HIPAA Risk Assessment

Executive Summary

Prepared For:

Matrixforce

Prepared By:

HIPAA HSN Secure Now!

July 16, 2019

Executive Summary Report

Table of Contents

Appendix A – Risk Assessment Supporting Information

1.1 – Organizational Profile

1.2 – Risk Assessment Questions / Answers

Section 1

Executive Summary

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 HIPAA Security Officer, concerned with both the increasing exposure to the risk of health information systems and compliance with the HIPAA Security Regulation, contracted with HIPAA Secure Now! for a HIPAA Risk Assessment.

HIPAA Secure Now! performed an administrative, physical, and technical assessment of Matrixforce against the HIPAA Security Regulations. 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. An overview of the Risk Assessment process is defined below:

Risk Assessment Methodology

Step	Process
1	Identify and document all ePHI repositories
2	Identify and document potential threats and vulnerabilities to each repository
3	Assess current security measures
4	Determine the likeliness of threat occurrence
5	Determine the potential impact of threat occurrence
6	Determine the level of risk
7	Determine additional security measures needed to lower level of risk
8	Document the findings of the Risk Assessment

The assessment included the offices located at:

Matrixforce, 9810 East 42nd Street Suite 209 Tulsa, OK 74146.

HIPAA Secure Now! paid special attention to all information systems used by Matrixforce that may contain electronic protected health information (ePHI).

Matrixforce has recently established policies and procedures to safeguard ePHI within their practice. It is critical that Matrixforce incorporate operational procedures into their daily workflow. The HIPAA Security Officer and entire staff should not focus on complying with the HIPAA Security Regulation but more on ensuring that ePHI is properly handled, maintained and protected.

Section 2

Areas to Focus on

In this section we have compiled 6 areas all organizations should focus on for improving compliance and lowering overall risks. These are not specific to your organization.

Based on Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients [1]

1) **E-mail phishing attacks:** Phishing emails are a leading cause of security breaches since they exploit a human-related vulnerability. According to the IBM Security Services 2014 Cyber Security Intelligence Index [2], 95% of all data breaches are a result of an employee or human-related error (e.g. phishing). In addition, according to the Verizon Data Breach Investigation Report (DBIR) [3], 92.4% of all malware is delivered via email. Healthcare organizations are at a significantly higher risk of being targeted by phishing scams due to the notably higher value of patient information on the dark web. To remediate the ever-growing threat of phishing scams, we recommend that proper employee training procedures are implemented, and simulated phishing attacks are evaluated.

2) **Ransomware attacks:** One of the most dangerous and common types of malware is known as ransomware. According to the Verizon DBIR, ransomware is found in 39% of all malware related breaches and is the most prevalent type of malware across all business sectors. Ransomware is most commonly delivered in the form of a phishing email. Ransomware will encrypt all files on a computer or possibly the entire network and demand a ransom payment for the decryption code to unlock the files. A paid subscription to a reputable anti-virus software must be implemented across all networkconnected devices within the organization, and virus/malware definitions are kept up to date.

A data backup/recovery plan must be implemented and tested. Proper employee training procedures are also crucial to stopping ransomware attacks delivered through phishing emails and other channels.

3) **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. Auditing workforce access to systems containing health records or sensitive data is crucial to detecting malicious activities. In addition, role-based access and proper termination procedures should be implemented to ensure that there is no unauthorized access to ePHI.

[1] https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
[2] https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf
[3] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

4) **Loss or 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 or more individuals, a significant number of reported breaches involved portable media. Devices such as USB drives, laptops, and backup drives are particularly vulnerable due to their portability and their high likelihood of traveling outside the organization. To help minimize the risk of a breach in this area, we recommend the following steps be taken:

a. **Minimize the amount of ePHI** – if portable media must be used for transporting ePHI, then it is important to restrict the amount of ePHI on portable media to the minimal needed to perform a function or task.
b. **Limit access** – it is important to limit who can copy ePHI to portable media. It is also important to ensure that prior approval has been granted before ePHI can be copied onto portable media.
c. **Track portable media** – ensure that a procedure is in place that tracks all portable

media containing ePHI that enters or leaves the organization.

d. **Encrypt portable media** – the HIPAA Breach Notification Rule states that if you comply with HIPAA encryption standards, it is a "Safe Harbor" if a device is lost or stolen, meaning no breach reporting is necessary. HIPAA Secure Now! recommends

that proper encryption is utilized on any device that may contain ePHI.

