Sample Client

InhouseCIO

The IT Department for Small Business

HIPAA Assessment

HIPAA Policy and Procedures

Sample Client

Prepared by:

InhouseCIO, LLC

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Contents

© InhouseCIO, LLC – ALL RIGHTS RESERVED

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Overview

This document enumerates the policies and procedures pursuant to 45 CFR 164.308 (a)(1)(i) and adopted by us to comply with technological aspects of the HIPAA Security Rule. The policies are intended to ensure the confidentiality, integrity and availability of ePHI residing on our networks and computers and the transmission of data outside of our networks when appropriate. These policies and procedures do not cover every condition, clause or stipulation of the HIPAA Security Rule nor were they intended to. The processes adopted by our organization herein are designed to automate the documentation and reporting of technological requirements and not, for example, tasks that involve administrative attention such as employee background checks, sanction warnings or beach notification. The following policies and procedures support the Administrative, Physical, and Technical safeguards of the Security Rule whether required or addressable, to the extent described below and identified by CFR code section as follows:

Standard	CFR Code Section	Description	R/A	Detail
Security Management Process	164.308(a)(1)	Risk Analysis	R	Technical assessment of risk through observed, automated collection, and automated verification.
Security Management Process	164.308(a)(1)	Risk Management	R	Issues are weighted by risk score, probability, and potential impact.
Security Management Process	164.308(a)(1)	Information System Activity Review	R	User and Login Analysis. Logins to systems with ePHI. Access to shares with ePHI. Look for access by terminated ee's and vendors. External Vulnerability scan.
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	A	Ensures group policy alignment to adequately protect technical resources. Looks for unauthorized access to ePHI and other systems.
Workforce Security	164.308(a)(3)	Termination Procedures	A	Validates terminated employees and vendors accounts are disabled. Looks for unauthorized access by terminated employees and vendors. Verifies removal of accounts from security groups. Identifies potential terminated employees through activity analysis.
Information Access Management	164.308(a)(4)	Access Authorization	A	Login Analysis. Account enablement. Access verification to ePHI.
Security Awareness and Training	164.308(a)(5)	Protection from Malicious Software	A	End-point security analysis. Firewall malware and IPS protection analysis.
Security Awareness and Training	164.308(a)(5)	Log-in Monitoring	A	Login Activity review of audit logs.
Security Awareness and Training	164.308(a)(5)	Password Management	A	Password compliance validation through group and local security policies. Baseline security analysis for weak passwords.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Contingency Plan	164.308(a)(7)	Applications and Data Criticality Analysis	A	Identification of potential locations for ePHI.
Business Associate Contracts	164.308(b)(1)	Written Contract or Other Arrangement	R	Identification of need for BAA with hosting and service providers.
Workstation Use	164.310(b)	Workstation Usage.	R	Account lockout settings. Local password validation. Login activity review. Potential ePHI verification. Network share permission checks.
Workstation Security	164.310(c)	Workstation Security.	R	Account lockout settings. Local password validation. Login activity review. Potential ePHI verification. Network share permission checks.
Access Control	164.312(a)(1)	Unique User Identification	R	Identification of domain versus workstation environment. Generic account identification. Administrative account identification.
Access Control	164.312(a)(1)	Automatic Logoff	A	Automatic screen lock validation. Account lockout policy validation.
Access Control	164.312(a)(1)	Encryption and Decryption (data at rest)	A	Drive and partition encryption identification (BitLocker).
Audit Controls	164.312(b)	Audit Controls	R	Audit policy compliance settings and validation versus best practices.
Person or Entity Authentication	164.312(d)	Account Authentication	R	Account authentication methodology identification and validation of best practices.
Transmission Security	164.312(e)(1)	Encryption (FTP and Email over Internet)	A	Identification of potential insecure use of network protocols.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Overall Risk

Conduct Risk Analysis

45 CFR §164.308(a)(1)(ii)(a) – "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."

Policy: A comprehensive Risk Analysis of all our assets including Information Systems will be conducted periodically and involves identifying risk and vulnerabilities in our information systems. To do this we will conduct an accurate and thorough assessment of the potential threats and vulnerabilities to the confidentiality, integrity and availability of ePHI at our office. Then we will reduce the risks and vulnerabilities to an appropriate and reasonable level or to the greatest extent possible though ongoing management. The risk analysis will be performed following industry best practice standards as described by HHS, NIST, ISACA, HIMSS and AHIMA organizations. A Risk Analysis will be completed no less than one time a year or after successful implementation of any major system change. Major system change would include an office relocation, replacement of EHR system containing PHI, etc. In addition, an abbreviated form of the Risk Assessment called a Risk Profile will be performed monthly to identify and prioritize risks to ePHI.

