Project Report: "HHA-1.4-All-N"

-

Contents

Risks that have been identified, evaluated and have an Action Plan

Problems that have been managed or are not present in your organisation

Risks that have been identified, evaluated and have an Action Plan

1 HIPAA/HITECH Administrative Security Safeguards

1.1 Security Management Process (§ 164.308(a)(1))

1.1.1 Your practice may not have adequate controls to safeguard ePHI if it does not develop and implement policies and procedures for assessing and managing risk to its ePHI.

This is a risk_priority_high priority risk.

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.

Measure

General approach (to eliminate or reduce the risk)

Conduct an accurate and thorough risk analysis for assessing and managing risks to ePHI. Perform Risk Analysis immediately then repeat on at least an annual basis. Update as needed to reflect changes in the company and overall security landscape.

Specific action(s) required to implement this approach

Identify all technology that will store or process PHI and evaluate which may be susceptible to data breach.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.1.2 Your practice may not be able to implement effective safeguards to manage risks to ePHI without a formal, documented program to mitigate threats and vulnerabilities identified by conducting the risk analysis.

This is a risk_priority_high priority risk.

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

Measure

General approach (to eliminate or reduce the risk)

Develop and follow a formal, documented program to mitigate threats and vulnerabilities to ePHI identified through the risk analysis.

Specific action(s) required to implement this approach

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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.1.3 Your practice may be unable to hold workforce members accountable (and take appropriate disciplinary action) if it does not have documented policies, procedures, and processes for disciplining those who violated the security policies and procedures put into place to safeguard your practice's ePHI.

This is a risk_priority_high priority risk.

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

Measure

General approach (to eliminate or reduce the risk)

Develop and implement 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.

Specific action(s) required to implement this approach

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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.1.4 Your practice may not be able to detect and prevent security violations or unauthorized uses/disclosures of ePHI without policies and procedures for reviewing information system activity.

This is a risk_priority_high priority risk.

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Measure

General approach (to eliminate or reduce the risk)

Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events. □ Enabling and monitoring of Windows Security Event Logs (workstation and servers). It is also important to monitor the other Event Logs (Application and System Logs). □ Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls □ Audit reduction, review, and reporting tools (i.e. a central syslog server) supports after-the-fact investigations of security incidents without altering the original audit records. □ Continuous monitoring of the information system by 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, networking equipment, and EMR software alerts to designated personnel. □ Track and document information system security incidents on an ongoing basis □ Reporting of incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO) □ 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 Indicators of attempts by unauthorized users o Escalation of rights o Installation of new services o Event log stopped o Virus activity

Specific action(s) required to implement this approach

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.2 Assigned Security Responsibility (§ 164.308(a)(2))

1.2.1 You are in violation if no security point of contact is assigned and

qualified to complete a security risk analysis and also serve as the point of contact for security policies, procedures, monitoring, and training.

This is a risk_priority_high priority risk.

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.

Measure

General approach (to eliminate or reduce the risk)

Assign a security point of contact 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.

Specific action(s) required to implement this approach

Identify and designate the security official who is responsible for the development and implementation of policies and procedures required for the covered entity or business associate.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.3 Workforce Security (§ 164.308(a)(3))

1.3.1 Individuals without a need to know can access your practice’s ePHI if there is no list that includes all members of the workforce, the roles assigned to each, and the corresponding access privileges for each role (including information systems, electronic devices, and ePHI).

This is a risk_priority_high priority risk.

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.

Measure

General approach (to eliminate or reduce the risk)

Maintain a list that includes all members of the firm's workforce, the roles assigned to each, and the corresponding access that each role enables for your practice’s facilities, information systems, electronic devices, and ePHI.

Specific action(s) required to implement this approach

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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.3.2 Unqualified or untrustworthy users could access your practice's ePHI if policies and procedures do not exist for screening workforce members prior to enabling access to facilities, information systems, and ePHI.

This is a risk_priority_high priority risk.

Implement procedures to determine that the access of workforce members to electronic protected health information is appropriate and the individuals are trustworthy.

Measure

General approach (to eliminate or reduce the risk)

Screen workforce members prior to enabling access to facilities, information systems, and ePHI to verify that users are trustworthy.

Specific action(s) required to implement this approach

Implement procedures to determine that the access of workforce members to electronic protected health information is appropriate and the individuals are trustworthy.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.3.3 A terminated employee, contractor, or other individual previously granted access to PHI continues to have access.

This is a risk_priority_high priority risk.

Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.

Measure

General approach (to eliminate or reduce the risk)

Set policies and procedures to perform timely actions to ensure that workforce termination procedures are appropriately followed.

Specific action(s) required to implement this approach

Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.4 Information Access Management (§ 164.308(a)(4))

1.4.1 Policies and procedures are not in place to protect ePHI data from the larger organization that may not require access to the data.

This is a risk_priority_high priority risk.

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: Restricted user access on laptops and workstations to help prevent software installations and modifications to the Operating System and its services Use of Microsoft Active Directory (Windows Domain Controller) accounts to limit permissions based on role or job function Firewall Access Control List set to deny access by default and to only allow the needed access (ports, protocols, and services) through

Measure

General approach (to eliminate or reduce the risk)

Implement policies and procedures to protect ePHI from the larger organization.

Specific action(s) required to implement this approach

Apply safeguards to limit or isolate access to ePHI for only those that are specifically authorized. The safeguards should include: - Restricted user access on laptops and workstations to help prevent software installations and modifications to the Operating System and its services - Use of Microsoft Active Directory (Windows Domain Controller) accounts to limit permissions based on role or job function - Firewall Access Control List set to deny access by default and to only allow the needed access (ports, protocols, and services) through

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.4.2 Not managing access to ePHI systems can result in improper disclosure of Protected Health Information.

This is a risk_priority_high priority risk.

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: 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) Process for disabling and removing accounts for voluntary and involuntary terminations EHR software to log and track all access which specifies each user 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. 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 The provider reviews the activities of users utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls. 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 The use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-ofinterest agreements 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

Measure

General approach (to eliminate or reduce the risk)

Implement policies and procedures for granting access to ePHI, for example through access to a workstation, transaction, program, or process.