5) **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 be running outdated operating systems. Some ways this risk can be mitigated is through proper communication and support agreements with equipment vendors, by disconnecting or segregating the equipment from the network and by tracking portable medical devices containing ePHI. The process for procuring medical devices should include security considerations and requirements for vendors should be developed.

6) **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. Some data breaches occur due to employee misconduct (intentional or unintentional), computer viruses, phishing scams, etc. Cyber-attacks and breaches of Protected Health Information (PHI) can be costly due to breach reporting and notification requirements, remediation services including information technology, forensics, legal, credit monitoring, and possible regulatory fines. HIPAA/Cyber insurance can offset these expenses.

Section 3

High Level Summary

HIPAA Secure Now!'s key findings and recommendations:

The HIPAA Security Rule states that **Addressable (A)** items must be assessed by the organization to determine whether they are reasonable and appropriate safeguards. **Required (R)** items must be implemented by the organization in order to comply with HIPAA Security Guidelines.

Section 3.1

Administrative Safeguards

Finding	**Recommendation**
○ Additional security training measures should be implemented (A)	Phishing emails continue to be a leading source of breaches and computer vulnerabilities. **All staff members should be educated on how to spot phishing attacks. Additionally, an anti-phishing campaign should be implemented to periodically test and train staff with real-time phishing training.** These campaigns provide measurable feedback on vulnerable employees so additional education can be focused on the weaker links.
○ Lack of sufficient cyber-insurance funds could lead to major out of pocket expenses during a breach (A)	In this current landscape, breaches of PHI are a realistic concern for all organizations, regardless of their size. While it is possible to lower the impact or probability of a breach through security improvements, a breach can still occur and can be very expensive for an organization to properly handle. **Matrixforce should evaluate their current risks and ensure that there is an appropriate level of cyber insurance coverage.**

Section 3.2

Physical Safeguards	
Finding	**Recommendation**
○ No Finding	There are no recommendations for this section.

Section 3.3

Technical Safeguards	
Finding	**Recommendation**
○ Vulnerability/Penetration Testing (A)	Vulnerability testing is a process of identifying weaknesses in both internal and external facing hardware and software. These weaknesses can be exploited to gain access to ePHI. After performing vulnerability scans and remediating known vulnerabilities, penetration testing should be performed. Penetration testing is a simulated external attack on key components of the infrastructure. Penetration testing can reveal weaknesses, technical flaws and opportunities for malicious code or hackers to gain access to ePHI. **It is recommended that Matrixforce contine to perform extensive Penetration and Vulnerability scans of all aspects of infrastructure. Any technical flaws or weaknesses should be mitigated.**

Section 4

HIPAA Compliance with Existing Controls

HIPAA Compliance based on existing controls	Implemented	Partially Implemented	Not Implemented
Administrative Policies			
O Administrative - HIPAA Security Management Policy	X		
O Administrative - Assigned security responsibility policy	X		
O Administrative - Workforce security	X		
O Administrative - Information access management	X		
O Administrative - Security awareness and training	X		
O Administrative - Incident response	X		
O Administrative - Contingency plan	X		
O Administrative - Evaluation	X		
O Administrative - Business associate contracts and other arrangements	X		
Physical Policies			
O Physical - Facility access controls	X		
O Physical - Workstation use	X		
O Physical - Workstation security	X		
O Physical - Device and media controls		X	
Technical Policies			
O Technical - Access control	X		
O Technical - Audit controls	X		
O Technical - EPHI Integrity	X		
O Technical - Person or entity authentication	X		
O Technical - Transmission security	X		