Procedure: The objective of the Risk Assessment is to complete comprehensive, periodic and independent review of our security vulnerabilities. We will start a risk assessment with a current inventory of all know devices and applications on our network and we will "map" or diagram their interdependencies so we can better understand the complex relationships between applications and devices. We will also identify frequency and format of the risk assessment (self-risk assessment versus third party, independent risk assessment), and document it. The risk assessment process will include review of administrative, physical and technical safeguards, and also take into consideration criticality, impact and creation of recommendations identifying mitigation strategies. The Risk Assessment will include a risk score for measurement and ongoing change analysis and an executive level summary report in narrative form. An automated Risk Profile will be performed monthly. A more comprehensive Risk Analysis involving more manual input through on-site surveys as well as using automated data collection routines will be performed, at least, annually or in the event of a significant change (office move, changing EHR system, moving servers to the cloud, etc.) or conducted at the direction of the Security Officer.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Risk Management

45 CFR §164.308(a)(1)(ii)(b) – "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule."

Policy: Once we have completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of ePHI and protect against any reasonably anticipated threats, hazards, or disclosures of ePHI not permitted or required under the HIPAA Privacy Rule.

The first step in the risk management process should be to develop and implement a Risk Management Plan. The purpose of a Risk Management Plan is to provide structure for the evaluation, prioritization, and implementation of risk-reducing measures and controls. The risk prioritization and mitigation decisions will be determined by answering which controls and measures should be implemented and the priority in which they should be addressed based upon their risk score.

An important component of the Risk Management Plan is the plan for implementation of the selected security measures and controls. The implementation component of the plan should address:

- Risk score (threat and vulnerability combinations) assigned to a particular issue being addressed;
- Recommendation of measures and controls selected to reduce the risk of an issue;
- Implementation project priorities, such as required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstance. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors we must consider when determining measures and controls to fix an issue. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate. The output of this step is a Risk Management Plan that contains prioritized risks, options for mitigation of those risks, and a plan for implementation. The plan will guide our actual implementation of security measures to reduce risks to ePHI to reasonable and appropriate levels.

The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Procedure: The objective of risk management is to create and document a planned risk management approach as follows:

a. The most recent Risk Assessment shall be used to develop or modify the risk Management Plan.
b. The Management Plan shall include implementation specifics and prioritized timelines for selected risk mitigation strategies identified in the monthly Risk Profiles, or Risk Assessment report.
c. The Security Officer or designated third party will execute the Management Plan by reviewing and addressing issues identified therein and will be responsible for implementation of the IT security, network and system recommendations.

We will implement automated tools and use other means to continually review and evaluate systems and devices that might store or have access to ePHI. We will conduct a regular inventory of our information systems containing ePHI and the security measures used to protect those systems. We will give highest priority to fixing issues associated with unacceptably high risk rankings and will then work to minimize or eliminate the risk based upon feasibility and effectiveness of specific method. Our HIPAA Security Officer will oversee the implementation of solutions to better secure systems that store, process or transmit electronic Protected Health Information (ePHI.)

Automated tools will be used to validate that remediation has occurred and reports will be archived for at least six years. The tool activities will focus on collecting data through open protocols across the network or operating systems and producing reports and analysis on antivirus, patch and reliability, for example. We will complement the automated reporting with walk through audits, device inspections and user list reviews.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Environment – Physical Safeguards

Facility Access Controls

45 CFR §164.310(a)(1) - "Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

Policy: We will take steps to limit physical access to systems that access or store ePHI. The purpose of this policy is to limit physical access to our electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. All physical safeguard requirements apply to business associates in the same way they apply to us. We must protect the confidentiality, integrity, and availability of our information systems by preventing unauthorized physical access, tampering and theft to the systems and to the facility in which they are located, while ensuring that properly authorized access is allowed.

Procedure: Our information systems containing ePHI must be physically located in areas where unauthorized access is minimized. We must perform an annual inventory and review of all physical access controls used to protect the information systems at our office. The perimeter of the building or site containing our information systems containing ePHI must be physically sound and all external doors must have appropriate protections against unauthorized access. Doors and windows should be locked when unattended. Additional external protection should be considered for windows, particularly at ground level.

Facility Security Plan

45 CFR §164.310(a)(2)(ii) "Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."

Policy: Based on our Risk Analysis, we will create a written Facility Security Plan describing the steps to limit physical access to systems that access or store ePHI. This plan must be updated as necessary.

Procedure: We will document physical security controls. Allow authorized access and deny unauthorized access to and within facilities, to limit access to devices that can access or store ePHI. Authorized users must be identified by name, title, or job role. Methods used to control physical access can include door locks, electronic access control systems, security officers, or video monitoring. Access to our facilities and systems will be controlled so only authorized individuals will be granted access. Workforce members will have access to facility based on their roles and functions.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Access Control and Validation Procedures

45 CFR §164.310(a)(2)(iii) "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."

Policy: We will take steps to control and validate a person's access to facilities. In addition, we will do the following:

a. Provide appropriate access for people based on their role or function. Controls will vary based on the facility and the organization's size. In some cases signage may be sufficient, while in other cases electronic access control systems and security guards may be appropriate. Everyone shall pay attention to locking cabinets with ePHI or Confidential Information, locking doors and windows after hours;
b. Workforce shall exercise vigilance about our property and shall report to Security Officer immediately any incidents, theft, unauthorized access or tampering with our property and especially with information systems components;
c. Doors to the waiting room shall be locked at the end of each business day;
d. Doors between the waiting and service areas shall be locked so they could only be opened from the service area, and access to the service area shall be monitored from the front desk;
e. Any additional entrance doors (non-monitored) to the facility shall always be locked so they only are opened from inside by authorized workforce or in emergency situation;
f. Any suspicious individuals wandering around the facility shall be confronted and asked about the purpose of being within the facility;
g. All non-patients and non-workforce individuals shall sign-in at the front desk (sign-in sheet shall document entry). Visitor's name, company and access time will be recorded in the sign-in sheet at the front desk. When sign-in sheet not used all visitors have to be accompanied by staff when entering practice beyond waiting area.
h. All workforce staff shall sign in their respective timesheets when coming in or leaving the facility.
i. Facility repairs and modifications shall be documented (scope, date and by whom).
j. When security monitoring systems are used (e.g. CCTV), Security Officer will determine who has access to these systems and recording media, and frequency of media retention and reuse.

