Sample HIPAA/HITECH Assessment Report - Demo Site

databrackets

August 21, 2019

Prepared By:
databrackets
None
None

Physician(s):
Dr. John Doe

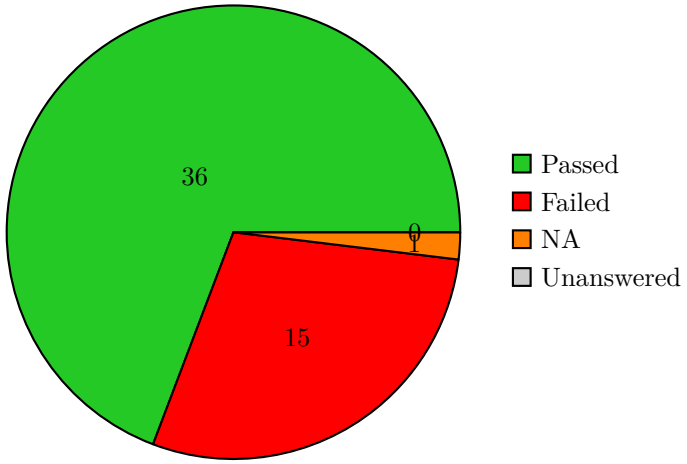
Contents

1 Executive Summary

60

Assessment Score

Disclaimer: Information provided by the customer and its associates for this assessment was not independently verified by databrackets; the customer has provided details about their operation to the best of their knowledge. These reports and recommendations are for evaluation purposes only and not intended to be con-strued as legal advice. The customer is advised to consult with attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on the company and/or its personnel.
How do we calculate assessment score: This assessment score is offered as a means for determining the degree to which threats and associated vulnerabilities apply to your organization's risks while this score is an optional feature in the risk analysis, it is strongly recommended that the organization utilize this score, as the scoring number will assist in determining the degree to which the current operations address the matching threat-vulnerability statement.
HIGH risk is defined as having a catastrophic impact on the organization; the organization is incapable of offering services and a significant number of records have been lost or compromised.
MEDIUM is defined as having a significant impact; the organization may offer a reduced array of services to customers; A moderate number of records within the organization have been lost or compromised.
LOW is defined as a modest or insignificant impact; the organization can continue to offer services and some records may be lost or compromised.
Based on the number of questions selected for the organization's scope of assessment and their priorities, we calculate the risk factor of the organization. For each of the open action items based on the priorities assigned, we multiply the risk factor with the priority of the pending action items to arrive at the assessment score.



2 Results Overview

Module	Incl in Assessment	# Areas Covered	Pass %	Failure %	Not Applicable
Administrative Security Safeguards	Yes	23	57.0%	43.0%	0
Physical Security Safeguards	Yes	10	70.0%	30.0%	0
Technical Security Safeguards	Yes	9	100.0%	0.0%	1
Organizational Requirements	Yes	2	100.0%	0.0%	0
Policies and Procedures and Documentation Requirements	Yes	1	100.0%	0.0%	0
Breach Notification Rules	Yes	7	71.0%	29.0%	0
HIPAA Privacy Rule	No				

3 Action Plan Summary

Module	Question	Action Plan	Priority	Due Date	Status
Administrat Security Safeguards	Contingency Plan : Have you established (and imple..	Establish (and implement as needed) procedures to ..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Workforce Security : Do you screen workforce membe..	Screen workforce members prior to enabling access ..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Workforce Security : Do you have timely actions to..	Set policies and procedures to perform timely acti..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Security Awareness and Training : Do you provide p..	Provide periodic information security reminders to..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Security Awareness and Training : Do you perform s..	Implement training on policies and procedures for ..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Security Awareness and Training : Do you perform s..	Implement training on procedures for monitoring lo..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Security Awareness and Training : Do you perform s..	Implement training on procedures for creating, cha..	Medium	2019-11-30	In Progress
Physical Security Safeguards	Facility Access Controls : Have you established (a..	Establish (and implement as needed) procedures tha..	Medium	2019-11-30	In Progress

Physical Security Safeguards	Facility Access Controls : Have you implemented po..	Implement policies and procedures to safeguard the..	Medium	2019-11-30	In Progress
Physical Security Safeguards	Facility Access Controls : Have you implemented pr..	Implement procedures to control and validate a per..	Medium	2019-11-30	In Progress
Breach Notification Rules	Do you have a process in place to demonstrate that..	Have a process in place to demonstrate that breach..	Medium	2019-11-30	In Progress
Breach Notification Rules	Do you have a policy to delay the breach notificat..	Have a policy in place to delay the breach notific..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Security Incident Procedures : Do you have procedu..	Implement procedures to identify and respond to su..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Business Associate Contracts and Other Arrangement..	o Establish written contracts or other arrangement..	Medium	2019-11-30	In Progress
Administrat Security Safeguards	Contingency Plan : Have you established and implem..	Establish and implemented procedures to create and..	Medium	2019-11-30	In Progress

4 Identified Risks with Action Plan

These are risks that have been identified, evaluated, and have an Action Plan. We have identified 0 high, 15 medium, and 0 low action items. Of all items in the action plan, 15 are pending and 0 are complete.

4.1 Contingency Plan : Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode? §164.308(a)(7)(ii)(C)

Module: Administrative Security Safeguards

Description: o Procedure for obtaining necessary PHI during an emergency should be part of the contingency plan
o The training of personnel in their contingency roles and responsibilities
o Training should occur at least annually
o Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness then document the results
o Reviewing the contingency plan at least annually and revising the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing)
o Procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.
o This could include procedures to restore backup tapes to a new server in response to a hardware failure.
Covered in the Information Security Policy Template, "Data Backup and Contingency Plan" Section, "Disaster Recovery and Emergency Mode Operations Plan" Subsection

Response: No

Risk Description: You might not have established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode; potential data loss could occur during vulnerable periods of the business.

Comments: No, we do have complete protection during emergency mode.

Action Plan: Establish (and implement as needed) procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode.
o Procedure for obtaining necessary PHI during an emergency should be part of the contingency plan
o The training of personnel in their contingency roles and responsibilities
o Training should occur at least annually
o Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness then document the results
o Reviewing the contingency plan at least annually and revising the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing)
o Procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.
o This could include procedures to restore backup tapes to a new server in response to a hardware failure.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(7): HIPAA § 164.308(a)(7)

4.2 Workforce Security : Do you screen workforce members prior to enabling access to facilities, information systems, and ePHI to verify that users are trustworthy? § 164.308(a)(3)(ii)(B)

Module: Administrative Security Safeguards

Description: Implement procedures to determine that the access of workforce members to electronic protected health information is appropriate and the individuals are trustworthy.
Covered in the Information Security Policy Template, "Employee Background Checks" Section.

Response: No

Risk Description: Your organization might not screen workforce members in high-risk positions prior to enabling access to facilities, information systems, and ePHI to verify that users are trustworthy. Therefore, unqualified or untrustworthy users could access your practice's ePHI.

Comments: No formal and informal background checks are conducted.

Action Plan: Screen workforce members prior to enabling access to facilities, information systems, and ePHI to verify that users are trustworthy.
Implement procedures to determine that the access of workforce members to electronic protected health information is appropriate and the individuals are trustworthy.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(3): HIPAA § 164.308(a)(3)

4.3 Workforce Security : Do you have timely actions to ensure that workforce termination procedures are appropriately followed? § 164.308(a)(3)(ii)(C)

Module: Administrative Security Safeguards

Description: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.
Covered in the Information Security Policy Template, "Identification and Authentication" Section, "Termination of User Login Account" Subsection.