Section 5

Compliance Chart Summary

Administrative

1) Administrative - HIPAA Security Management Policy

Questions	YES	NO
O Have you completed a Risk Assessment?	X	
O Have you implemented a Risk Management program?	X	
O Does the organization have a Sanction Policy?	X	

2) Administrative - Assigned Security Responsibility Policy

Questions	YES	NO
O Has the organization appointed a security officer?	X	

3) Administrative - Workforce security

Questions	YES	NO
O Is there a procedure in place to facilitate proper ePHI access being granted?	X	

4) Administrative - Information access management

Controls	Implemented	Not Implemented
O Implement procedure to ensure employees have correct access to ePHI (7)	X	
O Implement an employee termination procedure to remove data access (8)	X	

5) Administrative - Security awareness and training

Controls	Implemented	Not Implemented
O Security training and reminders for the entire workforce (12)	X	

6) Administrative - Incident response

Controls	Implemented	Not Implemented

O Implement a security response plan (9)	X	

7) Administrative - Contingency plan

Controls	Implemented	Not Implemented
O Implement a disaster recovery procedure (3)	X	
O Implement a data backup procedure (4)	X	
O Ensure hardware redundancy is in place (5)	X	
O Install redundant data circuits (6)	N/A	N/A
O Implement emergency operations procedures (10)	X	
O Ensure hardware support contracts are in place (11)	X	

8) Administrative – Evaluation

Questions	YES	NO
O Have you implemented a Risk Management program?	X	

9) Administrative – Business associate contracts and other arrangements

Controls	Implemented	Not Implemented
O Ensure Business Associates contracts are in place (2)	X	
O Ensure Business Associates are properly trained (1)	X	

Physical

10) Physical – Facility Access controls

Controls	Implemented	Not Implemented
O Ensure servers are in an environmentally safe location (13)	X	
O Ensure that all systems that contain ePHI are in a secure area (14)	X	
O Limit access to server room(s) (15)	X	
O Maintain log of who enters server room(s) (16)	X	

O Implement a procedure to track visitors and patients (25)	X	

11) Physical – Workstation Use

Controls	Implemented	Not Implemented
O Implement a workstation Use policy that explains what is prohibited (17)	X	
O Ensure workforce members acknowledge a workstation Use policy that explains what is prohibited (18)	X	

12) Physical – Workstation security

Controls	Implemented	Not Implemented
O Ensure that systems have the proper security patches applied (22)	X	
O Ensure that every computing device on the network has anti-malware installed and updated (23)	X	
O Install privacy screens on workstations (24)	X	

13) Physical – Device and media controls

Controls	Implemented	Not Implemented
O Track portable media used to transport ePHI (19)	N/A	N/A
O Limit amount and access of ePHI on portable media (21)		X
O Ensure that ePHI is removed from portable media before disposal (20)	X	

Technical

14) Technical – Access control

Controls	Implemented	Not Implemented
O Implement unique user id and password for each user (29)	X	
O Implement complex passwords (26)	X	
O Implement password aging (27)	X	

O Disable user accounts after failed password attempts (28)	X	
O Implement secure remote access (33)	X	
O Implement secure wireless network access (34)	X	
O Ensure that backup media are encrypted (36)	X	
O Implement encryption where appropriate (39)	X	
O Ensure that all smartphones have data encryption (32)	X	
O Implement encryption on laptops (35)	X	
O Ensure portable media is encrypted (37)	N/A	N/A
O Implement system inactivity timers (40)	X	
O Implement technical access controls (41)	X	
O Ensure network is protected by firewall (42)	X	
O Ensure that all smartphones have startup and time out password (43)	X	

15) Technical – Audit controls

Controls	Implemented	Not Implemented
O Implement system auditing (30)	X	
O Implement system audit log review procedure (31)	X	

16) Technical – EPHI Integrity

Controls	Implemented	Not Implemented
O Ensure that workstations and servers are connected to UPS (44)	X	

17) Technical – Person or entity authentication

Controls	Implemented	Not Implemented
O Implement unique user id and password for each user (29)	X	

18) Technical – Transmission security

Controls	Implemented	Not Implemented
O Implement email encryption (38)	X	

Section 6

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. Each of the threats and existing controls are described in the Risk Assessment Detailed Report.