Maintenance Records

45 CFR §164.310(a)(2)(iv) "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)."

Policy: We will document repairs and modifications to physical security components.

Procedure: Keep written records of repairs and modifications to the facility that are related to security.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Users

Information System Activity Review

§164.308(a)(1)(ii)(D): Security Management Process – " Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

Policy: We will clearly identify all critical systems that process ePHI. We will implement security procedures to regularly review the records of information system activity on all such critical systems that process ePHI.

The information that will be maintained in audit logs and access reports including security incident tracking reports must include as much as possible of the following, as reasonable and appropriate:

a. User IDs
b. Dates and times of log-on and log-off
c. Terminal identity, IP address and/or location, if possible
d. Records of successful and rejected system access attempts

Safeguards must be deployed to protect against unauthorized changes and operational problems including:

a. The logging facility being deactivated
b. Alterations to the message types that are recorded
c. Log files being edited or deleted
d. Log file media becoming exhausted, and either failing to record events or overwriting itself

Procedure: Our HIPAA Security Officer will oversee the names of current authorized users- Review reports to identify users that may still have access to ePHI but are either no longer with the organization or have a business relationship requiring access. Determine if generic accounts are used which do not support logging individual's access to ePHI.

Review the Active Directory User List with HR to validate that all users are still employed. Check access to other systems requiring authentication, including the EHR system, PACS, online systems with partners, labs, and any device or entity that stores ePHI. Verify that any vendors or subcontractors still need access.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Termination Procedures

45 CFR §164.308(a)(3)(ii)(C): - "Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b)."

Policy: People are the greatest threat to the security of any organization. It is thus important that any termination of a workforce member immediately results in both the Human Resources (HR) and the Information Technology (IT) departments quickly coordinating their activities to ensure:

a. Password access is immediately revoked
b. Access to all systems and applications is revoked
c. The workforce member is removed from any systems or applications that process ePHI
d. All digital certificates are revoked
e. Any tokens or smart cards issued to the workforce member are returned
f. Any keys and IDs provided to the workforce member during their employment are returned
g. The workforce member is not provided any access to their desk or office – any such access, if provided, must be limited and carefully supervised If the workforce member might know other worker's passwords, they should be changed immediately
h. HR must conduct an exit interview and document any issues or concerns related to the workforce member

Procedure: Validate that terminated employees are no longer on the active user list- Review the Security Assessment report with HR to identify users that may still have access to ePHI but are either no longer with the organization or have a business relationship requiring access. Determine if generic accounts are used which do not support logging individual's access to ePHI. Remember to check all systems and online services that contain ePHI.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Establish Clear Job Description and Responsibilities

45 CFR §164.308(a)(3) "Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information."

Policy: Job Descriptions and Responsibilities must be clear and documented so that members of the workforce are granted access only to that ePHI to which they are authorized in order to perform their job role or associated job function.

Procedure: Each role within the organization will be documented, including requirements for:

- Minimal Education
- Professional Certifications and/or Licenses
- Years of Experience
- Specific Skills as needed

For each role a job description will be defined, including:

- To whom the person reports
- Employees that report to the person
- Work hours, vacations, and benefits
- Access levels to facilities
- Access levels to programs and data

Each job description will include the role's Responsibilities and what access to ePHI is appropriate in both structured and unstructured systems.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Access Authorization

45 CFR §164.308(a)(4): "Implement policies and procedures for granting access to electronic protected health information; for example, through access to a workstation, transaction, program, process, or other mechanism."

Policy: Members of the workforce are to be granted access only to that ePHI to which they are authorized in order to perform their job role or associated job function. All members of the workforce will be trained regarding appropriate access to ePHI, including the awareness of information access controls. Safeguards such as role-based access control or context-based access control or mandatory access control or discretionary access control will be used as appropriate to control access to ePHI. We will develop security policies to identify core activities in the areas of isolating health care clearinghouse function, access authorization, access establishment and modification.

Procedure: This implementation specification is addressable. We have addressed its requirements and have determined that it is addressed elsewhere in our plan (see 4.1) Workforce should be trained to never access patient information using another person's credentials, including on a system left logged in by someone else. End users should be familiar with the Sanction Policy and know what to expect if they violate rules.

Evaluate Existing Security Measures Related to Access Controls

§164.308(a)(4) "Information Access Management - Implement policies and procedures for authorizing access to electronic protected health information."