Response: No

Risk Description: Your organization might not have timely actions to ensure that workforce termination procedures are appropriately followed; an individual with revoked permission to access PHI could continue to have access.

Comments: No, we do not have termination procedures implemented.

Action Plan: Set policies and procedures to perform timely actions to ensure that workforce termination procedures are appropriately followed.
Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(3): HIPAA § 164.308(a)(3)

4.4 Security Awareness and Training : Do you provide periodic information security reminders? 164.308(a)(5)(ii)(A)

Module: Administrative Security Safeguards

Description: Security awareness training to all users, i.e. during new employee orientation then periodic reminders.
Examples of providing information security reminders include:
o Face-to-face meetings
o Email updates
o Newsletters
o Postings in public areas, i.e. hallways, kitchen
o Company Intranet
Security awareness training should be conducted in an on-going basis. Maintain contact with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals to stay up to date with the latest recommended security practices, techniques, and technologies. Subscribe to email security alerts and advisories, including:
o Cisco security alerts
o CERT advisory alerts
o NIST publications and vulnerability alerts
o Other vendor-specific alerts like McAfee, Symantec, etc.

Response: No

Risk Description: Your organization might not provide periodic information security reminders. Users are the weakest link in healthcare data breach prevention, and lack of security training to staff is considered to be the major factor in patient data compromise.

Comments: No, we do not have periodic security reminders.

Action Plan: Provide periodic information security reminders to all staff.
o Security awareness training to all users before authorizing access to the system, i.e. during new employee orientation
o Examples of providing information security reminders include:
o Faceotooface meetings
o Email updates
o Newsletters
o Postings in public areas, i.e. hallways, kitchen
o Company Intranet
o Security awareness training should be conducted in an onogoing basis
o Maintain contact with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals to stay up to date with the latest recommended security practices, techniques, and technologies. Subscribe to email security alerts and advisories, including:
o Cisco security alerts
o CERT advisory alerts
o NIST publications and vulnerability alerts
o Other vendorospecific alerts like McAfee, Symantec, etc.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(5): HIPAA § 164.308(a)(5)

4.5 Security Awareness and Training : Do you perform staff training for policies and procedures for guarding against, detecting, and reporting malicious software? 164.308(a)(5)(ii)(B)

Module: Administrative Security Safeguards

Description: Train staff regarding security and privacy functions:
Security awareness training to all users before being granted access to the system, i.e. during new employee orientation.
o Security awareness training should be conducted in an onogoing basis. Ensuring acceptable antivirus protection on every workstation/server within the organization (i.e. McAfee, Symantec, etc.)
o Updated at least daily but would recommend every 4 hours
o Regularly scheduled antivirus scans of all systems, i.e. weekly or monthly
o Centralized administration, updating, and reporting is recommended
Being aware the use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including:
o Account locked due to failed attempts
o Failed attempts by unauthorized users
o Escalation of rights
o Installation of new services
o Event log stopped
o Virus activity, Spam protection performed on the workstations themselves and/or at the gateway (entry/exit point into the network)
o Workstation solutions include builtoin Microsoft Outlook Junkoemail option or McAfee/Symantec suites that include Spam protection with their antivirus solutions
o Gateway solutions include Websense, Barracuda Networks, TrendMicro, etc.

Response: No

Risk Description: You might not perform staff training for policies and procedures for guarding against, detecting, and reporting malicious software, so unprotected electronics could be be the target of attack.

Comments: No, we do not have this in place.

Action Plan: Implement training on policies and procedures for guarding against, detecting, and reporting malicious software.
Train staff regarding security and privacy functions:
Security awareness training to all users before being granted access to the system, i.e. during new employee orientation.
o Security awareness training should be conducted at an onogoing basis
Ensuring acceptable antivirus protection on every workstation/server within the organization (i.e. McAfee, Symantec, etc.)
o Updated at least daily but would recommend every 4 hours
o Regularly scheduled antivirus scans of all systems, i.e. weekly or monthly o Centralized administration, updating, and reporting is recommended
Being aware the use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including:
o Account locked due to failed attempts
o Failed attempts by unauthorized users
o Escalation of rights
o Installation of new services
o Event log stopped

o Virus activity
Spam protection performed on the workstations themselves and/or at the gateway (entry/exit point into the network) :
o Workstation solutions include builtoin Microsoft Outlook Junkoemail option or McAfee/Symantec suites that include Spam protection with their antivirus solutions
o Gateway solutions include Websense, Barracuda Networks, TrendMicro, etc.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(5): HIPAA § 164.308(a)(5)

4.6 Security Awareness and Training : Do you perform staff training for monitoring login attempts and reporting discrepancies? §164.308(a)(5)(ii)(C)

Module: Administrative Security Safeguards

Description: Staff should be trained pertaining login monitoring procedures include:
o Approval process for activating and modifying accounts to laptops/workstations and EHR systems (i.e. a network access request form which requires appropriate signatures before creating or modifying a user account)
o Process for disabling and removing accounts upon voluntary and involuntary employee terminations
o The provider reviewing user activities, utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls
o Email alerts of login failures, elevated access, and other events are recommended
o Audit logs compiled to a centralized location through the use of a syslog server
o Syslog servers for central monitoring and alerting of auditable events include Kiwisyslog, Gfi Event Manager, Syslog Manager, Solarwinds Syslog Monitor, Splunk Syslog
o Examples of auditable events include but are not limited to:
o Account creation
o Account modification
o Account disabled
o Account escalation
o Server health
o Network health
o Access allowed
o Access denied
o Service installation
o Service deletion
o Configuration changes
o Ensuring EMR and other audit logs are enabled and monitored regularly; email alerts also setup for login failures and other events.
o EHR software to log and track all access, specifying each user
o Enabling and monitoring of Windows Security Event Logs (workstation and servers), monitoring the other Event Logs as well (Application and System Logs).
o Monitoring of logs from networking equipment, i.e.switches, routers, wireless access points, and firewalls

Response: No

Risk Description: You might not perform staff training for monitoring login attempts and reporting discrepancies; unmonitored system access attempts could result in potential entry into the system using tools, social engineering, etc.

Comments: No, we do not cover this in our awareness training.

Action Plan: Implement training on procedures for monitoring login attempts and reporting discrepancies.
Approval process for activating and modifying accounts to laptops/workstations and EHR systems (i.e. a network access request form which requires appropriate signatures before creating or modifying a user account)
o Process for disabling and removing accounts upon voluntary and involuntary employee terminations
o The provider reviewing user activities, utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls
o Email alerts of login failures, elevated access, and other events are recommended
o Audit logs compiled to a centralized location through the use of a syslog server
o Syslog servers for central monitoring and alerting of auditable events include Kiwisyslog, Gfi Event Manager, Syslog Manager, Solarwinds Syslog Monitor, Splunk Syslog
o Examples of auditable events include but are not limited to:
o Account creation
o Account modification
o Account disabled
o Account escalation
o Server health
o Network health
o Access allowed
o Access denied
o Service installation
o Service deletion
o Configuration changes
o Ensuring EMR and other audit logs are enabled and monitored regularly; email alerts also setup for login failures and other events.
o EHR software to log and track all access, specifying each user
o Enabling and monitoring of Windows Security Event Logs (workstation and servers), monitoring the other Event Logs as well (Application and System Logs).
o Monitoring of logs from networking equipment, i.e.switches, routers, wireless access points, and firewalls

