For: Matrixforce
Date completed: October 23, 2025
Prepared by: HIPAA Secure Now!

Executive Summary Report

Matrixforce

Table of Contents

Executive Summary

An administrative, physical, and technical assessment was performed for Matrixforce against the HIPAA Security Rule. The methodology that was used to perform the HIPAA Risk Assessment was based on risk assessment concepts and processes described in NIST SP 800-30 Revision 1

The Assessment included the offices located at: 9810 East 42nd St. Ste. 209, Tulsa, OK 74146

Special attention was paid to all information systems used by Matrixforce that may contain electronic protected health information (ePHI)

OVERVIEW

Matrixforce relies on the use of automation for its daily business and clinical processes, most of them involving electronic health protected information (ePHI). The HIPAA Security Regulation, which deals with the security of ePHI, became final on April 21, 2005. The Matrixforce, concerned with both the increasing exposure to the risk of health information systems and compliance with the HIPAA Security Regulation, initiated the process of a thorough HIPAA Risk Assessment.

Risk Assessment Methodology

1 - Identify and document all ePHI repositories

Understanding where patient data is stored and accessed.

2 - Identify and document potential threats and vulnerabilities to each repository

27 industry standard threats and risks to ePHI were assessed

3 - Assess current security measures

Which safeguards are implemented vs not implemented.

4 - Determine the likeliness of threat occurrence

Based on existing safeguards, how probable is each threat to occur.

5 - Determine the potential impact of threat occurrence

If the threat were to occur, what is the impact to the confidentiality, integrity, and availability of ePHI.

6 - Determine the level of risk

Factoring the likelihood of a threat and its impact, an overall risk level is identified.

7 - Determine additional security measures needed to lower level of risk

Recommendations are provided for which safeguards must be implemented to best reduce each threat.

2. Compliance Score Details

We've provided an overall compliance score based on your implementation of safeguards within this assessment. Points are awarded based on the implementation of a safeguard and point totals vary based on the safeguard. To improve this score, work on addressing the remaining recommendations in this assessment.

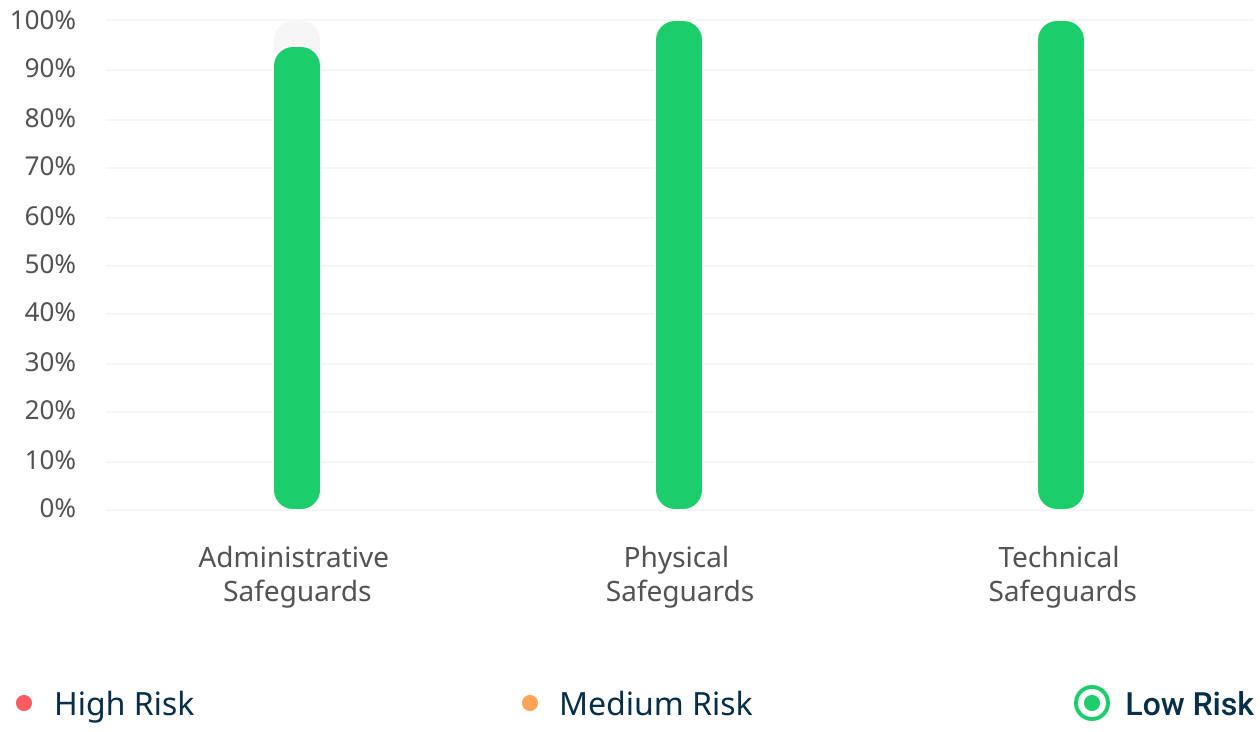
Your Company Overall Compliance Score

96 **of 100**

same points on your previous score of 96

- 0/60 - Poor
- 61/85 - Fair
- **86/100 - Good**

Safeguard Implementation Details



3.1. Administrative Safeguards

Administrative Safeguards

20 of 21 safeguard(s) were implemented

There are no changes since your last assessment

Finding	Recommendations
Cyber insurance coverage options should be applied for (A)	The appropriate level of cyber insurance coverage should be implemented to help offset costs associated with a cybersecurity incident. Matrixforce should work with a reputable cyber insurance provider to evaluate appropriate coverage levels for their organization.

3.2. Physical Safeguards

Physical Safeguards

16 of 16 safeguard(s) were implemented

There are no changes since your last assessment

Finding	Recommendations
No finding	There are no recommendations to this section.

3.3. Technical Safeguards

Technical Safeguards

23 of 23 safeguard(s) were implemented

There are no changes since your last assessment

Finding	Recommendations
No finding	There are no recommendations to this section.

4. HIPAA Compliance with Existing Controls

The compliance chart below provides a visual snapshot of the implementation status of each section throughout the assessment. A detailed breakdown of these implementation levels can be found in the detailed report.