Policy: Members of the workforce are to be granted access only to that ePHI to which they are authorized in order to perform their job role or associated job function. All members of the workforce will be trained regarding appropriate access to ePHI, including the awareness of information access controls. Safeguards such as role-based access control or context-based access control or mandatory access control or discretionary access control will be used as appropriate to control access to ePHI.

We will develop security policies to identify core activities in the areas of isolating health care clearinghouse function, access authorization, access establishment and modification.

Procedure: To validate that access policies are being followed, review Security Assessment report to determine if generic accounts are used which do not support logging individual's access to ePHI. Workforce should be trained to never access information about patient they are not treating or for whose records they have no business reason to see. End users should be familiar with the Sanction Policy and know what to expect if they violate rules.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Password Management

§164.308(a)(5)(ii)(d): “Security Awareness and Training - Procedures for creating, changing, and safeguarding passwords.”

Policy: We require the following password and credential management:

- All passwords must be changed at least once every 90 days.
- All production system-level passwords must be part of the Security Officer’s administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

Users must select strong passwords. Strong passwords have the following characteristics:

- Be at least eight characters in length
- Be a mixture of letters and numbers
- Be changed at least every 90 days
- Be different from the previous 6 passwords
- Not contain the user’s userid
- Passwords must not be inserted into email messages or other forms of electronic communication.

Note that poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, and so on
- Computer terms and names, commands, sites, companies, hardware, software
- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, and so on
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (for example, secret1, 1secret)

Further, systems that authenticate must require passwords of users and must block access to accounts if more than three unsuccessful attempts are made.

Members of the workforce must follow these guidelines for passwords:

- Don’t reveal a password over the phone to ANYONE
- Don’t reveal a password in an e-mail message
- Don’t talk about a password in front of others
- Don’t hint at the format of a password, like, "my family name"
- Don’t reveal a password on questionnaires or security forms
- Don’t share a password with family members
- Don’t reveal a password to co-workers
- Don’t ‘hide’ a password within view at your work area, on a badge, or under a mouse pad or keyboard.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

If someone demands a password, refer them to this document or have them call someone in the Information Security Department or contact the Security Officer. In addition, workforce must not write passwords down or store them anywhere in their office or on a badge. Further, passwords must not be stored on any computer system (including smartphones, tablets, or similar devices) without encryption.

Procedure: To validate that password policies are being followed, review the Security Assessment report and also determine if passwords are set to never expire.

Training Considerations: End users should be trained to avoid common tricks that hackers and other may use to get them to give up their passwords.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Administrative Access Control

45 CFR §164.312(a)(1) Access Control – "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)."

Policy: This policy is about the entity's initial right of access to ePHI. The individual's job description must be reviewed to determine their:

- Individual rights
- The group that this individual belongs to
- The principle of least privilege, the Minimum Necessary Standard from the HIPAA Privacy Rule, and separation of duties, shall be factors that influence the access rights granted to an individual or an entity.
- Access must be granted only on the basis of a valid business need.

By reviewing user activity such as by generic logins, are access policies really being followed?

- Is automatic logoff/lockout turned on?
- What is it set for?
- Are the settings appropriate, for example, is auto logoff/lockout set for a short interval in patient areas and for longer in more secure locations?

Procedure: To validate that access policies are being followed, we will generate regular monthly reports to determine if generic accounts are used which do not support logging individual's access to ePHI. We will also review and determine what users have not logged into the system as an indicator that their work is being delegated to others or that they are 'piggy-backing' on another user's login.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Unique User Identification

§164.312(a)(2)(i): Access Control – "Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions."

Policy: Each individual that accesses sensitive information, such as ePHI, via computer at work will be granted some form of unique user identification such as a login ID. At no time will any workforce member allow anyone else to use their unique ID. Likewise, at no time will any workforce member use anyone else's ID.

- We will develop a standard convention for assigning unique user identifiers.
- We will maintain a secure record of unique user identifiers assigned.
- We will track individual activities and record events as required by policies such as Audit and Information System Activity Review.

Procedure: To validate that access policies are being followed, review regular reports to determine if generic accounts are used which do not support logging individual's access to ePHI. Also determine what users have not logged into the system as an indicator that their work is being delegated to others or that they are 'piggy-backing' on another user's login.

Training Considerations: Work staff should be trained to never access patient information using generic passwords; logging in as someone else; or accessing a system left logged in by someone else. Staff should be familiar with the Sanction Policy and know what to expect if the rules are violated.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Audit Controls

§164.312(b) Audit Controls – "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Policy: We will identify critical systems that require event auditing capabilities. We will define the events to be audited on all such systems. At a minimal, event auditing capabilities will be enabled on all systems that process, transmit, and/or store ePHI. Events to be audited may include, logins, logouts, and file accesses, deletions and modifications. We will ensure the protection of all audit reports and log files. We will review the usage of software and application tools to review audit files. When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of the security team. This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, or stored on We equipment, premises, hosted service, or remote location
- Access to work areas (labs, offices, cubicles, storage areas, and so on)
- Access to interactively monitor and log traffic on We networks

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Person or Entity Authentication

§164.312(d): Person or Entity Authentication – "Weigh the relative advantages and disadvantages of commonly used authentication approaches." There are four commonly used authentication approaches available: Something a person knows, such as a password. Something a person has or is in possession of, such as a token (smart card, ATM card, etc.). Some type of biometric identification a person provides, such as a fingerprint. A combination of two or more of the above approaches.