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(5): HIPAA § 164.308(a)(5)

4.7 Security Awareness and Training : Do you perform staff training for creating, changing, and safeguarding passwords? §164.308(a)(5)(ii)(D)

Module: Administrative Security Safeguards

Description: Staff receives training in password management best practices:
o Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria:
o Enforce password history. Previous 12 passwords cannot be used
o Maximum password age. Passwords should expire every 30 – 90 days
o Minimum password age. Passwords can only be changed manually by the user after 1 day
o Minimum password length. 8 or more characters long
o Password complexity. Passwords should contain 3 of the following criteria

o Uppercase characters (AoZ)
o Lowercase characters (aoz)
o Numbers (0o9)
o Special characters (i.e. !,#,&,*)
o Account lockout. Accounts lock after 3 unsuccessful password attempts
o Enforced in the EMR system, Active Directory, or at least on the local workstation or server
o Passwords include Microsoft logins (Active Directory Domain Controller or just locally logging into a computer) for each individual user. Unique username and password for EHR systems
o The use of passwords and/or tokens for remote access through a Virtual Private Network (VPN)
o Example token products include, RSA SecureID or Aladdin's eToken
o Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource
o Security awareness and training program to educate users and managers for safeguarding of passwords
o See 164.308(a)(5)(i)
o No shared access for any resource or system (i.e. computer or EHR system)
o The management of authenticators (i.e. security tokens). Management includes the procedures for initial distribution, lost/compromised or damaged authenticators, or revoking of authenticators
o Authenticators could be tokens, PKI certificates, biometrics, passwords, or keycards
o Authenticator feedback includes the displaying of asterisks when a user types in a password
o The goal is to ensure the system does not provide information that would allow an unauthorized user to compromise the authentication mechanism

Response: No

Risk Description: You might not perform staff training for creating, changing, and safeguarding passwords, which could compromise security and privacy of patient data.

Comments: No, we do not cover it in our training.

Action Plan: Implement training on procedures for creating, changing, and safeguarding passwords.
o Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria:
o Enforce password history. Previous 12 passwords cannot be used
o Maximum password age. Passwords should expire every 30 – 90 days
o Minimum password age. Passwords can only be changed manually by the user after 1 day
o Minimum password length. 8 or more characters long
o Password complexity. Passwords should contain 3 of the following criteria
o Uppercase characters (AoZ)
o Lowercase characters (aoz)
o Numbers (0o9)
o Special characters (i.e. !,#,&,*)
o Account lockout. Accounts lock after 3 unsuccessful password attempts
o Enforced in the EMR system, Active Directory, or at least on the local workstation or server
o Passwords include Microsoft logins (Active Directory Domain Controller or just locally logging into a computer) for each individual user. Unique username and password for EHR systems
o The use of passwords and/or tokens for remote access through a Virtual Private Network (VPN)
o Example token products include, RSA SecureID or Aladdin's eToken
o Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource
o Security awareness and training program to educate users and managers for safeguarding of passwords
o See 164.308(a)(5)(i)
o No shared access for any resource or system (i.e. computer or EHR system)
o The management of authenticators (i.e. security tokens). Management includes the procedures for initial distribution, lost/compromised or damaged authenticators, or revoking of authenticators
o Authenticators could be tokens, PKI certificates, biometrics, passwords, or keycards
o Authenticator feedback includes the displaying of asterisks when a user types in a password

o The goal is to ensure the system does not provide information that would allow an unauthorized user to compromise the authentication mechanism

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(5): HIPAA § 164.308(a)(5)

4.8 Facility Access Controls : Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data, under the disaster recovery plan and emergency mode operations plan, in the event of an emergency? (§164.310(a)(2)(i))

Module: Physical Security Safeguards

Description: Procedure for obtaining necessary PHI during an emergency should be part of the Contingency Plan
o Tape backups taken offsite to an authorized storage facility
o Identify alternate processing facility in case of disaster
o Ensure alternate work sites have appropriate administrative, physical, and technical safeguards

Response: No

Risk Description: You might not have established (and implemented as needed) procedures that allow facility access in support of the restoration of lost data, under the disaster recovery plan and emergency mode operations plan; alternate options may not be available to provide care during an emergency.

Comments: No, we do not have procedures in place.

Action Plan: Establish (and implement as needed) procedures that allow facility access in support of the restoration of lost data, under the disaster recovery plan and emergency mode operations plan, in the event of an emergency.
Procedure for obtaining necessary PHI during an emergency should be part of the Contingency Plan
o Tape backups taken offsite to an authorized storage facility
o Identify alternate processing facility in case of disaster
o Ensure alternate work sites have appropriate administrative, physical, and technical safeguards

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.310(a)(1): HIPAA § 164.310(a)(1)

4.9 Facility Access Controls : Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft? §164.310(a)(2)(ii)

Module: Physical Security Safeguards

Description: Policy and procedures that specify which physical and environmental safeguards used.
o 164.310(a)(2)(iii) outlines some specific safeguards that are recommended
o System security plan that specifies an overview of security requirements for the system and a description of the security controls in place or planned for meeting those requirements.
o Covered in the Information Security Policy Template, "Building and Physical Security" Section.

Response: No

Risk Description: You might not have implemented sufficient policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Lack of physical security poses a substantial risk for electronic devices that store or process ePHI.

Comments: No, we have not completely safeguarded the facility yet.

Action Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Policy and procedures that specify which physical and environmental safeguards used.
o 164.310(a)(2)(iii) outlines some specific safeguards that are recommended
o System security plan that specifies an overview of security requirements for the system and a description of the security controls in place or planned for meeting those requirements.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.310(a)(1): HIPAA § 164.310(a)(1)

HIPAA: Security Standards: Physical Safeguards

4.10 Facility Access Controls : Have you implemented 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? §164.310(a)(2)(iii)

Module: Physical Security Safeguards

Description: o Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL
o VPN access to office when connecting from home, hotel, etc., using IPSec
o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore, your firewall should not have TCP port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software
o Role-based access to data that allows access for users based on job function/role within the organization.
o This includes access to EMR systems, workstations, servers, networking equipment, etc.
o Policy and procedures that specify physical and environmental safeguards used.
o A list of personnel with authorized access to specific areas. If a card-access system is used then the list can be generated by the card-access system.

o The use of cipher locks and/or a card access control system to sensitive areas of the facility
o Cipher locks require a code for entry instead of just a standard physical key
o Keri Access Control System is an example of a system that requires the user to have a card to be swiped or held in front of a sensor for entry
o Monitoring physical access through the use of video cameras
o Control physical access by authenticating visitors at the front desk (or other sensitive areas) before authorizing access to the facility
o Presenting an authorized badge or ID for access
o Records of physical access are kept that including:
(i) name and organization of the person visiting;
(ii) signature of the visitor;
(iii)form of identification;
(iv) date of access;
(v) time of entry and departure;
(vi) purpose of visit;
(vii)name and organization of person visited.
o Designated personnel within the facility review the visitor access records daily.

Response: No

Risk Description: You might not have implemented 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. Unauthorized access to facilities can result in theft of devices that contain or process ePHI.

Comments: No, we are yet to implement access controls.