HIPAA Compliance based on existing controls	Implemented	Partially Implemented	Not Implemented
Administrative Safeguards			
Administrative - HIPAA Security Management Policy	✓		
Administrative - Assigned security responsibility policy	✓		
Administrative - Workforce security	✓		
Administrative - Information access management	✓		
Administrative - Security awareness and training	✓		
Administrative - Incident response		⊖	
Administrative - Contingency plan	✓		
Administrative - Evaluation	✓		
Administrative - Business associate contracts and other arrangements	✓		
Physical Safeguards			
Physical Safeguards - Facility access controls	✓		

4. HIPAA Compliance with Existing Controls

HIPAA Compliance based on existing controls	Implemented	Partially Implemented	Not Implemented
Physical Safeguards - Workstation use	✓		
Physical Safeguards - Workstation security	✓		
Physical Safeguards - Device and media controls	✓		
Technical Safeguards			
Technical - Access control	✓		
Technical - Audit controls	✓		
Technical - EPHI Integrity	✓		
Technical - Person or entity authentication	✓		
Technical - Transmission security	✓		

5. Threats and Risk with Existing Controls

The report shows all threats to electronic protected health information (ePHI) with existing controls (safeguards and existing security measures). The probability of the threat, the impact to ePHI and the overall risk level has been determined based on the responses to the risk assessment questions that were completed on the HIPAA Compliance Portal.

Overall Risk Determinations

		Probability		
		LOW	MEDIUM	HIGH
Impact	HIGH	Medium	High	High
	MEDIUM	Low	Medium	High
	LOW	Low	Low	Medium

Threat	Safeguards Implemented vs. Total Evaluated	Probability with Existing Controls	Impact with Existing Controls	Overall Risk
1. Internal water damage could disrupt hardware and corrupt data	6/6	Low	Low	Low
2. Unauthorized access or theft of data could occur	17/18	Low	Medium	Low
3. Fire could damage critical systems	4/4	Low	Low	Low
4. Lost or stolen smartphone may contain ePHI	8/8	Medium	Low	Low
5. Unauthorized individuals could gain access to the network	16/17	Low	Low	Low
6. Data integrity could be compromised intentionally or unintentionally	4/4	Medium	Low	Low
7. Files could be deleted	6/6	Medium	Low	Low

5. Threats and Risk with Existing Controls

Threat	Safeguards Implemented vs. Total Evaluated	Probability with Existing Controls	Impact with Existing Controls	Overall Risk
8. Lost or stolen portable media device could contain ePHI	6/6	Low	Low	Low
9. Lost or stolen backup media could contain ePHI	9/9	Low	Low	Low
10. Malicious code such as ransomware could compromise critical systems	17/18	Low	Medium	Low
11. Former employees could access critical systems and compromise data integrity	17/17	Low	Medium	Low
12. A physical intrusion could lead to unauthorized access of critical data	13/13	Low	Medium	Low
13. Data on unattended systems may be viewed/accessed by unauthorized individuals	9/9	Low	Medium	Low
14. A power failure could damage critical systems and corrupt data	6/6	Low	Low	Low
15. Insecure email could expose confidential information	4/5	Low	Low	Low
16. Sensitive information is visible on a computer screen	5/5	Low	Medium	Low
17. Employees could share passwords	4/4	Low	Medium	Low
18. Improper disposal of electronic media may result in unauthorized access of sensitive information	7/7	Low	Medium	Low
19. Temporary or newly hired employees may not receive adequate training	4/4	Low	Medium	Low
20. Hardware failures may affect the availability of ePHI	6/6	Medium	Low	Low
21. A data circuit/internet failure may prevent access to critical systems	3/3	Low	Low	Low

5. Threats and Risk with Existing Controls

Threat	Safeguards Implemented vs. Total Evaluated	Probability with Existing Controls	Impact with Existing Controls	Overall Risk
22. Natural disasters could damage the infrastructure/network	5/5	Low	Medium	Low
23. A power failure could disrupt critical system access	7/7	Low	Medium	Low
24. A Business Associate could cause a data breach	3/4	Low	High	Medium
25. An employee could access ePHI without authorization	10/10	Low	Medium	Low
26. An employee could disclose ePHI on a public forum or social media platform	3/3	Low	Medium	Low
27. Use of unauthorized software could lead to exposure of critical data	6/6	Low	Low	Low

Additional Recommendations

We have compiled 6 areas all organizations should focus on for improving compliance and lowering overall risks.

These are not specific to your organization.

Email Phishing

Phishing emails are a leading cause of security breaches because they exploit a human-related vulnerability. During an assessment performed in 2022 by the Cybersecurity & Infrastructure Security Agency (CISA), 84% of employees replied to a phishing email with sensitive information or interacted with a spoofed link or attachment.

Ransomware Attacks

One of the most dangerous and common types of malware is known as ransomware. According to the Health and Human Services (HHS) Health Sector Cybersecurity report of December 2023, there was a 278% increase in breaches reported to OCR due to ransomware from 2018 to 2022.

Accidental or Intentional Data Loss

Data loss is another way that ePHI confidentiality, integrity, or availability may be compromised. Some common threats that result in data loss include: improper media disposal, insider threats, improper access to ePHI. loss or theft of devices containing ePHI, system vulnerabilities and a lack of employee security awareness, just to name a few.

Loss to theft of equipment or data

A leading cause of breaches results from the loss or theft of equipment or data. Based on the U.S. Department of Health and Human Services' Breach Notification website, which lists all reported breaches affecting 500 of more individuals, a significant number of reported breaches involved portable media. Some additional tips include:

- Minimize the amount of ePHI
- Limit access
- Track Portable media

Attacks against connected medical devices

Poor cybersecurity for the Internet of Things (IoT) medical devices can also pose a major risk to not only patient data but patient safety as well. In many situations these devices can be difficult, or impossible, to patch or update, and could run outdated operating systems.

HIPAA/Cyber Insurance

Threats and risks to organizations cannot be mitigated to zero (i.e. tornado destroying an office). Even organizations that implement strong security policies could run the risk of a data breach.