Policy: We recognize that the use of passwords as an authentication method is inherently insecure and intend to require the use of strong authentication solutions for workforce members that have access to sensitive information where reasonable and appropriate. Strong authentication solutions use a combination of two or more factors (described above) when granting or denying access; such as the presence of a fingerprint (something you have) combined with a pin number (something you know).

We will evaluate emerging strong authentication technologies on a periodic basis and implement them when one is found that is:

- Technically sound and useable
- Financially reasonable
- Meets business objectives

We will give strong authentication preference to users who pose a higher risk to the organization. High risk users include (but are not limited to):

- Users that have administrator rights to systems that contain sensitive information
- Users that connect to the network remotely
- Users that have portable computing devices such as laptops or PDAs that may be carried off the premises

All workforce members that use passwords will make efforts to keep those passwords safe and secure. At no time will any workforce member:

- Write down their password, either on paper or in an electronic file
- Share or otherwise disclose their password to anyone else for any reason including technical support, managers, and supervisors
- Keep the same password for longer than 90 days
- Use a password that is the same as or a variation of any password has been used before
- Use the "remember password" option on any program that supplies the password for the user
- Use a "weak" password as described below

Weak passwords will not be used for any reason. Weak passwords have the following characteristics:

- Contain less than eight characters
- A word found in a dictionary (English or foreign)
- Common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, and so on

© InhouseCIO, LLC – ALL RIGHTS RESERVED

- Computer terms and names, commands, sites, companies, hardware, software
- Birthdays and other personal information such as addresses and phone numbers
- Word and/or number patters like aaabbb, qwerty, zyxwvuts, 123321, and so on
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (for example, secret1, 1secret)

If a password is suspected to have been compromised (or if anyone requests or demands a password), it shall be treated as a security incident and reported to the Security Officer.

Procedure: Use automated software and reporting to determine that user passwords meet the criteria described above and review violations with the users and report incidents to the security officer.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Minimal Necessary Access (Privacy Rule)

164.502(b), 164.514(d)

Policy:

This policy is about the entity's initial right of access to ePHI. The individual's job description must be reviewed to determine:

- The individual's rights
- The group that this individual belongs to
- The principle of least privilege, the Minimum Necessary Standard from the HIPAA Privacy Rule, and separation of duties, shall be factors that influence the access rights granted to an individual or an entity.

Access must be granted only on the basis of a valid business need.

Procedure: End users should be trained to never snoop in patient records. End users should be familiar with the Sanction Policy and know what to expect if they violate rules.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Servers and Local Computers

Protection Against Malicious Software

§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.

Policy: We will deploy malicious software checking programs at the perimeter (edge) of the network and on individual end-user systems. We will subscribe to receiving and deploying updates to malicious software checking programs. We will conduct security training that will include information on:

- Potential harm that can be caused by malicious software
- Prevention of malicious software such as viruses
- Steps to take if malicious software such as a virus is detected

Procedure: Utilize automated software and reporting to validate that anti-malware protection is installed and receives current definition updates on all applicable devices, including firewalls, servers, and endpoint devices.

Training Considerations: End users should be trained to be wary of phishing e-mails and never click on links unless they are absolutely sure it is legitimate. They should also be taught not to connect thumb drives and other portable drives unless they are sure they come from a safe source.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Applications and Data Criticality Analysis

§ 164.308(a)(7)(ii) - Assess the relative criticality of specific applications and data in support of other contingency plan components.

Policy: We will assess the "critical" areas of the business, which would include:

- Critical business functions
- Critical infrastructure
- Critical ePHI or records

The specific components of applications and data criticality analysis must include:

- Network architecture diagrams and system flowcharts that show current structure, equipment addresses, communication providers, hosted services, and system interdependencies.
- Identification and analysis of critical business processes surrounding ePHI.
- Identification and analysis of key applications and systems used to support critical business processes.
- A prioritized list of key applications and systems and their recovery time objectives.
- Documented results of an analysis of the internal and external interfaces with key applications and systems.
- Adequate redundancies within the network infrastructure to reduce or eliminate single points of failure.
- Mitigating controls or work-arounds in place and tested for single points of failure that cannot be eliminated.

Procedure: We will use automated software data collection and report analysis to identify all locations of ePHI outside of the EHR systems, including local PC's, servers, and portable devices.

Training Considerations: End users should be trained to always store ePHI on secured servers, not local workstations or unencrypted portable devices.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Data Backup Plan

§164.308(a)(7)(ii)(A) - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. Contingency Plan §164.308(a)(7)(ii)(b) - Establish (and implement as needed) procedures to restore any loss of data.

Policy: We will develop the capability to secure the receipt, transport, and removal of:

- Hardware
- Software and
- And electronic media, such as portable drives, tapes, optical platters, and CD-ROMs

We will document the following:

- Who has control of the hardware/software/or electronic media at all times
- Accountability, the ability to ensure that the actions of an entity can be traced back to that specific entity
- Data backup
- Data storage for recovery and retention requirements
- Disposal

In developing the backup schedule, the Security Officer will consider factors such as:

- What data (systems, files, directories, folders) should be backed up?
- How frequent are backups done?
- Who is responsible/authorized to retrieve the media?