Overall Risk		Probability		
		Low	Medium	High
Impact	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Threats with Existing Controls				
Threat #	**Threat**	**Probability w/Existing Controls**	**Impact w/Existing Controls**	**Risk w/Existing Controls**
24	Business Associate could cause a data breach	Low	High	Medium
1	Flood Internal	Low	Low	Low
2	Unauthorized access to data / theft	Low	Low	Low
3	Explosion could damage main computing infrastructure	Low	Low	Low
4	Stolen or lost smartphone may contain ePHI	Medium	Low	Low
5	Hackers could gain unauthorized access to network	Low	Low	Low
6	Data Error - Intentional or Unintentional	Medium	Low	Low
7	Files could be deleted	Medium	Low	Low
8	Stolen or lost laptop / portable media containing ePHI	Low	Low	Low

9	Lost or stolen backup media could have ePHI	Low	Low	Low
10	Virus/Worm/Malicious code could negatively impact the network	Low	Medium	Low
11	Terminated employee accesses system - corrupts, steals or destroys data	Low	Medium	Low
12	Physical intrusion by unauthorized persons	Low	Medium	Low
13	Unauthorized persons may use an unattended workstation	Low	Medium	Low
14	A power failure could corrupt information	Low	Low	Low
15	Insecure email could contain confidential information	Low	Low	Low
16	Confidential information is left in plain view on a computer screen	Low	Medium	Low
17	Employee passwords could be shared	Low	Medium	Low
18	Not adequately destroying electronic media may leave information available to unauthorized persons	Low	Medium	Low
19	Temporary or new employees may be insufficiently trained	Low	Medium	Low
20	Hardware failures could impact the availability of ePHI	Medium	Low	Low
21	A failure in a data circuit could prohibit systems access	Low	Low	Low
22	Acts of God: flood, tornado, tsunami, hurricane	Low	Medium	Low
23	A power failure could interrupt employee access	Low	Medium	Low
25	An employee accesses ePHI that should not have access to ePHI	Low	Medium	Low
26	An employee may post ePHI on a social network or public forum	Low	Medium	Low
27	Employees may install illegal or unauthorized software	Low	Low	Low

Section 7

Classifications

The Risk Assessment uses the classifications below to categorize each risk identified in the IT environment.

Low Risk	– these are areas that have been identified as having low risk, from a business as well as an audit perspective. Impact to ePHI is minimal and no additional action is required.
Medium Risk	– these are areas that have been identified as medium risk from a business as well as an audit perspective. An important risk exists, but it is not so material that it is likely to result in significant impact to ePHI. This may require action to lower the overall risk.
High Risk	– these areas are considered to be inherently high risk from either a business or audit perspective and therefore capable of resulting in significant impact to ePHI. Immediate action should be taken to lower the overall risk.

Description of terms

Administrative Safeguards - are administrative actions and policies and procedures (1) to manage the selection, development, implementation, and maintenance of security measures, and (2) to protect ePHI and to manage the conduct of the "Covered Entities" workforce in relation to the protection of ePHI.

Physical Safeguards - are measures, policies, and procedures to physically protect the Covered Entities and related buildings and equipment that contain ePHI, from natural and environmental hazards and unauthorized intrusion.

Technical Safeguards - are the technology and the policy and procedures for its use that protect ePHI and control access to it.

ePHI – In general, patient health information that has been converted to, stored in, or transmitted by electronic media is deemed to be "ePHI" and as such is to be controlled and protected under the HIPAA Privacy and Security Rules.