Additional Recommendations

- Encrypt portable media

Appendix A

Risk Assessment Supporting Information

1. Organization Info

Name and Location

Name	Matrixforce
Industry	Information Technology
Administrator Name	Kevin Fream
Administrator Email	kfream@matrixforce.com
Administrator Phone (Primary)	+1 918 622 1167
Administrator Phone (Alternate)	+1 918 645 4741
Address 1	9810 East 42nd St. Ste. 209
Address 2	
City	Tulsa
State	OK
Zip Code	74146
Number of Employees	10

1. Organization Info

Network

Number of Servers	2
Network Operating System	Windows
Network Details	We utilize Microsoft Cloud Services for: - Office 365 for messaging and SharePoint/OneDrive for our corporate data. - CRM Online / Zoho for sales/marketing as well as support case management. - Enterprise Mobility/Intune for device management, anti-malware, and updates. - Entra AD Connect, site recovery, and virtual machines. Local LAN consists of: - 2 Hyperv servers with rolling refresh under warranty - 2 Virtual Domain Controllers - all servers protected by Windows Defender - Separate EqualLogic SAN network with 3 members consisting of approx. 60TB - Virtual Remote Desktop Server and Azure MFA with Office, Peachtree, Visual Studio, Visio - Virtual Data server for user folders and printers - Fortinet 100E firewall with on-site spare - Cable modem for 1000/30 Mbs throughput with on-site spare - 2 SAN switches and 2 network switches each with on-site spare
Number of Laptops	2
Number of Workstations	10
Workstation/Laptop Operating System	Windows 11, Windows 10

EMR/EHR

Implemented	No
Vendor	
Internal Name	
Operating System	
Other Operating System	
Location	
Other Location	

1. Organization Info

Email

Email	Yes
Email Vendor	Office365 (Exchange Online)
Email Vendor Details	Microsoft E5 licensing
Email Vendor Other	
Email Server Location	Hosted by a 3rd party
Additional Email Details	We utilize Office 365 with multi-factor authentication, encrypted e-mail enabled, inbound disclaimer, terms disclaimer, journaling, 7 year retention for financial users, 3 year retention for all others, and Advanced Threat Protection.

Portable Media

Portable Media	Yes
Tablets	Yes
PHI or Sensitive Data	No
Portable Media Devices	Surface tablets with Bitlocker encryption.

Backup Media

Backup Media	Yes

Smartphones

Smartphones	Yes
Smartphone Vendors	iPhone & Android. We currently enforce an Office 365 policy to require a pin to use the phone, enforce encryption, and have the capability to quarantine and fully or selectively wipe corporately registered devices (PC, Tablets, and Smartphones).

1. Organization Info

System

Name	
Operating System	Windows
System Vendor	
# of ePHI on Sensitive Data	0
System Location	Hosted by a 3rd party
System Details	

Additional Information

Additional Info	We've been fortunate to not have any acts of God, theft, cybercrime, terrorism or the like.

2. Risk Assessment Questions/Answers

#1 Have you completed a Risk Assessment? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule requires that a Risk Assessment be completed. The purpose of a Risk Assessment is to: identify where ePHI is located, the threats to ePHI, the risks to ePHI and determine safeguards to better protect ePHI.

Description

Answer “YES“ if the organization has previously completed a Risk Assessment.

Answer “NO“ if the organization has not completed a Risk Assessment.

#2 Have you implemented a Risk Management program? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule requires that a Risk Management program be implemented. The Risk Management program evaluates and implements the recommended safeguards of a Risk Assessment to reduce risks and vulnerabilities to a reasonable and appropriate level. In addition, a Risk Management program periodically reviews system audit logs and activity. The HIPAA Security Rule further states that an organization should: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of [ePHI], that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule].

Description

Answer “YES“ if the organization has implemented a Risk Management program.

Answer "NO" if the organization has not implemented a Risk Management program or has not implemented a periodic review of system audit logs, and activity, or has not performed periodic technical and non-technical evaluations.

#3 Does the organization have a Sanction Policy? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule requires that a formal Sanction Policy be implemented to address situations where workforce members violate the HIPAA Security policies and procedures. Consequences for non-compliance could include retraining the workforce member who violated the policies and procedures, or perhaps terminating the individual if the violation is serious.

Description

Answer “YES“ if the organization has implemented and enforced a Sanction Policy for non-compliance with the HIPAA Security Rule.

Answer “NO“ if the organization does not have a formal Sanction Policy or does not enforce the Sanction Policy.

2. Risk Assessment Questions/Answers

#4 Has the organization appointed a security/privacy officer? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security & Privacy Rules requires that an organization appoint an individual that will be responsible for developing, implementing, maintaining and monitoring adherence to the HIPAA Security/Privacy policies and procedures.

Description

Answer “YES“ if the organization has appointed a HIPAA security/privacy officer.

Answer “NO“ if the organization has not appointed a HIPAA security/privacy officer.

#5 Have your Business Associates signed Business Associate agreements? **Control Implemented?** N/A

HIPAA Related Info

HIPAA defines a "Business Associate" as: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. The HIPAA Security Rule requires that all Business Associates have signed agreements with covered entities (i.e. practices) stating that they will protect ePHI and comply with the HIPAA Security Rule.

Description

Answer “YES“ if all your Business Associates have signed Business Associate agreements.

Answer “NO“ if all your Business Associates have not signed Business Associate agreements.

#6 Have your Business Associates been trained on the HIPAA Security Rule and how to protect ePHI? **Control Implemented?** N/A

HIPAA Related Info

In order for Business Associates to protect ePHI and to comply with the HIPAA Security Rule, they need to understand the HIPAA Security Rule. Ensuring that Business Associates are trained on the HIPAA Security Rule will help protect ePHI.

Description

Answer “YES“ if your Business Associates have been trained on the HIPAA Security Rule and protecting ePHI.

Answer “NO“ if your Business Associates have not been trained on the HIPAA Security Rule and protecting ePHI.

2. Risk Assessment Questions/Answers

#7 Is your telehealth/telemedicine tool HIPAA compliant and will the vendor sign the appropriate Business Associate Agreement?

Control Implemented? N/A

HIPAA Related Info

Telehealth/telemedicine tools assist in facilitating patient care through electronic communication channels. These tools are beneficial for both sides but efforts should be made to ensure these tools are protecting patient information. A secure and HIPAA compliant telehealth/telemedicine tool should be implemented. This vendor should sign the required Business Associate Agreement (BAA) and meet the acceptable standards for the protections of patient information.

Description

Answer “YES“ if the organization utilizes a HIPAA compliant telehealth/telemedicine tool and has signed the appropriate Business Associate Agreement.

Answer “NO“ if the telehealth/telemedicine tool used by the organization is not HIPAA compliant or will not sign the appropriate Business Associate Agreement.

#8 Does your telehealth/telemedicine tool create a private (non-public facing) and encrypted communication channel?

Control Implemented? N/A

HIPAA Related Info

Telehealth/telemedicine tools should be equipped with security safeguards that protect sensitive information and the privacy of a patient. Telehealth/telemedicine tools should be non-public facing and a secure and private connection must be made between the organization and the patient. All communication channels should be encrypted to protect data in transit within the tool.

Description

Answer “YES“ if the organization utilizes telehealth/telemedicine tools that are non-public facing and employ encrypted communication channels.

Answer “NO“ if the organization utilizes telehealth/telemedicine tools that either are public facing or do not employ encrypted communication channels.

#9 Does the organization have documented disaster recovery procedures in place?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

Description

Answer “YES“ if the organization has documented disaster recovery procedures in place and regularly test the procedures.