Procedure: We will use automated software data collection and report analysis to identify the location of all ePHI across the network to ensure that it is backed up and secure.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Business Associate Contracts for Cloud Servers and Data Centers

§164.308(b)(1): Business Associate Contracts and Other Arrangements - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in $160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards.

Policy: We will identify all organizations that process or maintain ePHI. Such businesses will sign Business Associate Contract(s) executed by Entity Name. The HIPAA Omnibus Final Rule of 2013 requires Business Associate Contracts to include new wording. Existing Business Associate Contracts must be replaced by September 22, 2014. We will establish the flow of ePHI to all outside entities and identify how such information is transmitted, and the requirements for processing ePHI at the business associate site. We will review all existing BAC and ensure that all such agreements are modified with Addendums or revised for compliance with the HIPAA Security Rule. Business associates must be required to report any instance of misuse or unauthorized disclosure to ePHI. The termination of an agreement with the business associate must result in return or destruction of all ePHI with the business associate. Business associate must train all members of their workforce that process or come into contact with ePHI. This training must include awareness of the requirements of the HIPAA Security Rule as well as information about the business associates security policies and procedures.

- We must have the right to audit the business associate in the event of violations related to its ePHI.
- We must reserve the right to take “reasonable steps” including canceling the BAC without penalty.
- If the business associate intends to process or transmit the ePHI outside the United States of America then we will be informed of specific details related to such processing or transmission and reserves the right to not authorize any such flow of ePHI.
- Business Associates are now directly liable for HIPAA violations.
- Business Associates must adhere to disclosure requirements as detailed in their Business Associate Agreement.

Procedure: We will use automated software data collection and report analysis to identify Cloud vendors and online backup providers that are linked to the network. We will use automated software data collection and report analysis to identify ePHI on servers located outside of Entity Name’s facilities that may be on physical servers located in a data center, or through a Cloud service.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Encryption and Decryption (data at rest)

§164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.

Policy: We shall protect "data at rest" by implementing encryption that meets the HIPAA Standards. We will identify systems that require ePHI to be encrypted for the purpose of transmission. We will identify members of the workforce who require encryption capabilities for transmission purposes. We will follow guidelines published by NIST for guidance on implementing solutions, and 45 CFR § 170.210 standards for health information technology to protect electronic health information created, maintained, and exchanged. The (HHS) Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged: (a) Encryption and decryption of electronic health information—(1) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2 (incorporated by reference in § 170.299).

- Our key length requirements will be reviewed annually and upgraded as technology allows. All keys generated will be securely escrowed.
- The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer.
- We will test encryption and decryption capabilities of products and systems to ensure proper functionality.

Procedure: We will use automated software data collection and report analysis to verify that encryption is installed and working on all devices that contain ePHI.

Training Considerations: End users should be trained to never store ePHI on an unencrypted device.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Audit Controls

§164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Policy: We will identify critical systems that require event auditing capabilities. We will define the events to be audited on all such systems. At a minimal, event auditing capabilities will be enabled on all systems that process, transmit, and/or store ePHI. Events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions and modifications. We will ensure the protection of all audit reports and log files. We will review the usage of software and application tools to review audit files. When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of security team. This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, or stored on We equipment, premises, hosted service, or remote location
- Access to work areas (labs, offices, cubicles, storage areas, and so on)
- Access to interactively monitor and log traffic on our networks

Procedure: We will use automated software data collection and report analysis to validate that logging is turned on and review reports generated monthly.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Business Associate Contracts for Sync folders (DropBox, Box, Google Drive, etc.)

§164.308(b)(1): Business Associate Contracts and Other Arrangements - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in $160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards.

Policy: Free sharing services and some paid services are not HIPAA compliant because of their lack of security and because the companies will not sign Business Associate Agreements. We will identify all organizations that process or maintain ePHI. Such businesses will sign Business Associate Contract(s) executed by Entity Name. The HIPAA Omnibus Final Rule of 2013 requires Business Associate Contracts to include new wording. Existing Business Associate Contracts must be replaced by September 22, 2014. We will establish the flow of ePHI to all outside entities and identify how such information is transmitted, and the requirements for processing ePHI at the business associate site. We will review all existing BAC and ensure that all such agreements are modified with Addendums or revised for compliance with the HIPAA Security Rule. Business associates must be required to report any instance of misuse or unauthorized disclosure to ePHI. The termination of an agreement with the business associate must result in return or destruction of all ePHI with the business associate. Business associate must train all members of their workforce that process or come into contact with ePHI. This training must include awareness of the requirements of the HIPAA Security Rule as well as information about the business associates security policies and procedures. We must have the right to audit the business associate in the event of violations related to its ePHI. We must reserve the right to take “reasonable steps” including canceling the BAC without penalty. If the business associate intends to process or transmit the ePHI outside the United States of America then we will be informed of specific details related to such processing or transmission and reserves the right to not authorize any such flow of ePHI. Business Associates are now directly liable for HIPAA violations. Business Associates must adhere to disclosure requirements as detailed in their Business Associate Agreement.