HIPAA – Health Insurance Portability and Accountability Act, the HIPAA law requires all health care Covered Entities (CEs) and their Business Associates (BAs) to safeguard the privacy of patient health information. The HIPAA law also requires CEs and BAs to implement required security measures to protect patient health information.

Business Associate - A Business Associate is a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI. A Business Associate is not a member of the health care provider, health plan, or other covered entity's workforce. A health care provider, health plan, or other covered entity can also be a business associate to another covered entity.

Covered Entities - Covered Entities (CEs) include all health care providers (doctors, dentists, therapists, psychologists, pharmacists, etc.), health care clearinghouses, and health plans (i.e., health insurance companies) that electronically store, process or transmit electronic protected health information (ePHI).

U.S. Department of Health and Human Services' Breach Notification website -
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Appendix A

Matrixforce

Risk Assessment Supporting Information

Section 1.1

Organization Info

Name and Location

Name	Matrixforce
Administrator Name	Kevin Fream
Administrator Email	kfream@matrixforce.com
Administrator Phone (Primary Contact)	918-622-1167 ext. 25
Administrator Phone (Alternate)	918-645-4741
Address 1	9810 East 42nd Street
Address 2	Suite 209
City	Tulsa
State	OK
Zip	74146
Number of Employees	10

Network

Number of Servers	7
Network Operating System	Windows
Network Details	We utilize Microsoft Cloud Services for: - Office 365 for messaging and SharePoint/OneDrive for ourcorporate data. - CRM Online for sales/marketing as well as support casemanagement. - Enterprise Mobility/Intune for device management,anti-malware, and updates. - Azure 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 membersconsisting of approx. 60TB - Virtual Relay server for SAN alerts from replication partnercustomers - Virtual Remote Desktop Server and Azure MFA with Office, Peachtree, Visual Studio, Visio - Fortinet 90D firewall with on-site spare - Cable modem for 200/10 Mbs throughput with on-site spare- 2 SAN switches and 2 network switches each with on-site spare
Number of Workstations	10
Number of Laptops	2
Workstation/Laptop Operating System	
Vulnerability scans	Yes
Vulnerability Scans Details	

EMR/EHR

EMR/EHR Implemented	No
EMR/EHR Vendor	
EMR/EHR Internal Name	
EMR/EHR Operating System	

EMR/EHR Details	
EMR/EHR Location Description	

Email

Email	Yes
Email Vendor	Microsoft Exchange
Email Vendor Details	
Email Vendor Other	
Email Server Location	Hosted by a 3rd part
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, 2 year retention for all others, and Advanced Threat Protection.

Portable Media

Portable Media	Yes
Tablets	Yes
Portable Media Devices	USB for secondary Accounting backup. External drive stored in a secure location quarterly refreshed with current SharePoint Online data.

Backup Media

Backup Tapes	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).

Additional Systems

System 1

Name	Azure Backup
Operating System	Windows
Vendor	Microsoft
Location	Hosted by a 3rd party
Number of ePHI Records	0

System Details	Microsoft Azure backup of server system states to Microsoft.
Number of ePHI Records	0

Additional Information

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

Section 1.2

Risk Assessment Questions / Answers

Question #	Question	Description	HIPAA Related Info	Control Implemented
1	Have you completed a Risk Assessment?	Answer 'YES' if the organization has previously completed a Risk Assessment. Answer 'NO' if the organization has not completed a Risk Assessment.	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.	Yes

2	Have you implemented a Risk Management program?	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 nontechnical evaluations.	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 polices and procedures meet the requirements of [the Security Rule].	Yes
3	Does the organization have a Sanction Policy?	Answer "YES" if the organization has implement and enforces 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.	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.	Yes
4	Has the organization appointed a security officer?	Answer "YES" if the organization has appointed a HIPAA security officer. Answer "NO" if the organization has not appointed a HIPAA security officer.	The HIPAA Security Rule requires that an organization appoint an individual that will be responsible for developing, implementing, maintaining and monitoring adherence to the HIPAA Security policies and procedures.	Yes Security officer Name :Kevin Fream Security officer email :kfream@matrixforce.com
5	Have your Business Associates signed Business Associate agreements?	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.	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.	Yes
6	Have your Business Associates been trained on the HIPAA Security Rule and how to protect ePHI?	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.	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.	Yes