Answer “NO“ if the organization does not have documented recovery procedures in place or does not test the procedures regularly.

2. Risk Assessment Questions/Answers

#10 Does the organization have documented data backup procedures in place?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Description

Answer “YES“ if the organization does have a documented and tested data backup procedure in place.

Answer “NO“ if the organization does not have a documented data backup procedure in place or does not test the backup procedure.

#11 Is there an encrypted offline version of critical data backups, such as with a physical external drive, that are conducted on a regular basis?

Control Implemented? Yes

HIPAA Related Info

Ransomware events are on the rise and affecting all industries, especially healthcare. When ransomware occurs, it can spread across systems and can infect any connected backups. Having an offline version of your backed up data will protect the information from ransomware, making recovery easier should an event occur. This can generally occur through a physical piece of hardware such as an external drive. Encryption technology should be applied for this offline backup to protect the data if the device were to be lost or stolen.

Description

Answer “YES“ if the organization performs regular backups of critical data using an encrypted offline backup method such as an external drive.

Answer “NO“ if the organization does not perform regular backups of critical data using offline backup method such as an external drive or if the external drive is not encrypted.

Answer “N/A“ if the organization does not have any local patient or critical information that would need to be backed up.

2. Risk Assessment Questions/Answers

#12 Does the organization have redundancy in place for all critical systems? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Description

Answer “YES“ if the organization has redundancy in place, including spare equipment, for all critical systems.

Answer “NO“ if the organization does not have redundancy in place including spare equipment that can be used in case of disaster or hardware failure.

#13 Does the organization have redundant data circuits in place in case of circuit failure? **Control Implemented?** N/A

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. An outage of a data circuit may prevent access to ePHI. Having redundant circuits such as a T-1 with a backup DSL or Cable Modem can minimize or reduce the chances of outages that can prevent access to ePHI.

Description

Answer “YES“ if the organization has redundant data circuits in place in case of a circuit failure.

Answer “NO“ if the organization does not have redundant circuits in place in case of a circuit failure.

#14 Does the organization have hardware support contracts in place on all critical systems? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data. Having hardware support contracts in place will help in the event of a disaster. If equipment if damaged, hardware contracts can speed up the process of replacing the hardware.

Description

Answer “YES“ if the organization has hardware support contracts in place in case of critical server/system failures due to hardware failures or caused by disaster.

Answer “NO“ if the organization does not have any hardware support contracts already in place.

2. Risk Assessment Questions/Answers

#15 Does the organization have emergency operations procedures in place in the event of an emergency? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. Emergency Mode Operations Plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. When operating in an emergency mode it is important to protect ePHI.

Description

Answer “YES“ if the organization has implemented and tested a documented procedure for emergency operations in case of disasters such as floods, tornadoes, hurricanes or power failures. A documented process for handling a possible disaster.

Answer “NO“ if the organization does not have a documented emergency operations plan in case of a disaster.

#16 Is there a procedure in place to facilitate proper ePHI access being granted? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule - Information Access Management Standard states that all users that access ePHI must have the proper authority. Initial access to ePHI must be granted (i.e. to a new workforce member) and periodic review of access must be performed. Any changes in job functions should result in a review of the person's access to ePHI. Upon termination a person's access to ePHI should be immediately revoked.

Description

Answer “YES“ if there is a procedure or policy in place that facilitates and verifies proper ePHI access is being granted to appropriate members.

Answer “NO“ if there is not a procedure or policy that facilitates or verifies that ePHI access is being granted to the proper workforce members.

2. Risk Assessment Questions/Answers

#17 Is there a documented and adhered to procedure for terminating a workforce member's access including physical network and data access?

Control Implemented? Yes

HIPAA Related Info

It is important to implement procedures that remove physical, network and data access to all workforce members when their employment is terminated. The HIPAA Security Rule states: Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends.

Description

Answer “YES“ if there is a documented and followed procedure for terminating a workforce member. Does the procedure cover removing all access and ID's from all systems in a timely manner?

Answer “NO“ if there is not an actual documented procedure that is to be followed in the event of a workforce member termination or if the procedure is not performed on a constant or timely basis.

#18 Does the organization have an incident response procedure to follow in the event of a security breach?

Control Implemented? Yes

HIPAA Related Info

Organizations should be prepared in the event of a data breach containing ePHI. There should be a detailed procedure on the steps that should be taken in the event of a breach. The procedure should include the steps to respond to the breach and breach notification procedures. The HIPAA Security Rule states: Standard: Security incident procedures. Implement policies and procedures to address security incidents. Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Description

Answer “YES“ if the organization has a documented incident response procedure to follow in the event of a security breach. A documented procedure that outlines the steps to be taken if a security breach occurs.

Answer “NO“ if the organization does not have a documented procedure for handling security breaches.

2. Risk Assessment Questions/Answers

#19 Does your organization have an IT specialist (either internal or external) or Managed Service Provider (MSP) who are competent in addressing cybersecurity issues in your office?

Control Implemented? Yes

HIPAA Related Info

Having a competent Information Technology (IT) team supporting your organization is critical in the protection of company equipment and patient data. With countless cybersecurity threats, and healthcare being a prime target for cybercrime, it is imperative that all organizations, regardless of employee size, work with an IT team. This IT team should be available when called upon for security threats and assist in configuring computing equipment with the proper security features. The IT team must also be in compliance with the HIPAA Security Rule and sign the appropriate Business Associate Agreement.

Description

Answer “YES“ if the organization has a competent IT team who assist with protecting the organization’s devices and information.

Answer “NO“ if the organization does not rely on a competent IT team to assist in protecting their devices and information.

#20 Does your organization have cyber insurance coverage options that can help offset the cost associated with a breach or security incident?

Control Implemented? No

HIPAA Related Info

Breaches and security incidents can be very costly to organizations. With cybercrime at an all-time high, healthcare is a premier target. Organizations who suffer a cyber event such as ransomware, phishing, hacking, compromised account or other, face many serious and expensive liabilities to resolve the situation. Cyber insurance policies can help offset the costs of these events by covering the costs of forensics, legal, public relations, fines and more. Policies should be evaluated to ensure the appropriate level of coverage is available to protect the organization.

Description

Answer “YES“ if the organization has an appropriate level of cyber insurance coverage.

Answer “NO“ if the organization does not have cyber insurance coverage or the coverage is not sufficient to protect the organization in the event of a cyber event.

#21 Are all workforce members required to go through security training?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule Security Awareness and Training Standard states that an organization must implement a security awareness and training program for all members of its workforce (everyone coming into contact with patient information, including managers, owners, etc.). The organization must also provide workforce members with periodic security reminders.