Procedure: We will use automated software data collection and report analysis to validate that logging is turned on and review reports generated monthly to identify Cloud vendors and online backup providers that are linked to the network. We will also identify ePHI on servers located outside of Entity Name’s facilities that may be on physical servers located in a data center, or through a Cloud service.

Training Considerations: End users should be trained to never set up their own cloud or data center services without ensuring the data will be properly protected and the vendor will sign a BAA and comply with HIPAA.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Encryption and Decryption (data at rest)

§164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.

Policy: We must understand the type of encryption used to encrypt ePHI and maintain AES-256 to comply with HIPAA and NIST. We must protect "data at rest" by implementing encryption that meets the above standards. We will identify systems that require ePHI to be encrypted for the purpose of transmission. We will identify members of the workforce who require encryption capabilities for transmission purposes. We will follow guidelines published by NIST for guidance on implementing solutions, and 45 CFR § 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged. The (HHS) Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged: (a) Encryption and decryption of electronic health information—(1) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140–2 (incorporated by reference in § 170.299). Our key length requirements will be reviewed annually and upgraded as technology allows. All keys generated will be securely escrowed. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer. We will test encryption and decryption capabilities of products and systems to ensure proper functionality.

Procedure: We will use automated software data collection and report analysis to verify that encryption is installed and working on all devices that contain ePHI.

Training Considerations: End users should be trained to never store ePHI on an unencrypted device.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Firewall

Access Authorization

§164.308(a)(4): Implement policies and procedures for granting access to electronic protected health information; for example, through access to a workstation, transaction, program, process, or other mechanism.

Policy: We will protect our network perimeter with a business-class firewall to prevent unauthorized access to ePHI. The firewall must incorporate Intrusion Prevention and Intrusion Detection services and reporting to validate that the protection is enabled and working.

Procedure: We will use automated software data collection and report analysis to identify the manufacturer and model of the network firewall, and determine what security features are installed and enabled. Security subscriptions will be evaluated to ensure they are current.

Protection Against Malicious Software

§164.308(a)(5)(ii)(B): Security Awareness and Training - Procedures for guarding against, detecting, and reporting malicious software.

Policy: We will deploy malicious software checking programs at the perimeter (edge) of the network and on individual end-user systems. We will subscribe to receiving and deploying updates to malicious software checking programs. We will conduct security training that will include information on:

- Potential harm that can be caused by malicious software
- Prevention of malicious software such as viruses
- Steps to take if malicious software such as a virus is detected

Procedure: We will use automated software data collection and report analysis to validate that anti-malware protection is installed and receives current definition updates on all applicable devices, including firewalls, servers, and endpoint devices.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Email

Applications and Data Criticality Analysis

§ 164.308(a)(7)(ii)-Assess the relative criticality of specific applications and data in support of other contingency plan components.

Policy: We will assess the "critical" areas of the business, which would include:

- Critical business functions
- Critical infrastructure
- Critical ePHI or records

The specific components of applications and data criticality analysis must include:

a. Network architecture diagrams and system flowcharts that show current structure, equipment addresses, communication providers, hosted services, and system interdependencies.
b. Identification and analysis of critical business processes surrounding ePHI.
c. Identification and analysis of key applications and systems used to support critical business processes.
d. A prioritized list of key applications and systems and their recovery time objectives.
e. Documented results of an analysis of the internal and external interfaces with key applications and systems.
f. Adequate redundancies within the network infrastructure to reduce or eliminate single points of failure.
g. Mitigating controls or work-arounds in place and tested for single points of failure that cannot be eliminated.

Procedure: We will use automated software data collection and report analysis to identify all locations of ePHI outside of the EHR systems, including local PC's, servers, and portable devices. It should also identify links to any external webmail sites or connections to Outlook and other mail clients to external services. Free services such as Gmail, Hotmail, Yahoo! mail, and addresses at Internet services, GoDaddy, and other vendors that will not sign Business Associate Agreements must be identified so their use can be immediately discontinued.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Business Associate Contracts for External Email Providers

§164.308(b)(1): Business Associate Contracts and Other Arrangements - Covered entities must enter into a contract or other arrangement with persons that meet the definition of business associate in $160.103. The covered entity must obtain satisfactory assurance from the business associate that it will appropriately safeguard the information in accordance with §164.314(a)(1) standards.

Policy: We will identify all organizations that process or maintain ePHI. Such businesses will sign Business Associate Contract(s) executed by the entity's name. The HIPAA Omnibus Final Rule of 2013 requires Business Associate Contracts to include new wording. Existing Business Associate Contracts must be replaced by September 22, 2014. We will establish the flow of ePHI to all outside entities and identify how such information is transmitted, and the requirements for processing ePHI at the business associate site. We will review all existing BAC and ensure that all such agreements are modified with Addendums or revised for compliance with the HIPAA Security Rule. Business associates must be required to report any instance of misuse or unauthorized disclosure to ePHI. The termination of an agreement with the business associate must result in return or destruction of all ePHI with the business associate. Business associate must train all members of their workforce that process or come into contact with ePHI. This training must include awareness of the requirements of the HIPAA Security Rule as well as information about the business associates security policies and procedures. We must have the right to audit the business associate in the event of violations related to its ePHI. We must reserve the right to take "reasonable steps" including canceling the BAC without penalty. If the business associate intends to process or transmit the ePHI outside the United States of America then we will be informed of specific details related to such processing or transmission and we reserve the right to not authorize any such flow of ePHI. Business Associates are now directly liable for HIPAA violations. Business Associates must adhere to disclosure requirements as detailed in their Business Associate Agreement.