Action Plan: 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. Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL.
o VPN access to office when connecting from home, hotel, etc., using IPSec
o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefor,e your firewall should not have TCP port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software
o Role-based access to data that allows access for users based on job function / role within the organization.
o This includes access to EMR systems, workstations, servers, networking equipment, etc.
o Policy and procedures that specify physical and environmental safeguards used.
o A list of personnel with authorized access to specific areas. If a card-access system is used then the list can be generated by the card-access system.
o The use of cipher locks and/or a card access control system to sensitive areas of the facility
o Cipher locks require a code for entry instead of just a standard physical key
o Keri Access Control System is an example of a system that requires the user to have a card to be swiped or held in front of a sensor for entry
o Monitoring physical access through the use of video cameras
o Control physical access by authenticating visitors at the front desk (or other sensitive areas) before authorizing access to the facility
o Presenting an authorized badge or ID for access
o Records of physical access are kept that including:
(i) name and organization of the person visiting;
(ii) signature of the visitor;
(iii) form of identification;
(iv) date of access;
(v) time of entry and departure;
(vi) purpose of visit;

(vii) name and organization of person visited.
o Designated personnel within the facility review the visitor access records daily.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.310(a)(1): HIPAA § 164.310(a)(1)

4.11 Do you have a process in place to demonstrate that breach notifications were made on time and according to HITECH act requirements? §164.414

Module: Breach Notification Rules

Description: In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402.

Response: No

Risk Description: You might not have a process in place to demonstrate that breach notifications were made on time and according to HITECH act requirements. Lack of a process to demonstrate breach notifications were made properly could result in additional liabilities.

Comments: No, we do not have timely notification process in place.

Action Plan: Have a process in place to demonstrate that breach notifications were made on time and according to HITECH act requirements.
In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

4.12 Do you have a policy to delay the breach notification if the request is from a law enforcement authorities? §164.412

Module: Breach Notification Rules

Description: If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security... If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official. If the statement is made orally document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement... is submitted during that time.

Response: No

Risk Description: You might not have a policy to delay the breach notification if the request is from a law enforcement authorities. Lack of a process to delay notification upon request from law enforcement could prevent authorities from properly carrying out their investigation.

Comments: No, we do not have the process in place yet.

Action Plan: Have a policy in place to delay the breach notification if the request is from a law enforcement authorities.
If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security... If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official. If the statement is made orally document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement... is submitted during that time.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

4.13 Security Incident Procedures : Do you have procedures to identify and respond to suspected or known security incidents, mitigate to the extent practicable any harmful effects of known security incidents, and document incidents and their outcomes? §164.308(a)(6)(ii)

Module: Administrative Security Safeguards

Description: o Incident handling process can include audit monitoring of the EMR system, network monitoring, and physical access monitoring. The process should detail how the incident is reported, contained, eradicated, and then recovered.
o Track and document information system security incidents on an ongoing basis
o Reporting of incidents to the appropriate personnel i.e. designated Privacy Officer or Information Security Officer (ISO)
o The training of personnel for the handling and reporting of security incidents

Response: No

Risk Description: You might not have procedures to identify and respond to suspected or known security incidents, mitigate to the extent practicable any harmful effects of known security incidents, and document incidents and their outcomes. Unmanaged security incidents result in not notifying patients on time to mitigate the risks.

Comments: No, we do not have procedures in place yet.

Action Plan: Implement procedures to identify and respond to suspected or known security incidents, mitigate to the extent practicable any harmful effects of known security incidents, and document incidents and their outcomes.
o Incident handling process can include audit monitoring of the EMR system, network monitoring, and physical access monitoring. The process should detail how the incident is reported, contained, eradicated, and then recovered.
o Track and document information system security incidents on an ongoing basis
o Reporting of incidents to the appropriate personnel i.e. designated Privacy Officer or Information Security Officer (ISO)
o Training of personnel for the handling and reporting of security incidents

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(6): HIPAA § 164.308(a)(6)

4.14 Business Associate Contracts and Other Arrangements : Have you established written contracts or other arrangements with your trading partners that document satisfactory assurances that the BA will appropriately safeguard the information? §164.308(b)(4)

Module: Administrative Security Safeguards

Description: o Authorization and monitoring of all connections from the information system to other information systems, i.e. a VPN connection from the provider's system to an EMR software vendor.
o The organization requires that providers of external information systems (i.e. EMR vendors) employ adequate security controls in accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.
o This will ultimately involve a Business Associate Agreement but can also include additional contracts as well.
o Download Business Associate Agreement provisions and customize from our document template section.

Response: No

Risk Description: You might not have established written contracts or other arrangements with your trading partners that document satisfactory assurances that the BA will appropriately safeguard the information. PHI shared without a valid, up-to-date business associate contract exposes the provider to several liabilities, including HIPAA/HITECH security violation.

Comments: No, this is not in place yet.

Action Plan: o Establish written contracts or other arrangements with your trading partners that document satisfactory assurances that the BA will appropriately safeguard the information.
o Authorization and monitoring of all connections from the information system to other information systems, i.e. a VPN connection from the provider's system to an EMR software vendor.
o The organization requires that providers of external information systems (i.e. EMR vendors) employ adequate security controls in accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.
o This will ultimately involve a Business Associate Agreement but can also include additional contracts as well.
o Download sample Business Associate Agreement provisions and customize for your practice.

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(b)(1): HIPAA § 164.308(b)(1)

EHR 2.0: Business Associate Agreement Template

4.15 Contingency Plan : Have you established and implemented procedures to create and maintain retrievable exact copies of ePHI? §164.308(a)(7)(ii)(A)

Module: Administrative Security Safeguards

Description: o Perform nightly backups of PHI which are taken offsite on a daily, at a minimum weekly, basis to an authorized storage facility
o It's recommended that the storage location be at least 60 miles away
o Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis)
o All backups should be encrypted using FIPS 140-2 compliant software and algorithms
o Backups should be verified to help ensure the integrity of the files being backed up
o Even for hosted EMR solutions, it is important to ensure the vendor is performing these functions and that these procedures are part of the Agreement
o Covered in the Information Security Policy Template, "Data Backup and Contingency Plan" Section, Data Backup Plan" Subsection

Response: No

Risk Description: You might not have established and implemented procedures to create and maintain retrievable exact copies of ePHI. Lack of backup results in eventual loss of patient data needed to provide quality care.

Comments: No, we do not have a periodic backup.

Action Plan: Establish and implemented procedures to create and maintain retrievable exact copies of ePHI.
o Perform nightly backups of PHI which are taken offsite on a daily, at a minimum weekly, basis to an authorized storage facility
o It's recommended that the storage location be at least 60 miles away
o Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis)
o All backups should be encrypted using FIPS 140-2 compliant software and algorithms
o Backups should be verified to help ensure the integrity of the files being backed up
o Even for hosted EMR solutions, it is important to ensure the vendor is performing these functions and that these procedures are part of the Agreement

Status: In Progress

Priority: Medium

Target Date for Completion: 2019-11-30

Legal and Policy References:

HIPAA § 164.308(a)(7): HIPAA § 164.308(a)(7)

5 Managed or Not Present Risks

Problems that have been managed or are not present in your organization.

5.1 Physical Security Safeguards

5.1.1 Facility Access Controls : Have you implemented 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)? §164.310(a)(2)(iv)

Description: o Policies and procedures that specify maintenance to the facility
o Change management process that allows request, review, and approval of changes to the information system or facility
o Spare parts available for quick maintenance of hardware, doors, locks, etc.
Covered in the Information Security Policy Template, "Change Management Tracking Log" Appendix

Response: Yes

Comments: Yes, we have documentation for repairs in place.