7	Does the organization have documented disaster recovery procedures in place?	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.	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.	Yes

8	Does the organization have documented data backup procedures in place?	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.	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.	Yes
9	Does the organization have redundancy in place for all critical systems?	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.	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.	Yes
10	Does the organization have redundant data circuits in place in case of circuit failure?	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.	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.	N/A
11	Does the organization have hardware support contracts in place on all critical systems?	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.	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.	Yes

12	Does the organization have emergency operations procedures in place in the event of an emergency?	Answer "YES" if the organization has implemented and tested a documented procedure for emergency operations in case of disasters such as floods, tornados, 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.	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.	Yes

13	Is there a procedure in place to facilitate proper ePHI access being granted?	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.	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.	Yes
14	Is there a documented and adhered to procedure for terminating a workforce member's access including physical network and data access?	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.	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.	Yes
15	Does the organization have an incident response procedure to follow in the event of a security breach?	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.	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.	Yes

16	Are all workforce members required to go through security training?	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.	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 (including management). The organization must also provide workforce members with periodic security reminders.	Yes
17	Are servers protected from water damage and not located near a water source?	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.	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.	Yes

18	Does the organization use any methods to track who or when someone enters the room(s) where the servers are located?	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.	The HIPAA Security Rule states: Â§ 164.310 Physical safeguards. A covered entity must, in accordance with Â§ 164.306: (a)(1) 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 personâ??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).	Yes
19	Is the location(s) where the organization keeps their servers locked at all times?	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.	The HIPAA Security Rule states: Â§ 164.310 Physical safeguards. A covered entity must, in accordance with Â§ 164.306: (a)(1) 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.	Yes

20	Does the organization restrict access to the room(s) or location where servers are located?	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.	The HIPAA Security Rule states: Â§ 164.310 Physical safeguards. A covered entity must, in accordance with Â§ 164.306: (a)(1) 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).	Yes
21	Does the organization track the movement of visitors and patients while they are in the organization's facility?	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.	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.	Yes

22	Are workforce members aware of workstation use policies that prohibit online activities such as email, social networks, etc.?	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.	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.	Yes
23	Are workforce members advised on what is a permitted use of a workstation, are they required to sign off on that?	Answer "YES" if workforce members are advised and instructed on what is permiited 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.	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.	Yes

24	Does the organization protect PHI on monitors from unauthorized access?	Answer "YES" if the organization uses privacy screens for monitors to protect ePHI from being displayed on the screens. Answer "NO" if the organization does not use privacy screens on monitors.	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.	Yes
25	Are all systems and servers fully patched for OS vulnerabilities and updated with all required application updates and service packs?	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.	Hackers and malware exploit system vulnerabilities in operating systems (Windows XP, Vista, 7 and 2003 and 2008 Server) as well as applications such as Adobe Acrobat and Microsoft Office. It is important to keep all operating systems and applications up to date with security patches.	Yes

26	Is anti-malware (anti-virus and anti-spyware) installed and updated on each of the organizations workstations and servers?	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.	Malware (computer viruses and spyware) is one of the leading cause 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.	Yes
27	Do all servers use a Uninterrupted Power Supply (UPS)?	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.	The HIPAA Security Rule states that covered entities must ensure that ePHI is protected to ensure confidentiality, integrity, and availability. Installing a 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.	Yes
28	Does the organization track the movement and ownership of portable media?	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.	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 drives, USB thumb drives, USB flash drives, CDs, DVDs, floppy drives, 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 electronic 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.	N/A