Procedure: We will use automated software data collection and report analysis to identify Cloud e-mail vendors that are linked to the network.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Access Authorization & Access Establishment

§164.308(a)(4): Implement policies and procedures for granting access to electronic protected health information; for example, through access to a workstation, transaction, program, process, or other mechanism.

Policy: Members of the workforce are to be granted access only to that ePHI to which they are authorized in order to perform their job role or associated job function. All members of the workforce will be trained regarding appropriate access to ePHI, including the awareness of information access controls. Safeguards such as role-based access control or context-based access control or mandatory access control or discretionary access control will be used as appropriate to control access to ePHI. We will develop security policies to identify core activities in the areas of isolating health care clearinghouse function, access authorization, access establishment and modification.

Procedure: We will use automated software data collection and report analysis to identify and ensure core activities in the areas of isolating health care clearinghouse function, access authorization, access establishment and modification.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Wireless

Access Authorization

§164.308(a)(4): Implement policies and procedures for granting access to electronic protected health information; for example, through access to a workstation, transaction, program, process, or other mechanism.

Policy: Our wireless infrastructure must follow these guidelines:

Design

a. Configure a firewall between the wireless network and the wired infrastructure.
b. Ensure that 128-bit or higher encryption is used for all wireless communication.
c. Fully test and deploy software patches and updates on a regular basis.
d. Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.

Access Points (AP)

a. Maintain and update an inventory of all Access Points (AP) and wireless devices.
b. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
c. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
d. The default settings on APs, such as those for SSIDs, must be changed.
e. APs must be restored to the latest security settings when the reset functions are used.
f. Ensure that all APs have strong administrative passwords.
g. Enable user authentication mechanisms for the management interfaces of the AP.
h. Turn on audit capabilities on AP; review log files on a regular basis.

Mobile Systems

a. Install anti-malware software on all wireless clients.
b. Install personal firewall software on all wireless clients.
c. Disable file sharing between wireless clients.

Procedure: We will use automated software data collection and report analysis to identify and ensure the hardware used across the wireless network and all security settings. Mobile devices will be checked to ensure they all have anti-malware protection and local firewalls enabled.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Access Establishment

§164.308(a)(4)(ii)(c) - Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Policy: The wireless network key must be changed annually, and whenever a key employee has been terminated from the organization.

Procedure: We will use automated software data collection and report analysis to identify when the wireless key was last changed and then update or change when appropriate.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Workforce Security

§164.308(a)(3)(ii)(C): - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).

Policy: People are the greatest threat to the security of any organization. It is thus important that any termination of a workforce member immediately results in both the Human Resources (HR) and the Information Technology (IT) departments quickly coordinating their activities to ensure:

a. Password access is immediately revoked
b. Access to the wireless network is disabled for IT and high risk employees
c. Access to all systems and applications is revoked
d. The workforce member is removed from any systems or applications that processed ePHI
e. All digital certificates are revoked
f. Any tokens or smart cards issued to the workforce member are returned
g. Any keys and IDs provided to the workforce member during their employment are returned
h. The workforce member is not provided any access to their desk or office – any such access, if provided, must be limited and carefully supervised
i. If the workforce member might know other worker's passwords, they should be changed immediately

HR must conduct an exit interview and document any issues or concerns related to the workforce member.

Procedure: Validate that terminated employees are no longer on the active user list. We will use automated software data collection and report analysis to identify and review users that may still have access to ePHI but are either no longer with the organization or have a business relationship requiring access. Determine if generic accounts are used which do not support logging individual's access to ePHI.

© InhouseCIO, LLC – ALL RIGHTS RESERVED

Transmission Security Policy

Develop and Implement Transmission Security Policy and Procedures

§164.312(e)(1) Transmission Security – "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

Policy: The purpose of our Data Transmission Security Policy and Procedures is to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. The establishment and implementation of effective Data Transmission Security Procedures is a crucial element in our overall objective of providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA). Any access to our networks must be done securely via VPN infrastructure or equivalent and must follow these guidelines:

a. Members of the workforce with VPN privileges must ensure that unauthorized users are not allowed access to Entity Name's internal networks.
b. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic must be dropped.
c. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
d. VPN gateways will be set up and managed by Entity Name's network operational groups.
e. All computers connected to Entity Name's internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
f. Users of computers that are not We-owned equipment must configure the equipment to comply with Entity Name's VPN and other policies.
g. Only approved VPN clients may be used.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of our network, and as such are subject to the same rules and regulations that apply to We-owned equipment; in other words, their machines must be configured to comply with the We' Security Policies.

Procedure: We will use automated software data collection and report analysis to identify and review all VPN's and ensure that all computers accessed or connected to our network adhere to the guidelines followed above.

© InhouseCIO, LLC – ALL RIGHTS RESERVED