of the wrong users is incredibly high. Recent stats bring to light the worrying state in which most healthcare providers prioritize security within their workplace.

Most of the data breaches reported this year alone could have been easily avoided if organizations were more careful in documenting strict access control policies and enabling more restrictions to ensure adequate data security when users access them remotely.

Your IT team would already be well aware of the role endpoint management solutions such as a UEM plays in improving the overall security structure of your organization. In addition to onboarding new users and devices across various platforms, UEMs makes it easier for your team to automatically deploy and keep track of all the restrictions and configurations you need in meeting the various requirements stated within the HIPAA security rule.

Device and data security

- Enable BitLocker and Filevault Encryption on Windows and macOS devices.
- Keep track of non-compliant devices.
- Remotely revoke access on non-compliant devices.
- Identify jailbroken iOS and rooted Android devices.
- Define complex passwords to strengthen password security.
- Define password age to restrict users from adopting a predictable pattern when updating passwords.
- Keep data more secure by disabling file sharing capabilities.

- Auto-lock devices after a set period of inactivity.
- Use smart cards to authenticate macOS users.
- Deploy security certificates to bring in an extra layer of security when authenticating users.
- Create a virtual fence on the device to restrict access to sensitive data once the intended user leaves the pre-defined area set as secure by the admin.
- Run scans at real-time or on a periodic basis to check device compliancy with organization policies.
- Remotely schedule OS updates.
- Enable factory reset.
- Configure privacy settings in Mac devices.

Protection of BYO devices

- Create separate encrypted work containers to store business sensitive information.
- Lock work containers with passwords.
- Auto-lock work containers after a defined time period.
- Restrict the transfer of sensitive data from work containers to the users' personal space.
- Setup business containers in iOS devices.
- Have access to multiple Android Enterprise features to securely manage devices, apps and files deployed by your organization.
- Disenroll devices and initiate a corporate wipe to ensure secure removal of ePHI.

Application security

- Remote deployment of store apps, enterprise apps and web apps.
- Install and uninstall critical applications without any user intervention.
- Pre-define critical applications as mandatory and deploy them to users during the onboarding process.
- Blacklist applications known to be a threat to your business operations.
- Prevent the installation of applications from unknown sources.
- Run periodic scans on devices to ensure users have the required applications installed.
- Create managed app catalogs for AE users to provide them with instant access to the applications they need.
- Create app groups to deploy different applications to individual and groups of users.
- Pre-define app permissions and configurations to ensure the integrity of applications used within the organization.
- Remotely update and downgrade applications without impacting the work of your users.
- Monitor network usage on a per app basis.
- Easily deploy UWP applications on Windows devices.
- Push MSI, PKG, MPKG and DMG files on the devices for easier app deployment.

Network security

- Configure Wi-Fi, VPN and APN settings to ensure users only connect to corporate approved networks.
- Deploy web filtering to restrict employees from accessing websites that could be a threat to the security implementations of your organization.
- Configure firewall settings.
- Monitor network usage across all endpoints and applications.

Securing lost devices

- Get real time location updates of lost devices.
- Run periodic scans to keep track of the path traversed by the lost device.
- Initiate corporate wipe on the device to minimize the risk of unauthorized access.
- Enable lost mode on Apple and Android devices.
- Enable remote ring to locate the whereabouts of the device.

WHAT YOU NEED TO DO TO IMPROVE YOUR HIPAA COMPLIANCE

Improving the measures, you've taken up to ensure the continuity of being HIPAA compliant is a time-consuming process that requires a team effort from multiple departments within your organization. Here are some of the measures you can take up to ensure your corporate resources stay protected in alignment with the requirements set by HHS OCR:

- Conduct a security risk assessment.
- Audit all devices and assets falling under the scope of your organization.
- Document all gaps identified during the assessment.
- Document remediation plans to rectify those gaps.
- Update and review the remediation plans on an annual basis.
- Retain the documented remediation plans for a period of 6 years.
- Ensure all staff have read the documented policies and procedures and have legally contested the requirements stated within the policies.
- Document the annual reviews of the policies and procedures.
- Have a Business Associate agreement with all Business Associates.
- Perform due diligence on Business Associates to check their compliance with HIPAA.
- Track and review Business Associate agreements on an annual basis.
- Have a defined process for managing and reporting information security incidents and data breaches in an efficient manner.

4

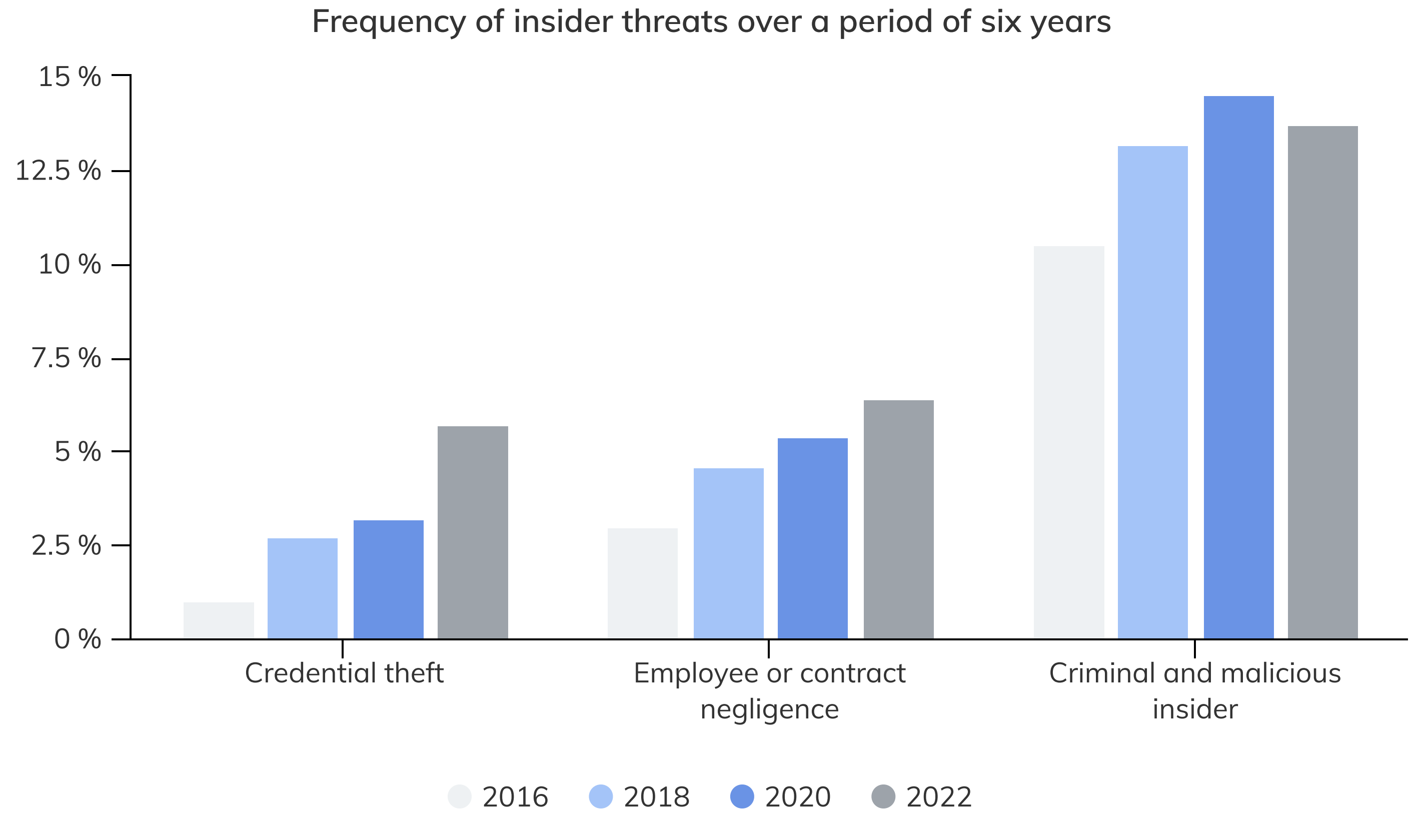
Why regulatory compliance is important

Insider threat continues to be one of the leading causes of data security breaches.

According to the latest cost of insider threats global report brought out by Ponemon Institute, 56% of incidents were caused as a result of negligence and the average annual cost taken to rectify it was $6.6 million.

HIPAA like most other regulatory compliance frameworks continuously updates its standard to keep up with the evolving cybersecurity threat landscape.

Conducting training on a periodic basis and building employee awareness on the various security implementations your organization has applied to protect data is a great way to significantly reduce the occurrence of insider threats and other breaches.



Recent statistics all point to the fact that most of the breaches reported within the healthcare industry within the past quarter could have been avoided if organizations were more careful and quicker enough to identify and deal with employee negligence.

The use of a UEM tool and other cloud-based solutions can automate a number of processes you would require in making sure corporate assets stays protected and ensure employee have all the necessary settings enabled on the devices to ensure complete protection of the sensitive health information they are working with.