Description

Answer “YES“ if all workforce members are required to go through security training to increase their awareness of HIPAA security requirements and protecting ePHI.

Answer “NO“ if all workforce members are not required to go through HIPAA security training.

2. Risk Assessment Questions/Answers

#22 Does management or IT send out periodic phishing simulations to all employees to track click rates and evaluate their awareness levels?

Control Implemented? Yes

HIPAA Related Info

Phishing scams are increasingly common for most organizations. Employees must be aware of the threats that a phishing email poses to the organization and should have a strong understanding of how to spot a malicious message. Sending periodic phishing simulations to employees of all levels can provide measurable awareness of employee's phishing awareness levels and those who fail a simulation can be provided with additional training to ensure that they do not click on a real phishing message.

Description

Answer "YES" if the organization or IT performs periodic phishing simulations to evaluate employee's phishing awareness levels and provide additional training for those who fail the simulation.

Answer "NO" if the organization or IT do not perform periodic phishing simulations to evaluate employee's phishing awareness levels or "NO" additional training is provided for those who fail the simulation.

#23 Does the organization perform any form of baseline cybersecurity assessments to evaluate a new employee's cybersecurity strengths and weaknesses?

Control Implemented? Yes

HIPAA Related Info

New employees can present many cybersecurity vulnerabilities for organizations. A new employee's previous cybersecurity experience levels are often a mystery and can vary greatly. Without proper insight into the new employee's cybersecurity strengths, and more importantly their weaknesses, your organization may be at risk of an incident stemming from a lack of awareness. Baseline cybersecurity assessments can offer insight into the core areas of cybersecurity and highlight risks while offering suggestions to increase awareness when the employee begins.

Description

Answer "YES" if the organization performs baseline cybersecurity assessments on new employees before they begin accessing sensitive information.

Answer "NO" if the organization does not perform baseline cybersecurity assessments on new employees before they begin accessing sensitive information.

#24 Are servers protected from water damage and not located near a water source?

Control Implemented? Yes

HIPAA Related Info

In order to protect ePHI it is important to ensure that systems containing ePHI are protected from environmental danger. Co-locating servers containing ePHI by water sources may lead to damage or destruction of ePHI.

Description

Answer "YES" if servers are not located near a water source.

Answer "NO" if the servers are located anywhere near a water source, Ex: water pipes going through the room, servers located near bathrooms or kitchens.

2. Risk Assessment Questions/Answers

#25 Does the organization use any methods to track who or when someone enters the room(s) where the servers are located?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule states: 164.310 Physical safeguards. A covered entity must, in accordance with 164.306: (a)(i) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. (ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. (iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a persons access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. (iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Description

Answer “YES“ if the organization tracks who and when someone enters the room(s) where servers are located. Note: Servers may be located in multiple locations.

Answer "NO" if the organization does not track access to the room(s) where servers are located.

#26 Is the location(s) where the organization keeps their servers locked at all times?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule states: 164.310 Physical safeguards. A covered entity must, in accordance with 164.306: (a)(i) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. (ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Description

Answer “YES“ if the location(s) where the organization keeps their servers is locked at all times. Note: Servers may be located in multiple locations.

Answer “NO“ if the location(s) where the organization keeps their servers is not locked at all times and the servers are accessible to workforce members, visitors, and patients.

2. Risk Assessment Questions/Answers

#27 Does the organization restrict access to the room(s) or location where servers are located? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule states: 164.310 Physical safeguards. A covered entity must, in accordance with 164.306: (a)(i) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. (ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. (iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. (iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Description

Answer “YES“ if the organization restricts access to the room(s) or location where servers are located. Note: Servers may be located in multiple locations.

Answer “NO“ if the access to the room(s) or location where servers are located is not restricted.

#28 Does the organization track the movement of visitors and patients while they are in the organization's facility? **Control Implemented?** N/A

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: Standard: Facility Access Control. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Implementation specific: Facility Security Plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Tracking visitors is a key part of a Facility Security Plan.

Description

Answer “YES“ if the organization has a procedure implemented to track the movement of individuals inside the organization. I.E. security cameras or restricted access between rooms.

Answer “NO“ if the organization does not track the movement of individuals inside the organization.

2. Risk Assessment Questions/Answers

#29 Are workforce members aware of workstation use policies that prohibit online activities such as email, social networks, etc.?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule states that all workforce members should be made aware of proper workstation use. Workstation use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. Categories of websites that are deemed inappropriate by the organization should be blocked and filtered by IT security controls.

Description

Answer “YES“ if workforce members have been made aware of what is allowed or not allowed in regards to posting or mentioning ePHI. Would they know that posting ePHI data on a social network would be prohibited?

Answer “NO“ if workforce members have not been informed of ePHI data restrictions and would be unaware that posting ePHI on a social network would be prohibited.

#30 Are workforce members advised on what is a permitted use of a workstation, are they required to sign off on that?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule states that all workforce members should be made aware of proper workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. Categories of websites that are deemed inappropriate by the organization should be blocked and filtered by IT security controls.

Description

Answer “YES“ if workforce members are advised and instructed on what is permitted use of a workstation, what is not allowed use and are they required to sign off that they have been informed of what is allowed use.

Answer “NO“ if workforce members are not advised or instructed on what they are allowed and not allowed to do on a workstation.

2. Risk Assessment Questions/Answers

#31 Does the organization protect ePHI on monitors from unauthorized access? **Control Implemented? N/A**

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: Standard: Workstation Use (Required). Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. Privacy screens can help prevent unauthorized access or viewing of ePHI. This is especially true when workstations that access ePHI are located in common areas that patients or visitors might access.

Description

Answer “YES“ if the organization uses privacy screens for monitors to protect ePHI from being displayed on the screens, or takes additional methods to limit a patient or visitor's view of computer screens.

Answer “NO“ if the organization does not use privacy screens on monitors, or has computer screens that are in vulnerable areas and easily visible.

#32 Are all systems and servers fully patched for OS vulnerabilities and updated with all required application updates and service packs? **Control Implemented? Yes**

HIPAA Related Info

Hackers and malware exploit system vulnerabilities in operating systems as well as applications running on your network. It is important to keep all operating systems and applications up to date with security patches.

Description

Answer “YES“ if you have an implemented procedure for patching all systems/servers with required application and OS updates.

Answer “NO“ if you do not have an implemented procedure for keeping all systems/servers updated with the required application and OS updates.