29	Does the organization have a procedure for the disposal of electronic media that stores ePHI?	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.	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.	Yes
30	Do workforce members with laptops take the system home, or out of the office?	Answer "YES" if workforce members take laptops out of the office at anytime. Answer "NO" if workforce members laptops are never removed from the organization.	One of the leading causes of ePHI data breaches is lost laptops and portable media. Laptops that contain ePHI should be tracked and only authorized workforce members should be allowed to remove them from an organization's offices.	Yes

31	Do employees protect passwords and do not share with other employees?	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.	When accessing ePHI every member of the workforce must use an 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.	Yes
32	Are workforce members required to create a complex password?	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.	A complex password, sometime known as a strong password is a password that consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc) if allowed. Passwords are typically case-sensitive, so a complex password contains letters in both uppercase and lowercase. Complex passwords also do not contain words that can be found in a dictionary or parts of the users own name.	Yes
33	Are workforce members required to change their passwords periodically?	Answer "YES" if the organization has procedures in place that require workforce members to change their passwords on a periodic basis for all systems that contain ePHI. Answer "NO" if the organization does not have procedures in place that require workforce members to change their passwords on a periodic basis.	Requiring workforce members to change passwords every 30 or 60 or 90 days will help secure their user account. Password changes prevent breached accounts from being access over a long period of time.	Yes

34	Will workforce member accounts get disabled or locked if they mistype or incorrectly put in their password numerous times?	Answer "YES"Â• if workforce members accounts get disabled or locked after failed password attempts for all systems that contain ePHI. Answer "NO"Â• if workforce members accounts do not get disabled or locked after failed password attempts.	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 passwords attempts it makes it extremely difficult for hackers to compromise accounts.	Yes
35	Does the organization have system auditing setup to facilitate the detection of unauthorized access?	Answer "YES" if the organization does have system auditing setup. Answer "NO" if the organization does not have system auditing setup.	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.	Yes
36	Does the organization, on a regular basis review audit logs?	Answer "YES" if the organization does review audit logs. Answer "NO" if the organization does not have a procedure to review audit logs.	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 userids are accessing ePHI and that the userids 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.	Yes

37	Are all the organization's laptops encrypted to protect the data stored on them?	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.	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.	Yes
38	Is backup media encrypted to protect the data?	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.	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.	Yes
39	Is portable media (USB drives, CDs, DVDs, etc) encrypted to protect the data stored on them?	Answer "YES" if all portable media is encrypted to protect the data stored on them. Answer "NO" if the all portable media is not encrypted and the data is not protected in case of loss or theft.	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 drives, USB thumb drives, USB flash drives, CDs, DVDs, floppy drives, etc.	N/A
40	Does the organization encrypt email to protect ePHI and important information sent through email?	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.	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.	Yes

41	Are smartphones encrypted to protect ePHI data stored on them?	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.	Smartphones include Blackberries, iPhones, Android phones, etc. Smartphones may contain ePHI (in emails, attachments, spreadsheets, documents, etc.). Smartphone 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.	Yes
42	Does the organization encrypt all devices that store ePHI?	Answer "YES" if the organization has a procedure to encrypt all devices that store ePHI. Answer "NO" if the organization does not have a procedure to ensure all devices that store ePHI are encrypted.	Encryption is the best way to protect ePHI in the event the device is lost or stolen. Devices include laptops, portable media, desktops, and even servers. Each of the devices might be stolen in the event of a theft or break-in.	Yes

43	Is the organization's remote access secured to prevent unauthorized access?	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.	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 and utilize encryption to protect the data.	Yes
44	Is the organization's wireless access properly secured?	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.	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.	Yes
45	Do workstations, laptops, and servers have inactivity timers to prevent unauthorized access to systems storing ePHI?	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.	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 prevents this from occurring.	Yes

46	Do all smartphones employ startup passwords and timeout locks?	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.	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.	Yes

47	Does the organization have a technical access control policy that is closely adhered to, to prevent unauthorized access to systems?	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.	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.	Yes
48	Does the organization have a firewall in place on the network?	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.	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.	Yes