Specific action(s) required to implement this approach

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: 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) Process for disabling and removing accounts for voluntary and involuntary terminations EHR software to log and track all access which specifies each user 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. 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 The provider reviews the activities of users utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls. 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 The use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-ofinterest agreements 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.4.3 Access not managed based on a "Need to Know" and "Minimum Necessary" basis introduces risk to patient data privacy and security.

This is a risk_priority_high priority risk.

Information Access Management generally includes the following aspects: Policies and procedures that specify how and when access is granted to EHR systems, laptops, etc. to only those individuals that require access 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) Process for disabling and removing accounts for voluntary and involuntary terminations EHR software to log and track all access, which specifies each user

Measure

General approach (to eliminate or reduce the risk)

Implement 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.

Specific action(s) required to implement this approach

Information Access Management should include the following aspects: Policies and procedures that specify how and when access is granted to EHR systems, laptops, etc. to only those individuals that require access 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) Process for disabling and removing accounts for voluntary and involuntary terminations EHR software to log and track all access, which specifies each user

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.5 Security Awareness and Training (§ 164.308(a)(5))

1.5.1 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.

This is a risk_priority_high priority risk.

Security awareness training to all users, i.e. during new employee orientation then periodic reminders Examples of providing information security reminders include: - Face-to-face meetings - Email updates - Newsletters - Postings in public areas, i.e. hallways, kitchen - 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: - Cisco security alerts - CERT advisory alerts - NIST publications and vulnerability alerts - Other vendor-specific alerts like McAfee, Symantec, etc.

Measure

General approach (to eliminate or reduce the risk)

Provide periodic information security reminders to all staff.

Specific action(s) required to implement this approach

- Security awareness training to all users before authorizing access to the system, i.e. during new employee orientation - Examples of providing information security reminders include: - Face-to-face meetings - Email updates - Newsletters - Postings in public areas, i.e. hallways, kitchen - 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: - Cisco security alerts - CERT advisory alerts - NIST publications and vulnerability alerts - Other vendor-specific alerts like McAfee, Symantec, etc.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.5.2 Unprotected electronics could be easily be the target of attack.

This is a risk_priority_high priority risk.

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. - Security awareness training should be conducted at an on-going basis Ensuring acceptable antivirus protection on every workstation/server within the organization (i.e. McAfee, Symantec, etc.) - Updated at least daily but would recommend every 4 hours - Regularly scheduled antivirus scans of all systems, i.e. weekly or monthly - 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: - Account locked due to failed attempts - Failed attempts by unauthorized users - Escalation of rights - Installation of new services - Event log stopped - Virus activity Spam protection performed on the workstations themselves and/or at the gateway (entry/exit point into the network) - Workstation solutions include built-in Microsoft Outlook Junk-email option or McAfee/Symantec suites that include Spam protection with their antivirus solutions - Gateway solutions include Websense, Barracuda Networks, TrendMicro, etc.

Measure

General approach (to eliminate or reduce the risk)

Implement policies and procedures for guarding against, detecting, and reporting

malicious software.

Specific action(s) required to implement this approach

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. - Security awareness training should be conducted at an on-going basis Ensuring acceptable antivirus protection on every workstation/server within the organization (i.e. McAfee, Symantec, etc.) - Updated at least daily but would recommend every 4 hours - Regularly scheduled antivirus scans of all systems, i.e. weekly or monthly - 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: - Account locked due to failed attempts - Failed attempts by unauthorized users - Escalation of rights - Installation of new services - Event log stopped - Virus activity Spam protection performed on the workstations themselves and/or at the gateway (entry/exit point into the network) - Workstation solutions include built-in Microsoft Outlook Junk-email option or McAfee/Symantec suites that include Spam protection with their antivirus solutions - Gateway solutions include Websense, Barracuda Networks, TrendMicro, etc.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.5.3 Unmonitored system access attempts result in potential entry into the system using tools, social engineering, etc.

This is a risk_priority_high priority risk.

Staff should be trained pertaining login monitoring procedures include:· 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) · Process for disabling and removing accounts upon voluntary and involuntary employee terminations · The provider reviewing user activities, utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls · Email alerts of login failures, elevated access, and other events are recommended · 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 · 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 · 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 · Enabling and monitoring of Windows Security Event Logs (workstation and servers), monitoring the other Event Logs as well (Application and System Logs). · Monitoring of logs from networking equipment, i.e.switches, routers, wireless access points, and firewalls

Measure

General approach (to eliminate or reduce the risk)

Implement procedures for monitoring login attempts and reporting discrepancies.

Specific action(s) required to implement this approach

· 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) · Process for disabling and removing accounts upon voluntary and involuntary employee terminations · The provider reviewing user activities, utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls · Email alerts of login failures, elevated access, and other events are recommended · 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 · 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 · 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 · Enabling and monitoring of Windows Security Event Logs (workstation and servers), monitoring the other Event Logs as well (Application and System Logs). · Monitoring of logs from networking equipment, i.e.switches, routers, wireless access points, and firewalls

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.5.4 Unmanaged ePHI system passwords directly compormise security and privacy of patient data.

This is a risk_priority_high priority risk.

Staff receives training in password management best practices:· 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 · 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 · 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 · Each user has a unique identifier

(i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource · Security awareness and training program to educate users and managers for safeguarding of passwords o See 164.308(a)(5)(i) · No shared access for any resource or system (i.e. computer or EHR system) · 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

Measure

General approach (to eliminate or reduce the risk)

Implement procedures for creating, changing, and safeguarding passwords.

Specific action(s) required to implement this approach

· 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 · 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 · 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 · Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource · Security awareness and training program to educate users and managers for safeguarding of passwords o See 164.308(a)(5)(i) · No shared access for any resource or system (i.e. computer or EHR system) · 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.6 Security Incident Procedures (§ 164.308(a)(6))

1.6.1 Unmanaged security incidents result in not notifying patients on time to mitigate the risks.

This is a risk_priority_high priority risk.