#33 Is anti-malware (anti-virus and anti-spyware) installed and updated on each of the organization's workstations and servers? **Control Implemented? Yes**

HIPAA Related Info

Malware (computer viruses and spyware) is one of the leading causes of data being stolen or breached. It is critical to have anti-malware installed on all systems including workstations, laptops, servers, etc. The anti-malware should be automatically updated with new definition files.

Description

Answer “YES“ if the organization has implemented anti-malware protection on all systems to prevent malicious intrusions.

Answer “NO“ if the organization does not have anti-malware on all systems to protect from malicious intrusions.

2. Risk Assessment Questions/Answers

#34 Do all servers use an Uninterrupted Power Supply (UPS)? **Control Implemented?** Yes

HIPAA Related Info

The HIPAA Security Rule states that covered entities must ensure that ePHI is protected to ensure confidentiality, integrity, and availability. Installing an Uninterrupted Power Supply (UPS) can help ensure access (availability) to ePHI in the event of a power loss. A UPS should be installed on every system that contains ePHI as well as network equipment.

Description

Answer “YES“ if all systems that contain ePHI use a UPS (Uninterrupted Power Supply) in case of power failures to maintain system uptime.

Answer “NO“ if all systems that contain ePHI do not use a UPS in case of power failure.

#35 Does the organization track the movement and ownership of portable media? **Control Implemented?** N/A

HIPAA Related Info

One of the leading causes of ePHI data breaches is lost laptops and portable media. Portable media that contains ePHI should be tracked and records maintained of the movement of all portable media. Portable media includes USB flash drives, external/removable drives, tablets, DVDs, etc. The HIPAA Security Rule states: Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronically protected health information into and out of a facility, and the movement of these items within the facility. Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Description

Answer “YES“ if the organization tracks the movement (in and out of an organization) and ownership of portable media and if records are kept with this information.

Answer “NO“ if the organization does not track movement or ownership of portable media and records of this are not kept.

#36 Does the organization have a procedure for the disposal of electronic media that stores ePHI? **Control Implemented?** Yes

HIPAA Related Info

Media that contains ePHI must be properly disposed of. All ePHI must be removed prior to disposing. Simply deleting the ePHI from the media is not enough to safeguard the data. Special programs that totally eliminate the data from the media must be used. The HIPAA Security Rule states: Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

Description

Answer “YES“ if the organization has a documented procedure for steps to follow for the disposal of electronic media that stores ePHI.

Answer “NO“ if the organization does not document a procedure to be followed when disposing of electronic media that stores ePHI.

2. Risk Assessment Questions/Answers

#37 Are all devices that are taken out of the office either encrypted or physically secured during transportation? **Control Implemented?** Yes

HIPAA Related Info

Devices that are taken out of the office are vulnerable to loss or theft. Encrypting those devices or physically securing them (like in a locked trunk), is the best way to protect them during transportation.

Description

Answer “YES“ if the organization encrypts or physically secures all portable devices when transporting them outside of the office.

Answer “NO“ if the organization does not encrypt or physically secure all portable devices when transporting them outside of the office.

#38 Is there a documented and adhered to Bring Your Own Device (BYOD) policy that is signed by all applicable staff? **Control Implemented?** Yes

HIPAA Related Info

Many organizations now allow their employees to use their own personal devices for work purposes. Personal mobile devices such as smartphones, tablets, and laptops, that are used for work purposes should still have strong security protections and the owner of the device should be aware of the best practices for protecting their device and the information it may be storing. A Bring Your Own Device (BYOD) policy can help establish these responsibilities and should be presented to and signed by employees that are given the privilege of using their personal device for work purposes.

Description

Answer “YES“ if the organization has a Bring Your Own Device (BYOD) policy that is signed by all applicable staff members.

Answer “NO“ if the organization does not have a Bring Your Own Device (BYOD) policy or the policy is not signed by all applicable staff members.

#39 Is there a documented and acknowledged policy that addresses the security requirements that employees are expected to follow when working remotely? **Control Implemented?** Yes

HIPAA Related Info

Employees need to understand what is expected of them when working remotely. A robust remote work policy should be documented and explain how devices should be utilized, protected and what precautions the employee should take. Policies should be clear and concise and the employee(s) working remotely should be required to acknowledge their understanding and acceptance of their expectations.

Description

Answer “YES“ if the organization has a documented remote work policy that addresses remote work security requirements that has been acknowledged by the applicable staff.

Answer “NO“ if there is not a documented remote work policy or this remote work policy has not yet been acknowledged by the applicable staff.

2. Risk Assessment Questions/Answers

#40 Do employees protect passwords and do not share with other employees?

Control Implemented? Yes

HIPAA Related Info

When accessing ePHI every member of the workforce must use a unique userid and password. Workforce members should not share passwords with each other. This includes leaving passwords in plain sight, posting them on notes and sticking them to the monitor, leaving passwords written under the keyboard, etc. These practices should also be considered when using Single Sign on (SSO) capabilities.

Description

Answer “YES“ if workforce members protect userids and passwords and do not share userids and passwords.

Answer “NO“ if workforce members use shared userids and passwords or if workforce members at times share userids and passwords among themselves or if workforce members post passwords on monitors or under keyboards.

#41 Are workforce members required to create a complex password?

Control Implemented? Yes

HIPAA Related Info

A complex password also called a strong password, is one that meets industry standards and is made up of at least 8 characters. It should include a combination of letters, numbers, and symbols like "@" or "$". However, it's worth noting that longer passwords, with 12 or more characters, are even more secure than the minimum requirement of 8 characters, according to industry standards. In fact, using passphrases, which are longer phrases or sentences, is highly recommended due to their increased length and ease of memorization for the user. These practices should also be considered when using Single Sign on (SSO) capabilities.

Description

Answer “YES“ if the organization has implemented procedures to require workforce members to create complex passwords for all systems that contain ePHI.

Answer “NO“ if workforce members are allowed to use non-complex passwords.

2. Risk Assessment Questions/Answers

#42 Are critical accounts and accounts with administrative credentials protected with a form of multi-factor authentication (MFA)?

Control Implemented? Yes

HIPAA Related Info

Multi-factor authentication (MFA) is an additional authentication method that provides an additional layer of security for critical accounts. With MFA enabled, a second or more verification method would be required after initially entering login credentials for an account. Examples of additional verification methods include a one-time passcode sent via email or text message, biometrics like a fingerprint or a key card. Due to the critical importance of ePHI, MFA should be enabled on all administrator level accounts and critical accounts where large quantities of patient data are stored. MFA should also be enabled when using a VPN to access critical systems containing ePHI. These practices should also be considered when using Single Sign on (SSO) capabilities.

Description

Answer “YES“ if the organization has multi-factor authentication methods enabled for all critical accounts and administrative level accounts.