Legal and Policy References:

HIPAA § 164.310(a)(1): HIPAA § 164.310(a)(1)

5.1.2 Workstation Use : Have you implemented 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 ePHI?

Description: 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.
Covered in the Information Security Policy Template, "Employee Responsibilities" Section, "Employee Requirements" Subsection.

Response: Yes

Comments: Yes, we have the procedures in place.

Legal and Policy References:

HIPAA § 164.310(b): HIPAA § 164.310(b)

5.1.3 Workstation Security : Have you implemented physical safeguards for all workstations that access ePHI, to restrict access to authorized users?

Description: Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.
Covered in the Information Security Policy Template, "Building and Physical Security" Section.

Response: Yes

Comments: Yes, we have restrictions in place.

Legal and Policy References:

HIPAA § 164.310(c): HIPAA § 164.310(c)

5.1.4 Device and Media Controls : Have you implemented policies and procedures to address final disposition of ePHI and/or hardware or electronic media on which it is stored? § 164.310(d)(2)(i)

Description: o Destruction of hard drives, removable media, etc, including:
o Physical destruction. There are companies like Retire-IT that offer these services and also come onsite to destroy media.
o DoD wiping of media before reuse. DoD wiping should also be performed even before physically destroying media. DoD wiping involves writing over the hard drive with random data 7 times before it's considered unrecoverable.
o Degaussing of media. Degaussing erases data from magnetic media through the use of powerful magnets or electrical energy.
Covered in the Information Security Policy Template, "Disposal of External Media / Hardware" Section.

Response: Yes

Comments: Yes, procedures are in place.

Legal and Policy References:

HIPAA § 164.310(d)(1): HIPAA § 164.310(d)(1)

NIST: Guidelines for Media Sanitization

5.1.5 Device and Media Controls : Have you implemented procedures for removal of ePHI from electronic media before the media are available for reuse? 164.310(d)(2)(ii)

Description: DoD wiping of media before reuse and should also be performed even before destroying media. DoD wiping involves writing over the hard drive with random data 7 times before it's considered unrecoverable. Covered in the Information Security Policy Template, "Disposal of External Media / Hardware" Section.

Response: Yes

Comments: Yes, we have wiping procedures in place.

Legal and Policy References:

HIPAA § 164.310(d)(1): HIPAA § 164.310(d)(1)

5.1.6 Device and Media Controls : Do you maintain a record of the movements of hardware and electronic media, along with the person responsible for its movement? 164.310(d)(2)(iii)

Description: o Maintain a record that shows who has what equipment.
o Records can be kept in an inventory system as well as a billing or help desk system.
o Media transported only by authorized personnel and secured in a locked container. All media should be encrypted using FIPS 140-2 compliant software or algorithms.
o The use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of interest agreements.

Response: Yes

Comments: Yes, we do have records.

Legal and Policy References:

HIPAA § 164.310(d)(1): HIPAA § 164.310(d)(1)

5.1.7 Device and Media Controls : Do you create a retrievable, exact copy of ePHI, when needed, before movement of equipment? 164.310(d)(2)(iv)

Description: o Perform daily/nightly, at minimum weekly backups of PHI taken offsite to an authorized storage facility; also backup before transporting any equipment.
o It's recommended that the storage location be at least 60 miles away.
o Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis).
o All backups should be encrypted using FIPS 140-2 compliant software and algorithms.
o Backups should be verified to help ensure the integrity of the files being backed up.
o Even for hosted EMR solutions, it is important to ensure the vendor is performing these functions and that these procedures are part of the Business Associate Agreement.
o Media (backup tapes, hard drives, removable media, etc.) should be stored in a locked safe while in the office and stored in a vault at an authorized facility when taken offsite.
o Media should also be transported in an approved locked container.
Covered in the Information Security Policy Template, "Change Management" Section.

Response: Yes

Comments: Yes, we do maintain exact copy of ePHI.

Legal and Policy References:

HIPAA § 164.310(d)(1): HIPAA § 164.310(d)(1)

5.2 Technical Security Safeguards

5.2.1 Access Control : Have you assigned a unique name and/or number for identifying and tracking user identities? §164.312(a)(2)(i)

Description: o Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system/resource.
o No shared access for any resource or system (i.e.computer or EHR system).
o Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria:
o Enforce password history. Previous 12 passwords cannot be used.
o Maximum password age. Passwords should expire every 30 – 90 days.
o Minimum password age. Passwords can only be changed manually by the user after 1 day.

o Minimum password length. 8 or more characters long.
o Password complexity. Passwords should contain 3 of the following criteria
o Uppercase characters (A-Z)
o Lowercase characters (a-z)
o Numbers (0-9)
o Special characters (i.e. !,#,&,*)
o Account lockout. Accounts lock after 3 unsuccessful password attempts.
o Enforced in the EMR system, Active Directory, or at least on the local workstation or server.
Covered in the Information Security Policy Template, "Identification and Authentication" Section, "User LogIn IDs" Subsection.

Response: Yes

Comments: Yes, we do have unique names to access systems.

Legal and Policy References:

HIPAA § 164.312(a)(1): HIPAA § 164.312(a)(1)

5.2.2 Access Control : Have you established (and implemented as needed) procedures for obtaining necessary ePHI during an emergency? §164.312(a)(2)(ii)

Description: o Procedure for obtaining necessary PHI during an emergency should be part of the Contingency Plan
o Break-the-Glass procedures in place to ensure there is a process where a person that normally would not have access privileges to certain information can gain access when necessary
o Any emergency accounts should be obvious and meaningful, i.e. breakglass1
o Strong password should be used
o Account permissions should still be set to minimum necessary.
o Auditing should be enabled.
o Approval process for activating and modifying accounts to laptops/workstations and EHR systems (i.e. a network access request form that requires appropriate. signatures before creating or modifying a user account).
o Process for disabling and removing accounts upon voluntary and involuntary terminations of staff.
o EHR software to log and track all access, specifying each user.
o Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic, and anything allowed has to be explicitly added to the ACL.
o VPN access to office when connecting from home, hotel, etc. using IPSec.
o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore your firewall should not have TCP port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software.
o Role-based access to data that allows access for users based on job function/role within the organization.
o This includes access to EMR systems, workstations, servers, networking equipment, etc.
o Use of Uninterruptable Power Supplies (UPS's) or generators in the event of a power outage to help ensure emergency access to computers, servers, wireless access points, etc. in the event of an emergency.
Covered in the Information Security Policy Template, "Data Backup and Contingency Plan" Section.

Response: Yes

Comments: Yes, we have procedures in place to retrieve ePHI.

Legal and Policy References:

HIPAA § 164.312(a)(1): HIPAA § 164.312(a)(1)

5.2.3 Access Control : Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? §164.312(a)(2)(iii)

Description: o Enforce session lock after 10 minutes of inactivity on the computer system. This can be enforced through Active Directory Group Policies if in a Windows Domain environment or at least set locally on the computer if not on a domain.
o Users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter).
o Session lock should not be more than 15 minutes for remote access (VPN access) and portable devices (laptops, PDA's, etc.).
o Terminate VPN sessions after 10-15 minutes of inactivity.
o Terminate terminal services or Citrix sessions after 10-15 minutes of inactivity.
o Terminate EHR sessions after 15 minutes of inactivity.

Response: Yes

Comments: Yes, we do have time out settings enabled on all systems.