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. Track and document information system security incidents on an ongoing basis Reporting of incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO) The training of personnel for the handling and reporting of security incidents

Measure

General approach (to eliminate or reduce the risk)

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.

Specific action(s) required to implement this approach

- 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. - Track and document information system security incidents on an ongoing basis - Reporting of incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO) - Training of personnel for the handling and reporting of security incidents

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.7 Contingency Plan (§ 164.308(a)(7))

1.7.1 Lack of backup results in eventual loss of patient data needed to provide quality care.

This is a risk_priority_high priority risk.

· 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 · Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) · All backups should be encrypted using FIPS 140-2 compliant software and algorithms · Backups should be verified to help ensure the integrity of the files being backed up · 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

Measure

General approach (to eliminate or reduce the risk)

Establish and implemented procedures to create and maintain retrievable exact copies of ePHI.

Specific action(s) required to implement this approach

· 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 · Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) · All backups should be encrypted using FIPS 140-2 compliant software and algorithms · Backups should be verified to help ensure the integrity of the files being backed up · 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.7.2 When ePHI data cannot be restored from the backup copy, up-to-date patient clinical data is not available for providers.

This is a risk_priority_high priority risk.

· Procedure in place for obtaining necessary PHI during an emergency. This should be part of your Contingency Plan · Identified an alternate processing facility in case of disaster · 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 · 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 · Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) · All backups should be encrypted using FIPS 140-2 compliant software and algorithms · Backups should be verified to help ensure the integrity of the files being backed up · 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

Measure

General approach (to eliminate or reduce the risk)

Establish (and implement as needed) procedures to restore any loss of ePHI data that is stored electronically.

Specific action(s) required to implement this approach

· Procedure in place for obtaining necessary PHI during an emergency. This should be part of your Contingency Plan · Identified an alternate processing facility in case of disaster · 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 · 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 · Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) · All backups should be encrypted using FIPS 140-2 compliant software and algorithms · Backups should be verified to help ensure the integrity of the files being backed up · 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.7.3 Without security of the data being considered during emergency mode operation, potential data loss could occur during the most vulnerable period of the business.

This is a risk_priority_high priority risk.

· Procedure for obtaining necessary PHI during an emergency should be part of the contingency plan · The training of personnel in their contingency roles and responsibilities o Training should occur at least annually · Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness then document the results · 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) · 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.

Measure

General approach (to eliminate or reduce the risk)

Establish (and implement as needed) procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode.

Specific action(s) required to implement this approach

· Procedure for obtaining necessary PHI during an emergency should be part of the contingency plan · The training of personnel in their contingency roles and responsibilities o Training should occur at least annually · Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness then document the results · 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) · 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.7.4 An untested contigency plan may result in incomplete recovery during the actual contigency situation.

This is a risk_priority_high priority risk.

· Training of personnel in their contingency roles and responsibilities · Training should occur at least annually · Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness and document the results · 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.)

Measure

General approach (to eliminate or reduce the risk)

Implement procedures for periodic testing and revision of contingency plans.

Specific action(s) required to implement this approach

· Training of personnel in their contingency roles and responsibilities · Training should occur at least annually · Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness and document the results · 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.)

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.7.5 Uncategorized application restore priority increases the downtime of EHR and other patient care systems.

This is a risk_priority_high priority risk.

· 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 · 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

Measure

General approach (to eliminate or reduce the risk)

Assess the relative criticality of specific applications and data in support of other contingency plan components.

Specific action(s) required to implement this approach

· 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 · 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.8 Evaluation (§ 164.308(a)(8))

1.8.1 Outdated standard evaluation results in non-compliance with HIPAA/HITECH operational and administrative requirements.

This is a risk_priority_high priority risk.

· Policies and procedures that facilitate the implementation of the security assessment, certification, and accreditation of the system. · Annual assessment of the security safeguards to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. · A senior person in the practice signs and approves information systems for processing before operations or when there is a significant change to the system. · Continuous monitoring of information systems 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.

Measure

General approach (to eliminate or reduce the risk)

Establish 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.

Specific action(s) required to implement this approach

· Policies and procedures that facilitate the implementation of the security assessment, certification, and accreditation of the system. · Annual assessment of the security safeguards to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. · A senior person in the

practice signs and approves information systems for processing before operations or when there is a significant change to the system. · Continuous monitoring of information systems 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

1.9 Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))

1.9.1 PHI shared without a valid business associate contract exposes the provider to several liabilities including HIPAA/HITECH security violation.

This is a risk_priority_high priority risk.

· 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 · 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. Click here to download sample Business Associate Agreement provisions and customize >>

Measure

General approach (to eliminate or reduce the risk)

Establish written contracts or other arrangements with your trading partners that document satisfactory assurances that the BA will appropriately safeguard the information.

Specific action(s) required to implement this approach

· 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 · 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. Download sample Business Associate Agreement provisions and customize for your practice.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2 HIPAA/HITECH Physical Security Safeguards

2.1 Facility Access Controls (§ 164.310(a)(1))

2.1.1 Alternate options are not available to provide care during an emergency.

This is a risk_priority_high priority risk.

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

Measure

General approach (to eliminate or reduce the risk)

Establish (and implement 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.

Specific action(s) required to implement this approach

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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.1.2 Lack of physical security poses a huge risk for electronic devices that store or process ePHI.

This is a risk_priority_high priority risk.

· Policy and procedures that specify which physical and environmental safeguards used. o 164.310(a)(2)(iii) outlines some specific safeguards that are recommended · 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.

Measure

General approach (to eliminate or reduce the risk)

Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Specific action(s) required to implement this approach

· Policy and procedures that specify which physical and environmental safeguards used. o 164.310(a)(2)(iii) outlines some specific safeguards that are recommended · 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.1.3 Unauthorized access to facilities may result in theft of devices that contain or process ePHI.