Answer “NO“ if the organization does not utilize multi-factor authentication methods for all critical accounts and administrative level accounts.

#43 Will workforce member accounts get disabled or locked if they mistype or incorrectly put in their password numerous times?

Control Implemented? Yes

HIPAA Related Info

Disabling or locking user accounts protects user accounts from being compromised. Hackers, either human or malware, usually try to guess passwords or use brute force programs to continually try to guess a password. By disabling accounts after a certain number of failed password attempts makes it extremely difficult for hackers to compromise accounts. According to industry standards, 10 attempts is the maximum number of attempts, but 3-5 is best practice. These practices should also be considered when using Single Sign on (SSO) capabilities.

Description

Answer “YES“ if workforce members accounts get disabled or locked after failed password attempts for all systems that contain ePHI.

Answer “NO“ if workforce members accounts do not get disabled or locked after failed password attempts.

#44 Does the organization have system auditing setup to facilitate the detection of unauthorized access?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule requires that all access to ePHI be logged or audited. Information that is usually collected is: Who is the person or userid that is accessing ePHI? When did the person or userid access ePHI? What ePHI was accessed? EMRs, network shares and other server based systems need to have system auditing setup and configured.

Description

Answer “YES“ if the organization does have system auditing setup.

Answer “NO“ if the organization does not have system auditing setup.

2. Risk Assessment Questions/Answers

#45 Does the organization, on a regular basis review audit logs?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule requires that system audit logs be periodically reviewed to ensure that only appropriate access to ePHI is occurring. The review would ensure that only appropriate user IDs are accessing ePHI and that the user IDs are only accessing the ePHI that they are authorized to access. Regular review of system audit logs can detect data breaches and unauthorized access to ePHI.

Description

Answer “YES“ if the organization does review audit logs.

Answer “NO“ if the organization does not have a procedure to review audit logs.

#46 Are all the organization's laptops encrypted to protect the data stored on them?

Control Implemented? Yes

HIPAA Related Info

One of the leading causes of ePHI data breaches is lost laptops and portable media. Laptops that contain ePHI should be encrypted to prevent access to ePHI in the event a laptop if lost or stolen.

Description

Answer “YES“ if all of the organization's laptops are encrypted to protect the data stored on them.

Answer “NO“ if the organization's laptops are not encrypted and the data is not protected in case of loss or theft.

#47 Is backup media encrypted to protect the data?

Control Implemented? Yes

HIPAA Related Info

Backup media may hold a large amount of ePHI. Lost backup media could result in a large scale breach of ePHI. Ensuring that your backup media is encrypted is critical in preventing data breaches.

Description

Answer “YES“ if backup media is encrypted to protect their data.

Answer “NO“ if the backup media is not encrypted and the data is not protected in case of loss or theft.

2. Risk Assessment Questions/Answers

#48 Is portable media (USB drives, CDs, DVDs, etc) encrypted to protect the data stored on them? **Control Implemented?** Yes

HIPAA Related Info

One of the leading causes of ePHI data breaches is lost laptops and portable media. Portable media that contains ePHI should be encrypted to prevent access to ePHI in the event the media is lost or stolen. Portable media includes USB flash drives, external/removable drives, tablets, DVDs, etc.

Description

Answer “YES“ if all portable media is encrypted to protect the data stored on them.

Answer “NO“ if all portable media is not encrypted and the data is not protected in case of loss or theft.

#49 Does the organization encrypt email to protect ePHI and important information sent through email? **Control Implemented?** Yes

HIPAA Related Info

The security risks for email commonly include unauthorized interception of messages en route to recipient and messages being delivered to unauthorized recipients. These risks in using the Internet are addressed in the Security Rules technical safeguards section, particularly: - Person or Entity Authentication required procedures must be implemented for identification verification of entity or party requesting access to PHI. This means the identity of the person seeking information must be confirmed within the information system being utilized. - Transmission Security addressable data integrity controls and encryption reasonable and appropriate safeguards. All ePHI sent via email should be encrypted.

Description

Answer “YES“ if the organization implements a procedure to encrypt email to protect ePHI.

Answer “NO“ if the organization does not implement or enforce a procedure that requires encryption for all email to protect ePHI and important data sent through email.

#50 Are smartphones encrypted to protect ePHI data stored on them? **Control Implemented?** Yes

HIPAA Related Info

Smartphones include Blackberries, iPhones, Android phones, etc. Smartphones may contain ePHI (in emails, attachments, spreadsheets, documents, etc.). Smartphones like laptops and portable media are easily lost or stolen. It is critical to ensure that all ePHI on smartphones are encrypted to prevent access to ePHI in the event the phone is lost.

Description

Answer "YES" if the organization implements a procedure to encrypt all smartphones to protect data stored on them.

Answer "NO" if the organization does not have a procedure to encrypt all smartphones to protect the data.

2. Risk Assessment Questions/Answers

#51 Does the organization encrypt all desktop computers (non-laptops) that store ePHI?

Control Implemented? Yes

HIPAA Related Info

Encryption is the best way to protect ePHI in the event the device is lost or stolen. Desktop computers may store large quantities of patient information and although they lack the portability of laptops/tablets, may be a prime theft candidate during an office break-in.

Description

Answer “YES“ if the organization has all desktop computers (non-laptops) encrypted that store ePHI.

Answer “NO“ if the organization has not encrypted all desktop computers (non-laptops) that store ePHI.

#52 Is the organization's remote access secured to prevent unauthorized access?

Control Implemented? Yes

HIPAA Related Info

The Department of Health and Human Services states the following about remote access to ePHI. "We group some of the risks associated with remote access and offsite use of ePHI into three areas: access, storage and transmission. Risk management planning takes all three areas into account, based on the unique vulnerabilities they introduce to covered entities that rely on remote operations involving ePHI." It is critical to ensure that an organization's remote access is properly protected. Remote Access should be secure, require proper authentication (such as MFA) and utilize encryption to protect the data. The amount of users that are allowed to remotely access the organization's resources should also be limited to the minimum necessary.

Description

Answer “YES“ if the organization's remote access is secured to prevent unauthorized access.

Answer “NO“ if the remote access is unsecured and could be susceptible to unauthorized access.

#53 Are all remote employees required to securely connect to services and data via a Virtual Private Network (VPN) or through a remote desktop connection?

Control Implemented? Yes

HIPAA Related Info

Employees with the ability to work remotely create many security challenges to an organization. Remote workers accessing data and services controlled by the organization should ensure a secure connection is made between the device and the information being accessed. Virtual Private Networks (VPN) can create secure connections between a remote device and the data and services it is accessing. Also, remote desktop connections provide remote workers the ability to virtual access a more secure work device. Multi-Factor authentication should be used when using a VPN to access critical systems containing ePHI.