Legal and Policy References:

HIPAA § 164.312(a)(1): HIPAA § 164.312(a)(1)

5.2.4 Access Control : Have you implemented a mechanism to encrypt and decrypt ePHI? §164.312(a)(2)(iv)

Description: o Use of full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.). Any solution should be FIPS 140-2 compliant.
o Use of email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server).
o The use of appropriate wireless encryption, including:
o WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption recommended (minimum of 128-bit).
o WPA/WPA2-Personal (the use of a pre-shared key).
o Never use WEP because it is flawed, easy to crack, and widely publicized as such.
o Use of IPSec VPN for remote access to the network.
o Use of encryption for backups (tape or back-to-disk storage).
o Use of SSL/TLS for web-based access to EHR software.
o Use of file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP).
o Use of encryption of removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.).
o Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL.
o VPN access to office when connecting from home, hotel, etc. using IPSec.
o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore your firewall should not have TCP port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software.
o Role-based access to data that allows access for users based on job function and role within the organization.
o This includes access to EMR systems, workstations, servers, networking equipment, etc.

Response: Yes

Comments: Yes, all ePHI is encrypted.

Legal and Policy References:

HIPAA § 164.312(a)(1): HIPAA § 164.312(a)(1)

5.2.5 Audit Controls : Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI? §164.312(b)

Description: o Policies and procedures that specify audit and accountability can be included as part of the general information security policy for the practice.
o It's recommended to have audit logs go to a central server by using a syslog server.
o Example syslog servers for central monitoring and alerting of auditable events include Kiwisyslog, Gfi Event Manager, Syslog Manager, Solarwinds Syslog Monitor, Splunk Syslog.
o Audit reduction, review, and reporting tools (i.e. a central syslog server) support after-the fact investigations of security incidents without altering the original audit records.
o Examples of auditable events include but are not limited to:
o Account creation.
o Account modification.
o Account disabled.
o Account escalation.
o Server health.
o Network health.
o Access allowed.
o Access denied.
o Service installation.
o Service deletion.
o Configuration changes.
o Ensure audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component); (iii) type of event; (iv) user/subject identity; (v) the outcome (success or failure) of the event.
o Ensure the computers, servers, wireless access points/routers, and/or networking devices that perform audit logging have sufficient storage capacity.
o Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events.
o Enabling and monitoring of Windows Security Event Logs (workstation and servers); also monitor the other Event Logs (Application and System Logs).
o Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points and firewalls.

Response: Yes

Comments: We regularly monitor audit log files and document the same.

Legal and Policy References:

HIPAA § 164.312(b): HIPAA § 164.312(b)

5.2.6 Integrity : Have you implemented electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner? §164.312(c)(2)

Description: o VPN access to office when connecting from home, hotel, etc. using IPSec.
o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore your firewall should not have TCP port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software.
o Use of SSL/TLS for Web-based EMR software.
o Use of digital certificates for email communications.
o Use of unique user ID's and passwords to EMR systems to help prevent unauthorized access or alteration to PHI.
o Use of PKI for email communication to help ensure both confidentiality and integrity of the message.
o Endpoint security solutions (i.e. McAfee Enterprise, Cisco CSA, Symantec Endpoint, etc) have the ability

to prevent unauthorized modification to software running on the computer or server.
o The use of appropriate wireless encryption, including:
o WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption recommended (minimum of 128-bit).
o WPA/WPA2-Personal (the use of a pre-shared key).
o Never use WEP because it is flawed, easy to crack, and widely publicized as such.

Response: Yes

Comments: Yes, we have this implemented.

Legal and Policy References:

HIPAA § 164.312(c)(1): HIPAA § 164.312(c)(1)

5.2.7 Person or Entity Authentication : Have you implemented Person or Entity Authentication procedures to verify that the person or entity seeking access ePHI is the one claimed? §164.312(d)

Description: o Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource
o No shared access for any resource or system (i.e. computer or EHR system)
o Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria:
o Enforce password history. Previous 12 passwords cannot be used.
o Maximum password age. Passwords should expire every 30 – 90 days.
o Minimum password age. Passwords can only be changed manually by the user after 1 day.
o Minimum password length. 8 or more characters long.
o Password complexity. Passwords should contain 3 of the following criteria.
- Uppercase characters (A-Z)
- Lowercase characters (a-z)
- Numbers (0-9)
- Special characters (i.e. !,#,&,*)
o Account lockout. Accounts lock after 3 unsuccessful password attempts.
o Enforced in the EMR system, Active Directory, or at least on the local workstation or server.
o The use of passwords and/or tokens for remote access through a Virtual Private Network (VPN).
o Example token products include RSA SecureID or Aladdin's eToken.
o The use of IP Address and Access Control Lists to allow or deny access to the EHR system or other resource.
o Microsoft Active Directory (Windows Domain Controller) to permit only authorized computers on the domain.

Response: Yes

Comments: Yes, we have the verification procedures.

Legal and Policy References:

HIPAA § 164.312(d): HIPAA § 164.312(d)

5.2.8 Transmission Security : Have you implemented security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of? §164.312(e)(2)(i)

Description: o Use of cryptographic hashing functions such as SHA.
o VPN access to office when connecting from home, hotel, etc. using IPSec.
o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore your firewall should not have TCP port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software.
o Use of SSL/TLS for Web-based EMR software.
o Use of digital certificates for email communications.
o Use of unique user ID's and passwords to EMR systems to help prevent unauthorized access or alteration to PHI.
o Use of PKI for email communication to help ensure both confidentiality and integrity of the message.
o Endpoint security solutions (i.e. McAfee Enterprise, Cisco CSA, Symantec Endpoint, etc.) have the ability to prevent unauthorized modification to software running on the computer or server.
o Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events.
o Enabling and monitoring of Windows Security Event Logs (workstation and servers); also monitor the other Event Logs (Application and System Logs).
o Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls.
o Audit reduction, review, and reporting tools (i.e. a central syslog server) supporting after-the-fact investigations of security incidents without altering the original audit records.
o Continuous monitoring of the information system using manual and automated methods.
o Manual methods include the use of designated personnel or an outsourced provider that manually reviews logs or reports on a regular basis, i.e. every morning.
o Automated methods include the use of email alerts generated from syslog servers, servers and networking equipment, and EMR software alerts to designated personnel.
o Track and document information system security incidents on an ongoing basis.
o Report incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO).
o Use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including:
o Account locked due to failed attempts.
o Failed attempts by unauthorized users.
o Escalation of rights.
o Installation of new services.
o Event log stopped.
o Virus activity.

Response: Yes

Comments: Yes, we have detection process in place.

Legal and Policy References:

HIPAA § 164.312(e)(1): HIPAA § 164.312(e)(1)

5.2.9 Transmission Security : Have you implemented a mechanism to encrypt ePHI whenever deemed appropriate? §164.312(e)(2)(ii)

Description: VPN access to office when connecting from home, hotel, etc. using IPSec
o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore your firewall should not have TCP port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software.
o Use of SSL/TLS for Web-based EMR software.
o Use of PKI for email communications.
o Use of a centralized certificate server to assign certificates to Active Directory users and computers.
o Use of full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.). Any solution should be FIPS 140-2 compliant.
o Use of email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server).
o Use of FIPS 140-2 compliant encryption for backups (tape or back-to-disk storage).
o Use of SSL/TLS for web-based access to EHR software.
o Use of file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP).
o Use of encryption of removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.).
o The use of appropriate wireless encryption, including:
o WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption recommended (minimum of 128-bit).
o WPA/WPA2-Personal (the use of a pre-shared key).
o Never use WEP because it is flawed, easy to crack, and widely publicized as such.