This is a risk_priority_high priority risk.

· 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 · 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 · 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. · Policy and procedures that specify physical and environmental safeguards used. · 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. · 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 · Monitoring physical access through the use of video cameras · 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.

Measure

General approach (to eliminate or reduce the risk)

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.

Specific action(s) required to implement this approach

· 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 · 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 · 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. · Policy and procedures that specify physical and environmental safeguards used. · 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. · 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 · Monitoring physical access through the use of video cameras · 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.1.4 Uncontrolled access to the facility which hosts ePHI could result in data compromise.

This is a risk_priority_high priority risk.

 Policies and procedures that specify maintenance to the facility Change management process that allows request, review, and approval of changes to the information system or facility Spare parts available for quick maintenance of hardware, doors, locks, etc.

Measure

General approach (to eliminate or reduce the risk)

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).

Specific action(s) required to implement this approach

 Policies and procedures that specify maintenance to the facility Change management process that allows request, review, and approval of changes to the information system or facility Spare parts available for quick maintenance of hardware, doors, locks, etc.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.2 Workstation Use (§ 164.310(b))

2.2.1 Unsecured systems lead to ePHI access by unauthorized users.

This is a risk_priority_high priority risk.

· Role-based access to data based on job function and/or role within the organization. o This includes access to EMR systems, workstations, servers, networking equipment, etc. · Enforcement through Access Control Lists (ACL's), 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 · Firewall or border router prevents spoofing with outside incoming traffic by denying RFC 3330 (special use address space) and RFC 1918 (private internets) as the source address. ACL's (access control lists) are also used on routers, switches, and firewalls to specifically allow or deny traffic (protocols, ports, and services) through the devices and only on authorized interfaces. · Enforce session lock after 10 minutes (no more than 15 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. · Users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter) · Session lock should not be more than 15 minutes for remote access (VPN access) and portable devices (laptops, PDA's, etc.) · Terminate VPN sessions after 10-15 minutes of inactivity · Terminate terminal services or Citrix sessions after 30 minutes of inactivity. · Terminate EHR session after 10-15 minutes of inactivity · Controlling and monitoring of all remote access through the use of a syslog server, VPN server, and/or Windows Active Directory and/or Cisco Access Control Server (ACS). · IPSec VPN connections for remote access · Disable the ability for users to write data to USB & CD/DVD Drives through the use of Group Policies or enforced locally on the workstations. o Writing should only be allowed if FIPS 140-2 compliant encryption is utilized · Use of central management and encryption of removable media including USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.) · The use of cipher locks and/or 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 that has to be swiped or held in front of a sensor for entry · The use of privacy screens for each monitor and laptop to help prevent unauthorized viewing of EPHI. o Monitors and laptop screens should also be positioned so that unauthorized users cannot view the screen from office doors, lobby area, hallway, etc.

Measure

General approach (to eliminate or reduce the risk)

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 ePHI.

Specific action(s) required to implement this approach

· Role-based access to data based on job function and/or role within the organization. o This includes access to EMR systems, workstations, servers, networking equipment, etc. · Enforcement through Access Control Lists (ACL's), 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 · Firewall or border router prevents spoofing with outside incoming traffic by denying RFC 3330 (special use address space) and RFC 1918 (private internets) as the source address. ACL's (access control lists) are also used on routers, switches, and firewalls to specifically allow or deny traffic (protocols, ports, and services) through the devices and only on authorized interfaces. · Enforce session lock after 10 minutes (no more than 15 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. · Users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter) · Session lock should not be more than 15 minutes for remote access (VPN access) and portable devices (laptops, PDA's, etc.) · Terminate VPN sessions after 15 minutes of inactivity · Terminate terminal services or Citrix sessions after 15 minutes of inactivity. · Terminate EHR session after 15 minutes of inactivity · Controlling and monitoring of all remote access through the use of a syslog server, VPN server, and/or Windows Active Directory and/or Cisco Access Control Server (ACS). · IPSec VPN connections for remote access · Disable the ability for users to write data to USB & CD/DVD Drives through the use of Group Policies or enforced locally on the workstations. o Writing should only be allowed if FIPS 140-2 compliant encryption is utilized · Use of central management and encryption of removable media including USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.) · The use of cipher locks and/or 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 that has to be swiped or held in front of a sensor for entry · The use of privacy screens for each monitor and laptop to help prevent unauthorized viewing of EPHI. o Monitors and laptop screens should also be positioned so that unauthorized users cannot view the screen from office doors, lobby area, hallway, etc.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.3 Workstation Security (§ 164.310(c))

2.3.1 Unsecured systems that contain EPHI introduce several risks to patient data protection.

This is a risk_priority_high priority risk.

· Disable the ability for users to write data to USB & CD/DVD drives through the use of Group Policies or enforced locally on the workstations · 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 · The use of cipher locks and/or 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 that has to be swiped or held in front of a sensor for entry · The use of privacy screens for each monitor and laptop to help prevent unauthorized viewing of EPHI o Monitors and laptop screens should also be positioned so that unauthorized users cannot view the screen from office doors, lobby area, hallway, etc. · Positioning of equipment to help minimize potential damage from fire, flood, and electrical interference.

Measure

General approach (to eliminate or reduce the risk)

Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

Specific action(s) required to implement this approach

· Disable the ability for users to write data to USB & CD/DVD drives through the use of Group Policies or enforced locally on the workstations · 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 · The use of cipher locks and/or 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 that has to be swiped or held in front of a sensor for entry · The use of privacy screens for each monitor and laptop to help prevent unauthorized viewing of EPHI o Monitors and laptop screens should also be positioned so that unauthorized users cannot view the screen from office doors, lobby area, hallway, etc. · Positioning of equipment to help minimize potential damage from fire, flood, and electrical interference.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.4 Device and Media Controls (§ 164.310(d)(1))

2.4.1 Unsecured disposal of electronic media can result in access to ePHI by unauthroized people.

This is a risk_priority_high priority risk.