Description

Answer “YES“ if remote employees are required to connect to the organization’s services and data through a secured Virtual Private Network or remote desktop connection.

Answer “NO“ if remote employees are not required to connect to the organization’s services and data through a secured method.

2. Risk Assessment Questions/Answers

#54 Is the organization's wireless access properly secured?

Control Implemented? Yes

HIPAA Related Info

In order to protect ePHI from authorized access it is critical to ensure that wireless access requires authentication (proper login) and utilizes encryption to prevent ePHI from being accessed, modified or stolen. One way to tell if your organization's wireless is not secured is if visitors can bring in a laptop and connect to your wireless network without a password.

Description

Answer “YES“ if the organization's wireless connection is properly secured with encryption and authentication to prevent unauthorized access.

Answer “NO“ if the organization's wireless connection is not properly secured with encryption and authentication and could allow unauthorized access.

#55 Do workstations, laptops, and servers have inactivity timers to prevent unauthorized access to systems storing ePHI?

Control Implemented? Yes

HIPAA Related Info

Every system that contains ePHI should have an inactivity timeout that locks the screen or prevents access to the system. When a workforce member leaves their workstation another person could access ePHI without proper authorization. Inactivity timeouts prevent this from occurring.

Description

Answer “YES“ if the organization has implemented a procedure to have all systems setup with inactivity timers to prevent unauthorized access.

Answer “NO“ if the organization does not have a procedure to have inactivity timers on all systems.

#56 Do all smartphones employ startup passwords and timeout locks?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule states the following as a requirement: Standard: Person or Entity Authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. If smartphones contain ePHI it is important to implement startup passwords and timeout locks to ensure that only authorized persons can access the contents of the smartphone. Due to the likelihood that smartphones may be lost or stolen, passwords can protect the contents of the smartphone.

Description

Answer “YES“ if the organization has a procedure to implement startup passwords and timeout locks on all smartphones to help prevent against unauthorized access.

Answer “NO“ if the organization does not implement a procedure to employ startup passwords and timeout locks on all smartphones.

2. Risk Assessment Questions/Answers

#57 Does the organization have a technical access control policy that is closely adhered to, to prevent unauthorized access to systems?

Control Implemented? Yes

HIPAA Related Info

The HIPAA Security Rule requires that technical access controls be implemented to protect ePHI. Technical access controls limit access to information. On a network share, technical access controls, may limit access to a patient folder to only those workforce members who are authorized. Other workforce members would not have the ability to access the information. The same is true for an EMR/EHR where technical access controls will limit who can access patient records. It is critical to implement strong technical access controls to protect ePHI. The HIPAA Security Rule states: Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

Description

Answer “YES“ if the organization has implemented a technical access control policy to help prevent unauthorized access to systems and files, hackers, or intentional destruction of data.

Answer “NO“ if the organization does not have an implemented technical access control policy to facilitate specific security measures.

#58 Are all devices that are used for remote work protected with remote monitoring management (RMM), Mobile Device Management (MDM) or comparable solutions?

Control Implemented? Yes

HIPAA Related Info

Devices accessing an organization’s data and solutions remotely should be configured with the same or greater level of protection as devices within the office. In order to best protect these remote devices, solutions must be implemented to ensure a streamlined security configuration across all devices. Remote monitoring management (RMM) and comparable solutions assist in enforcing the appropriate security controls are met on all devices and remote devices can receive the attention and support remotely.

Description

Answer “YES“ if all devices used for remote work are protected with remote monitoring management (RMM) or comparable solutions.

Answer “NO“ if any devices used for remote work are not protected with remote monitoring management (RMM) or comparable solutions.

2. Risk Assessment Questions/Answers

#59 Does the organization have a firewall in place on the network?

Control Implemented? Yes

HIPAA Related Info

Network firewalls protect organizations and ePHI from unauthorized access. Firewalls stop hackers and malware from entering a network. If an organization has an Internet connection such as a T-1, DSL or cable modem it is critical to have the connection protected by a firewall. Network traffic should be restricted, and network ports that are not in use should be disabled.

Description

Answer “YES“ if the organization has implemented secure firewalls to prevent outside intrusions on the network.

Answer “NO“ if the organization has not implemented secure firewalls.

#60 Is there an Intrusion Detection and Prevention System (IDPS) implemented that monitors the network and systems for malicious activities or policy violations?

Control Implemented? Yes

HIPAA Related Info

Network security is critical in protecting ePHI. Although hardware and software firewalls mitigate many security risks, these technologies alone might not be enough to prevent the more sophisticated cyber attacks. Intrusion Detection and Prevention Systems (IDPS) continuously monitor the network for incidents, and security policy violations then blocks and reports back findings.

Description

Answer “YES“ if the organization has an Intrusion Detection and Prevention System in place to protect the network from sophisticated cyber threats.

Answer “NO“ if the organization does not have an Intrusion Detection and Prevention System in place to protect the network from sophisticated cyber threats or if there is "NO" network firewall.

Answer “N/A“ if the organization does not maintain a network or does not have ePHI accessible via their network.

2. Risk Assessment Questions/Answers

#61 Does your organization perform any tabletop exercises or simulations with your IT team to prepare for a ransomware attack and your response?

Control Implemented? Yes

HIPAA Related Info

As ransomware events continue, planning for this event is very important for the organization and their IT team to be able to handle and recover from an actual ransomware event. Simulations of these events can help identify vulnerabilities allowing additional measures to be taken to improve future responses. Simulations should be continuously conducted and repeated until the organization and IT have all immediate vulnerabilities addressed then simulations should continue periodically after that. The organization and IT should reassess their ransomware plans with new simulations when major network changes occur.

Description

Answer “YES“ if the organization performs tabletop exercises or simulations to prepare for a ransomware event.

Answer “NO“ if the organization does not perform tabletop exercises or simulations to prepare for a ransomware event.

#62 Does the organization perform vulnerability scans on the network on a periodic basis?

Control Implemented? Yes

HIPAA Related Info

Frequent vulnerability scans can identify weaknesses in an organization's network that can be exploited to allow unauthorized access to the network and potentially access ePHI. Identifying vulnerabilities will allow the organization an opportunity to patch or correct any vulnerabilities thus lowering the chance of having a data breach of ePHI.

Description

Answer “YES“ if the organization periodically performs a vulnerability scan and corrects any vulnerabilities that are identified.

Answer “NO“ if the organization has not performed vulnerability scans or does not perform these scans on a frequent basis.