Response: Yes

Comments: Yes, we have encryption in place wherever it is applicable.

Legal and Policy References:

HIPAA § 164.312(e)(1): HIPAA § 164.312(e)(1)

5.3 Administrative Security Safeguards

5.3.1 Security Management Process : Does your organization conduct an accurate and thorough risk analysis on a regular basis for assessing and managing risks to its ePHI? § 164.308(a)(1)(ii)(A)

Description: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
Covered in the Information Security Policy Template, "Security Management Process" Section.

Uploaded File(s): 14339660465518960_TEST_ZDlgUTk

Response: Yes

Comments: We conduct thorough and comprehensive security risk assessment at least on an annual basis.

Legal and Policy References:

HIPAA § 164.308(a)(1): HIPAA § 164.308(a)(1)

5.3.2 Security Management Process : Does your organization have a formal process to discipline workforce members who have access to your organization's ePHI if they are found to have violated the practice's policies to prevent system misuse, abuse, or any harmful activities that involve your practice's ePHI? § 164.308(a)(1)(ii)(C)

Description: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

Response: Yes

Comments: Workforce sanction policy is in place and actively enforced.

Legal and Policy References:

HIPAA § 164.308(a)(1): HIPAA § 164.308(a)(1)

5.3.3 Security Management Process : Have you implemented procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking? § 164.308(a)(1)(ii)(D)

Description: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Covered in the Information Security Policy Template, "Audit Controls" Section

Response: Yes

Comments: Activity logs, access reports, and security incidents are regularly monitored and actively managed.

Legal and Policy References:

HIPAA § 164.308(a)(1): HIPAA § 164.308(a)(1)

5.3.4 Assigned Security Responsibility : Have you assigned a security official qualified enough to assess the practice's security protections as well as serve as the point of contact for security policies, procedures, monitoring, and training? § 164.308(a)(3)(ii)(A)

Description: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

Response: Yes

Comments: Yes, we have a security officer to act as a point of contact.

Legal and Policy References:

HIPAA § 164.308(a)(2): HIPAA § 164.308(a)(2)

5.3.5 Workforce Security : Does your organization have a list that includes all members of its workforce, the roles assigned to each, and the corresponding access that each role enables for your organization's facilities, information systems, electronic devices, and ePHI? § 164.308(a)(3)(ii)(A)

Description: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
Covered in the Information Security Policy Template, "Employee Hiring and Termination Checklist" Appendix.

Response: Yes

Comments: Yes, we maintain an active list of role assignments to handle ePHI.

Legal and Policy References:

HIPAA § 164.308(a)(3): HIPAA § 164.308(a)(3)

5.3.6 Information Access Management : Have you implemented policies and procedures to protect ePHI from the larger organization? (§164.308(a)(4)(ii))

Description: Policies and procedures should be in place to help protect ePHI data from the larger organization that may not require access to the data. The organization may have a shared network, so it is important for the safeguards to limit or isolate access to ePHI for only those that are specifically authorized.
The safeguards should include:
o Restricted user access on laptops and workstations to help prevent software installations and modifications to the Operating System and its services
o Use of Microsoft Active Directory (Windows Domain Controller) accounts to limit permissions based on role or job function
o Firewall Access Control List set to deny access by default and to only allow the needed access (ports, protocols, and services) through Covered in the Information Security Policy Template, "Identification and Authentication" Section.

Response: Yes

Comments: Yes, it's in place.

Legal and Policy References:

HIPAA § 164.308(a)(4): HIPAA § 164.308(a)(4)

5.3.7 Security Management Process : Does your organization have a formal, documented program to mitigate the threats and vulnerabilities to ePHI identified through the risk analysis? § 164.308(a)(1)(ii)(B)

Description: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply.

Response: Yes

Comments: Updated risk management plan is being maintained to ensure risks identified through security risk analysis are being actively managed.

Legal and Policy References:

HIPAA § 164.308(a)(1): HIPAA § 164.308(a)(1)

5.3.8 Information Access Management : Have you implemented policies and procedures for granting access to ePHI, for example through access to a workstation, transaction, program, or process? §164.308(a)(4)(ii)(B)

Description: Policy and procedures that specify how and when access is granted to EHR systems, laptops, etc. to only those individuals that require access at that time:
o Approval process for activating and modifying accounts to laptops/workstations and EHR systems (i.e. a network access request form that requires appropriate signatures before creating or modifying a user account)
o Process for disabling and removing accounts for voluntary and involuntary terminations.
o EHR software to log and track all access which specifies each user.
o Role-based access to data that allows access for users based on job function/role within the organization.
o This includes access to EMR systems, workstations, servers, networking equipment, etc.
o Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic, and anything allowed has to be explicitly added to the ACL.
o The provider reviews the activities of users utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls.
o Email alerts of login failures, elevated access, and other events are recommended Audit logs should be compiled to a centralized location through the use of a syslog server.
o The use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of interest agreements.
o Security policy for third-party personnel and monitoring of compliance to the security policy.
o Third-party personnel include EMR vendors, outsourced IT functions, and any other third party provider or contractor.
Covered in the Information Security Policy Template, "Identification and Authentication" Section.

Response: Yes

Comments: Yes, procedures to grant access are in place.

Legal and Policy References:

HIPAA § 164.308(a)(4): HIPAA § 164.308(a)(4)

5.3.9 Information Access Management : Have you implemented policies and procedures that are based upon your access authorization policies to establish, document, review, and modify a user's rights of access to a workstation, transaction, program, or process? §164.308(a)(4)(ii)(C)

Description: Information Access Management generally includes the following aspects:
o Policies and procedures that specify how and when access is granted to EHR systems, laptops, etc. to only those individuals that require access.
o Approval process for activating and modifying accounts to laptops/workstations and EHR systems (i.e. a network access request form that requires appropriate signatures before creating or modifying a user account).
o Process for disabling and removing accounts for voluntary and involuntary terminations.
o EHR software to log and track all access, which specifies each user Covered in the Information Security Policy Template, "Identification and Authentication" Section, "User Login Entitlement Reviews" Subsection.

Response: Yes

Comments: It's in place.

Legal and Policy References:

HIPAA § 164.308(a)(4): HIPAA § 164.308(a)(4)

5.3.10 Contingency Plan : Have you established (and implemented as needed) procedures to restore any loss of ePHI data that is stored electronically? §164.308(a)(7)(ii)(B)

Description: o Procedure in place for obtaining necessary PHI during an emergency. This should be part of your Contingency Plan
o Identified an alternate processing facility in case of disaster
o The use of not only primary but also alternate telecommunication services in the event that the primary telecommunication capabilities are unavailable
o The time to revert to the alternate service is defined by the organization and is based on the critical business functions
o An example would be as simple as forwarding the main office number to an alternate office or even a cell phone
o Perform nightly backups of PHI which are taken offsite on a daily, at a minimum weekly, basis to an authorized storage facility
o It's recommended that the storage location be at least 60 miles away
o Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis)
o All backups should be encrypted using FIPS 140-2 compliant software and algorithms
o Backups should be verified to help ensure the integrity of the files being backed up
o Even for hosted EMR solutions, it is important to ensure the vendor is performing these functions and that these procedures are part of the Agreement

Response: Yes

Comments: Yes, procedures are in place to restore the loss of data.