· 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.

Measure

General approach (to eliminate or reduce the risk)

Implement policies and procedures to address final disposition of ePHI and/or hardware or electronic media on which it is stored.

Specific action(s) required to implement this approach

· 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.4.2 Unsecured disposal of electronic media results in access to ePHI by unauthroized people.

This is a risk_priority_high priority risk.

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.

Measure

General approach (to eliminate or reduce the risk)

Implement procedures for removal of ePHI from electronic media before the media are available for reuse.

Specific action(s) required to implement this approach

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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.4.3 Unaudited or untracked media containing ePHI may result in data loss or breach.

This is a risk_priority_high priority risk.

· 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 · 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 · The use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of interest agreements

Measure

General approach (to eliminate or reduce the risk)

Maintain a record of the movements of hardware and electronic media, along with the person responsible for its movement.

Specific action(s) required to implement this approach

· 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 · 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 · The use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of interest agreements

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

2.4.4 Lack of backup copy may result in not having up-to-date recovery capability of production system in case of a failure.

This is a risk_priority_high priority risk.

· Perform daily/nightly, at a 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 · Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) · All backups should be encrypted using FIPS 140-2 compliant software and algorithms · Backups should be verified to help ensure the integrity of the files being backed up · 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 · 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

Measure

General approach (to eliminate or reduce the risk)

Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

Specific action(s) required to implement this approach

· Perform daily/nightly, at a 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 · Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) · All backups should be encrypted using FIPS 140-2 compliant software and algorithms · Backups should be verified to help ensure the integrity of the files being backed up · 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 · 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3 HIPAA/HITECH Technical Security Safeguards

3.1 Access Control (§ 164.312(a)(1))

3.1.1 User access to EPHI systems not controlled properly result in data compromise.

This is a risk_priority_high priority risk.

· Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system/resource · No shared access for any resource or system (i.e.computer or EHR system) · 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.

Measure

General approach (to eliminate or reduce the risk)

Assign a unique name and/or number for identifying and tracking user identities.

Specific action(s) required to implement this approach

· Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system/resource · No shared

access for any resource or system (i.e.computer or EHR system) · 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.1.2 Procedures not available to access critical data during an emergency; i.e., no emergency access account, etc.

This is a risk_priority_high priority risk.

· Procedure for obtaining necessary PHI during an emergency should be part of the Contingency Plan · 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 · 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) · Process for disabling and removing accounts upon voluntary and involuntary terminations of staff · EHR software to log and track all access, specifying each user · 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 · 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 · 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. · 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.

Measure

General approach (to eliminate or reduce the risk)

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

Specific action(s) required to implement this approach

· Procedure for obtaining necessary PHI during an emergency should be part of the Contingency Plan · 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 · 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) · Process for disabling and removing accounts upon voluntary and involuntary terminations of staff · EHR software to log and track all access, specifying each user · 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 · 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 · 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. · 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.1.3 Constantly active connections to the ePHI systems without proper configurations introduce security and privacy risks.

This is a risk_priority_high priority risk.

· 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 · Users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter) · Session lock should not be more than 15 minutes for remote access (VPN access) and portable devices (laptops, PDA's, etc.) · Terminate VPN sessions after 10-15 minutes of inactivity · Terminate terminal services or Citrix sessions after 10-15 minutes of inactivity · Terminate EHR sessions after 15 minutes of inactivity

Measure

General approach (to eliminate or reduce the risk)

Implement procedures that terminate an electronic session after a predetermined time of inactivity.

Specific action(s) required to implement this approach

· 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 · Users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter) · Session lock should not be more than 15 minutes for remote access (VPN access) and portable devices (laptops, PDA's, etc.) · Terminate VPN sessions after 10-15 minutes of inactivity · Terminate terminal services or Citrix sessions after 10-15 minutes of inactivity · Terminate EHR sessions after 10-15 minutes of inactivity

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.1.4 Unencrypted patient data on electronic devices are the number one reason for data breach.

This is a risk_priority_high priority risk.

· Use of full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.). Any solution should be FIPS 140-2 compliant · Use of email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server) · 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 · Use of IPSec VPN for remote access to the network · Use of encryption for backups (tape or back-to-disk storage) · Use of SSL/TLS for web-based access to EHR software · Use of file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP) · Use of encryption of removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.) · 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 · 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 · 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.

Measure

General approach (to eliminate or reduce the risk)

Implement a mechanism to encrypt and decrypt ePHI.

Specific action(s) required to implement this approach

· Use of full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.). Any solution should be FIPS 140-2 compliant · Use of email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server) · 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 · Use of IPSec VPN for remote access to the network · Use of encryption for backups (tape or back-to-disk storage) · Use of SSL/TLS for web-based access to EHR software · Use of file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP) · Use of encryption of removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.) · 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 · 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 · 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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.2 Audit Controls (§ 164.312(b))

3.2.1 If logs are not audited in a timely fashion, improper system activities will not be identified.

This is a risk_priority_high priority risk.

· Policies and procedures that specify audit and accountability can be included as part of the general information security policy for the practice. · 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. · 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 · 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 · Ensure the computers, servers, wireless access points/routers, and/or networking devices that perform audit logging have sufficient storage capacity · Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events · Enabling and monitoring of Windows Security Event Logs (workstation and servers); also monitor the other Event Logs (Application and System Logs) · Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls

Measure

General approach (to eliminate or reduce the risk)

Implement Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Specific action(s) required to implement this approach

· Policies and procedures that specify audit and accountability can be included as part of the general information security policy for the practice. · 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. · 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 · 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 · Ensure the computers, servers, wireless access points/routers, and/or networking devices that perform audit logging have sufficient storage capacity · Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events · Enabling and monitoring of Windows Security Event Logs (workstation and servers); also monitor the other Event Logs (Application and System Logs) · Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.3 Integrity (§ 164.312(c)(1))

3.3.1 If electronic communications between two parties are not property secured, the data transmitted cannot be reliably used for treatment.

This is a risk_priority_high priority risk.

· 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 · Use of SSL/TLS for Web-based EMR software · Use of digital certificates for email communications · Use of unique user ID's and passwords to EMR systems to help prevent unauthorized access or alteration to PHI · Use of PKI for email communication to help ensure both confidentiality and integrity of the message · 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. · 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

Measure

General approach (to eliminate or reduce the risk)

Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Specific action(s) required to implement this approach

· 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 · Use of SSL/TLS for Web-based EMR software · Use of digital certificates for email communications · Use of unique user ID's and passwords to EMR systems to help prevent unauthorized access or alteration to PHI · Use of PKI for email communication to help ensure both confidentiality and integrity of the message · 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. · 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.4 Person or Entity Authentication (§ 164.312(d))

3.4.1 Data cannot be reliably used if person authentication is not in place.

This is a risk_priority_high priority risk.

· Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource · No shared access for any resource or system (i.e. computer or EHR system) · 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 · 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. · The use of IP Address and Access Control Lists to allow or deny access to the EHR system or other resource · Microsoft Active Directory (Windows Domain Controller) to permit only authorized computers on the domain

Measure

General approach (to eliminate or reduce the risk)

Implement Person or Entity Authentication procedures to verify that the person or entity seeking access ePHI is the one claimed.

Specific action(s) required to implement this approach

· Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource · No shared access for any resource or system (i.e. computer or EHR system) · 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 · 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. · The use of IP Address and Access Control Lists to allow or deny access to the EHR system or other resource · Microsoft Active Directory (Windows Domain Controller) to permit only authorized computers on the domain

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.5 Transmission Security (§ 164.312(e)(1))

3.5.1 PHI data transmitted electronically via internet is not secured.

This is a risk_priority_high priority risk.

· Use of cryptographic hashing functions such as SHA · 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 · Use of SSL/TLS for Web-based EMR software · Use of digital certificates for email communications · Use of unique user ID's and passwords to EMR systems to help prevent

unauthorized access or alteration to PHI· Use of PKI for email communication to help ensure both confidentiality and integrity of the message · 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 · Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events · Enabling and monitoring of Windows Security Event Logs (workstation and servers); also monitor the other Event Logs (Application and System Logs). · Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls · 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 · 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 · Track and document information system security incidents on an ongoing basis · Report incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO) · 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

Measure

General approach (to eliminate or reduce the risk)

Implemented security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

Specific action(s) required to implement this approach

· Use of cryptographic hashing functions such as SHA · 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 · Use of SSL/TLS for Web-based EMR software · Use of digital certificates for email communications · Use of unique user ID's and passwords to EMR systems to help prevent unauthorized access or alteration to PHI · Use of PKI for email communication to help ensure both confidentiality and integrity of the message · 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 · Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events · Enabling and monitoring of Windows Security Event Logs (workstation and servers); also monitor the other Event Logs (Application and System Logs). · Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls · 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 · 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 · Track and document information system security incidents on an ongoing basis · Report incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO) · 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

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

3.5.2 Unencrypted ePHI data transmitted between two parties is prone for interpretation by unauthorized people.

This is a risk_priority_high priority risk.

· 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 · Use of SSL/TLS for Web-based EMR software· Use of PKI for email communications · Use of a centralized certificate server to assign certificates to Active Directory users and computers · Use of full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.). Any solution should be FIPS 140-2 compliant · Use of email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server) · Use of FIPS 140-2 compliant encryption for backups (tape or back-to-disk storage) · Use of SSL/TLS for web-based access to EHR software · Use of file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP) · Use of encryption of removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.) · 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

Measure

General approach (to eliminate or reduce the risk)

NO STANDARD SOLUTION YET???

Specific action(s) required to implement this approach

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

4 Organizational Requirements

4.2 Requirements for Group Health Plans (§ 164.314(b)(1))

4.2.1 ePHI not protected in the same way by the plan sponsor as required is a violation of the HIPAA Privacy Rule.

This is a risk_priority_high priority risk.

The plan documents of the group health plan must incorporate provisions to require the plan sponsor to: (i) 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 (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) [of the Privacy Rule] is supported by reasonable and appropriate security measures(iii) 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 (iv) Report to the group health plan any security incident of which it becomes aware

Measure

General approach (to eliminate or reduce the risk)

Ensure 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.

Specific action(s) required to implement this approach

The plan documents of the group health plan must incorporate provisions to require the plan sponsor to: (i) 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 (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) [of the Privacy Rule] is supported by reasonable and appropriate security measures (iii) 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 (iv) Report to the group health plan any security incident of which it becomes aware

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6 HIPAA Privacy Rule

6.1 Protected health information should neither be used nor disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

This is a risk_priority_high priority risk.

Develop "minimum necessary" policies for: Uses Routine disclosures Non-routine disclosures Limit request to minimum necessary Ability to rely on request for minimum necessary Click here to download sample Privacy policy provisions and customize >>

Measure

General approach (to eliminate or reduce the risk)

Develop and implement minimum necessary policies for PHI.

Specific action(s) required to implement this approach

"Minimum necessary" policies are to include: Uses Routine disclosures Non-routine disclosures Limit request to minimum necessary Ability to rely on request for minimum necessary

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.2 If covered entities and business associates do not enter into and maintain updated contracts, privacy and security of protected health information cannot be ensured, and entities may face penalties.

This is a risk_priority_high priority risk.

Develop polices for business associate (BA) relationships and amend business associate contracts or agreements; the contract must: Describe the permitted and required uses of protected health information by the business associate Provide that the business associate will not use nor further disclose protected health information other than as permitted or required by the contract or as required by law Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract. Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) BA agreement usually stipulates the Business Associate is assuming liability in the event of any data breach on their end

Measure

General approach (to eliminate or reduce the risk)

Develop polices for business associate (BA) relationships and amend business associate contracts as required.