Legal and Policy References:

HIPAA § 164.308(a)(7): HIPAA § 164.308(a)(7)

5.3.11 Contingency Plan : Have you implemented procedures for periodic testing and revision of contingency plans? §164.308(a)(7)(ii)(D)

Description: o Training of personnel in their contingency roles and responsibilities
o Training should occur at least annually
o Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness and document the results
o Reviewing the contingency plan at least annually and revise the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing.)

Response: Yes

Comments: Yes, periodic testing of contingency plans is in place.

Legal and Policy References:

HIPAA § 164.308(a)(7): HIPAA § 164.308(a)(7)

5.3.12 Contingency Plan : Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? §164.308(a)(7)(ii)(E)

Description: o Procedure for obtaining necessary PHI during an emergency should be part of the Contingency Plan
o Business Impact Analysis (BIA) will help determine the criticality of specific applications and data
o Categorize the information system based on guidance from FIPS 199, which defines three levels of potential impact on organizations or individuals, should there be a breach of security (i.e. a loss of confidentiality, integrity, or availability)
o Potential impact options are Low, Moderate, or High
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdfCovered in the Information Security Policy Template, "Security Management Process" Section, along with "ePHI Inventory Template" Document

Response: Yes

Comments: Yes, criticality of applications/data has been completed.

Legal and Policy References:

HIPAA § 164.308(a)(7): HIPAA § 164.308(a)(7)

NIST: Standards for Security Categorization of Federal Information and Information Systems

5.3.13 Evaluation : Have you established a plan for periodic technical and nontechnical evaluation of the standards under this rule, in response to environmental or operational changes, affecting the security of ePHI? §164.308(a)(8)

Description: 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 electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements.
Covered in the Information Security Policy Template, "Security Management Process" Section.

Response: Yes

Comments: Yes, periodic evaluation is in place.

Legal and Policy References:

HIPAA § 164.308(a)(8): HIPAA § 164.308(a)(8)

5.4 Organizational Requirements

5.4.1 Business Associate Contracts or Other Arrangements : Are you in compliance according to the contract requirements listed below?

Description: A covered entity or business associate is not in compliance with the standards if the covered entity or business associate knew of a pattern of any activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation, under the contract or other arrangement, unless the covered entity took reasonable steps to remedy the breach or end the violation, as applicable, and if such steps were unsuccessful:
(A) Terminated the contract or arrangement, if feasible
or
(B) If termination is not feasible, reported the problem to the Secretary

Response: Yes

Comments: Yes, we have updated contracts in place with all business associates.

Legal and Policy References:

HIPAA § 164.314(a)(1): HIPAA § 164.314(a)(1)

5.4.2 Requirements for Group Health Plans : Do your plan documents require the plan sponsor to reasonably and appropriately safeguard ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan?

Description: A group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.
The plan documents of the group health plan must incorporate provisions to require the plan sponsor to:
o Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.
o Ensure that the adequate separation required by § 164.504(f)(2)(iii) [of the Privacy Rule] is supported by reasonable and appropriate security measures.
o Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.
o Report to the group health plan any security incident of which it becomes aware.

Response: Yes

Comments: Yes, we do have provisions for the plan sponsor to comply with the safeguards of HIPAA

Legal and Policy References:

HIPAA § 164.314(b)(1): HIPAA § 164.314(b)(1)

5.5 Policies and Procedures and Documentation Requirements

5.5.1 Policies and Procedures : Have you confirmed the policies and procedures documents are current? (§ 164.316(b)(1))

Description: Implement reasonable and appropriate policies and procedures to comply with the standards and implementation specifications. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
o Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and
o If an action, activity, or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.
Necessary document templates are included by EHR 2.0. Practice is responsible for maintaining and keeping up to date.

Response: Yes

Comments: Yes, documents and policies are up-to-date.

Legal and Policy References:

HIPAA § 164.316(a): HIPAA § 164.316(a)

EHR 2.0: Information Security Policy Template

5.6 Breach Notification Rules

5.6.1 Do you have a process in place to conduct risk assessment of a data breach? §164.402

Description: Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule, which compromises the security or privacy of the protected health information. It is presumed to be a breach unless the covered entity or business associate as applicable evidence demonstrating that there is a low probability that the protected health information has been compromised, based on a risk assessment of at least the following factors:
o The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
o The unauthorized person who used the protected health information or to whom the disclosure was made.
o Whether the protected health information was actually acquired or viewed.
o The extent to which the risk to the protected health information has been mitigated.

Response: Yes

Comments: Yes, we do have data breach risk assessment policies in place.

Legal and Policy References:

EHR 2.0: Policy on Breaches of Unsecured PHI Template

5.6.2 Do you have a process for notification to individuals following the event of a breach of unsecured PHI? §164.404

Description: Except as provided in § 164.412 [Law enforcement delay], a covered entity shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
"The notification... shall include, to the extent possible:
o A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
o A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
o Any steps individuals should take to protect themselves from potential harm resulting from the breach;
o A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
o Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
The notification... shall be written in plain language.
o Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.
o If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.
In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual..., a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual...
...such substitute notice may be provided by an alternative form of written notice, telephone, or other means.
...such substitute notice shall:

o Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
o Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to [written notice.]"

Response: Yes

Comments: Yes, we do have a process in place.

5.6.3 Do you have a process for notification to the media following the event of a breach of unsecured PHI? §164.406

Description: Except as provided in § 164.412 (Law enforcement delay), a covered entity shall provide the notification... without unreasonable delay and in no case later than 60 calendar days after discovery of a breach (same as in 164.404).

Response: Yes

Comments: Yes, we do have a process in place.

5.6.4 Do you have a process for notification to the secretary following the event of a breach of unsecured PHI? §164.408

Description: Breaches involving 500 or more individuals:
"A covered entity shall, except as provided in § 164.412 {Law enforcement delay], provide the notification required contemporaneously with the [notice to individuals] and in the manner specified on the HHS Web site."
Breaches involving less than 500 individuals:"A covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification... for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site."

Response: Yes

Comments: Yes, we do have this process in place.

5.6.5 Do you require your business associate to notify the covered entity following the event of any breach of unsecured PHI? §164.410

Description: Except as provided in §164.412 (Law enforcement delay), a business associate shall provide the notification... without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
The notification... shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach, (and) any other available information that the covered entity is required to include in notification to the individual, (at the same time) or promptly thereafter as information becomes available.

Response: Yes

Comments: Yes, we do have this requirement in place.

6 Unidentified Risks

Risks that have not been identified yet due to question not being answered.

6.1 HIPAA Privacy Rule

6.1.1 Have you developed and implemented minimum necessary policies for PHI? (§164.502 and §164.514)

6.1.2 Have you developed polices for business associate (BA) relationships and amended business associate contracts as required? (§164.504)

6.1.3 Do you limit PHI disclosures to those that are authorized by the client, or that are required or allowed by the privacy regulations and state law?

6.1.4 Do you share updated Notice of Privacy Practices (NPP) with all your patients? (§164.520)

6.1.5 Do you have policies for alternative means of communication requests? (§164.522)

6.1.6 Do you have policies for access to designated record sets? (§164.524)

6.1.7 Do you have policies for amendment requests? (§164.526)

6.1.8 Do you have policies for accounting of disclosures? (§164.528)

6.1.9 Have you implemented Privacy Rule Administrative requirements? (§164.530)