Specific action(s) required to implement this approach

Develop polices for business associate (BA) relationships and amend business associate contracts or agreements; the contract must: - Describe the permitted and required uses of protected health information by the business associate - Provide that the business associate will not use nor further disclose

protected health information other than as permitted or required by the contract or as required by law - Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract. Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). - BA agreements usually stipulate the Business Associate is assuming liability in the event of any data breach on their end

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.3 Individuals have the right to request restrictions on how a covered entity will use and disclose protected health information about themselves for treatment, payment, and health care operations.

This is a risk_priority_high priority risk.

The Privacy rule generally prohibits a covered entity from using or disclosing protected health information unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities. Ready access to treatment and efficient payment for health care, both of which require use and disclosure of protected health information, are essential to the effective operation of the health care system. In addition, certain health care operations—such as administrative, financial, legal, and quality improvement activities—conducted by or for health care providers and health plans, are essential to support treatment and payment. Many individuals expect that their health information will be used and disclosed as necessary to treat them, bill for treatment, and, to some extent, operate the covered entity's health care business. To avoid interfering with an individual's access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.

Measure

General approach (to eliminate or reduce the risk)

Develop and implement policies and procedures to limit PHI disclosures to only those that are authorized by the client, or that are required or allowed by the privacy regulations and state law.

Specific action(s) required to implement this approach

The Privacy rule generally prohibits a covered entity from using or disclosing protected health information unless authorized by patients, except where this prohibition would result in unnecessary interference with access to quality health care or with certain other important public benefits or national priorities. Ready access to treatment and efficient payment for health care, both of which require

use and disclosure of protected health information, are essential to the effective operation of the health care system. In addition, certain health care operations—such as administrative, financial, legal, and quality improvement activities—conducted by or for health care providers and health plans, are essential to support treatment and payment. Many individuals expect that their health information will be used and disclosed as necessary to treat them, bill for treatment, and, to some extent, operate the covered entity's health care business. To avoid interfering with an individual's access to quality health care or the efficient payment for such health care, the Privacy Rule permits a covered entity to use and disclose protected health information, with certain limits and protections, for treatment, payment, and health care operations activities.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.4 Inadequate communication with the patients on uses and disclosures of protected health information, as well as his or her rights and the covered entity's obligations, doesn't provide an opportunity to object or accept.

This is a risk_priority_high priority risk.

Develop and disseminate notice of privacy practice notice; the notice should include at least (not all-inclusive): The ways that the Privacy Rule allows the covered entity to use and disclose protected health information. It must also explain that the entity will get patient permission and/or authorization before using health records for any other reason. The covered entity's duties to protect health information privacy. Patient privacy rights, including the right to complain to HHS and to the covered entity if believed that their privacy rights have been violated. Patient's right to inspect and obtain a copy of their PHI upon written notice How to contact the entity for more information and to make a complaint. Click here to download sample Notice of Privacy Practices(NPP) and customize >>

Measure

General approach (to eliminate or reduce the risk)

Make available and share updated Notice of Privacy Practices (NPP) with all your patients.

Specific action(s) required to implement this approach

Develop and disseminate notice of privacy practice notice; the notice should include at least (not all-inclusive): The ways that the Privacy Rule allows the covered entity to use and disclose protected health information. It must also explain that the entity will get patient permission and/or authorization before using health records for any other reason. The covered entity's duties to protect health information privacy. Patient privacy rights, including the right to complain to HHS and to the covered entity if believed that their privacy rights have been violated. Patient's right to inspect and obtain a copy of their PHI upon written notice How to contact the entity for more information and to make a complaint. Develop and disseminate notice of privacy practice notice; the notice should include at least (not all-inclusive): The ways that the Privacy

Rule allows the covered entity to use and disclose protected health information. It must also explain that the entity will get patient permission and/or authorization before using health records for any other reason. The covered entity's duties to protect health information privacy. Patient privacy rights, including the right to complain to HHS and to the covered entity if believed that their privacy rights have been violated. Patient's right to inspect and obtain a copy of their PHI upon written notice How to contact the entity for more information and to make a complaint.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.5 Inability to accept alternate options of communication with patient may result in poor quality of health care and lack of timely notification to the individual.

This is a risk_priority_high priority risk.

Request for confidential communication by alternative means or alternate location provides additional privacy to an individual's protected health information, along with flexibility of contact.

Measure

General approach (to eliminate or reduce the risk)

Implement policies for alternative means of communication.

Specific action(s) required to implement this approach

Request for confidential communication by alternative means or alternate location provides additional privacy to an individual's protected health information, along with flexibility of contact.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.6 Lack of policy on access to designated record sets to clarify the rights of individuals to access, amend, restrict, and acquire an account of disclosures violates the HIPAA privacy rule.

This is a risk_priority_high priority risk.

Individuals have the right to inspect and obtain a copy, request amendments, and set

restrictions on accounts of medical and billing information used to make decisions about their care. Providing access Denying access

Measure

General approach (to eliminate or reduce the risk)

Implement policies for access to designated record sets.

Specific action(s) required to implement this approach

Individuals have the right to inspect and obtain a copy, request amendments, and set restrictions on accounts of medical and billing information used to make decisions about their care. Providing access Denying access

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.7 Lack of a policy on access to designated record sets to clarify the rights of individuals to access, amend, restrict, and acquire an account of disclosures violates HIPAA privacy rule.

This is a risk_priority_high priority risk.

Standard procedure includes: Accepting an amendment Denying an amendment Actions on notice of an amendment Documentation

Measure

General approach (to eliminate or reduce the risk)

Implement policies for amendment requests.

Specific action(s) required to implement this approach

Standard procedure includes: Accepting an amendment Denying an amendment Actions on notice of an amendment Documentation

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.8 Lack of policy on access to designated record sets to clarify the rights of individuals to access, amend, restrict, and acquire an accounting of disclosures violates HIPAA privacy rule.

This is a risk_priority_high priority risk.

An individual has a right to receive an account of disclosures of protected health information made by a covered entity in the six years prior to the date on which the account is requested.

Measure

General approach (to eliminate or reduce the risk)

Implement policies for accounting of disclosures.

Specific action(s) required to implement this approach

Be able to produce and deliver for any patient an account of disclosures of protected health information made by a covered entity in the six years prior to the date on which the account is requested.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

6.9 Not having administrative controls around PHI data violates HIPAA privacy rule.

This is a risk_priority_high priority risk.

Requirements include: Appoint a HIPAA privacy officer Training of workforce Sanctions for non-compliance Develop compliance policies Develop anti-retaliation policies Policies and Procedures

Measure

General approach (to eliminate or reduce the risk)

Implement Privacy Rule Administrative requirements.

Specific action(s) required to implement this approach

Requirements include: Appoint a HIPAA privacy officer Training of workforce Sanctions for non-compliance Develop compliance policies Develop anti-retaliation policies Policies and Procedures

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

7 HIPAA/HITECH Breach Notification Rules

7.1 Not having a proper procedure to determine if a data breach incident needs to be reported or not violates data breach notification standards.

This is a risk_priority_high priority risk.

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: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification(ii) The unauthorized person who used the protected health information or to whom the disclosure was made (iii) Whether the protected health information was actually acquired or viewed(iv) The extent to which the risk to the protected health information has been mitigated

Measure

General approach (to eliminate or reduce the risk)

Have a process in place to conduct risk assessment of a data breach.

Specific action(s) required to implement this approach

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part, 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: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification (ii) The unauthorized person who used the protected health information or to whom the disclosure was made (iii) Whether the protected health information was actually acquired or viewed (iv) The extent to which the risk to the protected health information has been mitigated

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

7.2 Lack of a process to notify individuals, media, and other entities results in the affected individuals not knowing the impact of the data compromise.

This is a risk_priority_high priority risk.

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: (A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) 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); (C) Any steps individuals should take to protect themselves from potential harm resulting from the breach; (D) 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 (E) 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. (i) 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. (ii) 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: (A) 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 (B) 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.]"

Measure

General approach (to eliminate or reduce the risk)

Have a process prepared for notification to individuals following the event of a breach of unsecured PHI.

Specific action(s) required to implement this approach

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: (A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) 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); (C) Any steps individuals should take to protect themselves from potential harm resulting from the breach; (D) 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 (E) 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. (i) 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. (ii) 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: (A) 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 (B) 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.]"

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

7.3 Lack of a process to notify individuals, media, and other entities results in the affected individuals not knowing the impact of the data compromise.

This is a risk_priority_high priority risk.

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).

Measure

General approach (to eliminate or reduce the risk)

Have a process prepared for notification to the media following the event of a breach of unsecured PHI.

Specific action(s) required to implement this approach

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).

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

7.4 Lack of process to notify individuals, media, and other entities results in the affected individuals not knowing the impact of the data compromise.

This is a risk_priority_high priority risk.

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."

Measure

General approach (to eliminate or reduce the risk)

Have process prepared for notification to the secretary following the event of a breach of unsecured PHI.

Specific action(s) required to implement this approach

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."

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

7.5 Lack of process to notify individuals, media, and other entities results in the affected individuals not knowing the impact of the data compromise.

This is a risk_priority_high priority risk.

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.

Measure

General approach (to eliminate or reduce the risk)

Require your business associate to notify the covered entity following the event of any breach of unsecured PHI.

Specific action(s) required to implement this approach

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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

7.6 Lack of a process to notify individuals, media, and other entities results in the affected individuals not knowing the impact of the data compromise.

This is a risk_priority_high priority risk.

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.

Measure

General approach (to eliminate or reduce the risk)

Have a policy in place to delay the breach notification if the request is from a law enforcement authorities.

Specific action(s) required to implement this approach

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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

7.7 Lack of a process to notify individuals, media, and other entities results in the affected individuals not knowing the impact of the data compromise.

This is a risk_priority_high priority risk.

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.

Measure

General approach (to eliminate or reduce the risk)

Have a process in place to demonstrate that breach notifications were made on time and according to HITECH act requirements.

Specific action(s) required to implement this approach

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.

Level of expertise and/or requirements needed

Who is responsible?

Budget

Planning start

Planning end

Problems that have been managed or are not present in your organisation

1 HIPAA/HITECH Administrative Security Safeguards

1.1 Security Management Process (§ 164.308(a)(1))

1.2 Assigned Security Responsibility (§ 164.308(a)(2))

1.3 Workforce Security (§ 164.308(a)(3))

1.4 Information Access Management (§ 164.308(a)(4))

1.5 Security Awareness and Training (§ 164.308(a)(5))

1.6 Security Incident Procedures (§ 164.308(a)(6))

1.7 Contingency Plan (§ 164.308(a)(7))

1.8 Evaluation (§ 164.308(a)(8))

1.9 Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))

2 HIPAA/HITECH Physical Security Safeguards

2.1 Facility Access Controls (§ 164.310(a)(1))

2.2 Workstation Use (§ 164.310(b))

2.3 Workstation Security (§ 164.310(c))

2.4 Device and Media Controls (§ 164.310(d)(1))

3 HIPAA/HITECH Technical Security Safeguards

3.1 Access Control (§ 164.312(a)(1))

3.2 Audit Controls (§ 164.312(b))

3.3 Integrity (§ 164.312(c)(1))

3.4 Person or Entity Authentication (§ 164.312(d))

3.5 Transmission Security (§ 164.312(e)(1))

4 Organizational Requirements

4.1 Business Associate Contracts or Other Arrangements (§ 164.314(a)(1))

4.2 Requirements for Group Health Plans (§ 164.314(b)(1))

5 Policies and Procedures and Documentation Requirements

5.1 Policies and Procedures (§ 164.316(a))

5.2 Documentation (§ 164.316(b)(1))

6 HIPAA Privacy Rule

7 HIPAA/HITECH Breach Notification Rules

Consultation of staff

The undersigned hereby declare that the staff have been consulted on the content of this document.

On behalf of the employer:

On behalf of the staff:

Date: