Access Controls

The Access Control Standard of the Security Rule requires that covered entities implement appropriate policies and procedures to ensure the confidentiality, integrity, and availability of electronic protected health information by allowing access only to persons or systems that have been granted access and only to the level appropriate to their position or role within the organization. The Access Controls standard requires covered entities to: “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)[Information Access Management].” There are four implementation specifications for this standard: Unique User Identification, Emergency Access Procedure, Automatic Logoff, Encryption and Decryption Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented integrity controls.

Unique User Identification

Effective	Revised
12/9/2019 11:55:42 AM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with HIPAA’s Security Rule requirements pertaining to the unique user identification. User identification is a way to identify a specific user of an information system, typically by name and/or number. A unique user identifier allows an entity to track specific user activity when that user is logged into an information system. It enables an entity to hold users accountable for functions performed on information systems with EPHI when logged into those systems.

Specification Language

§ 164.312(a)(2)(i) “Assign a unique name and/or number for identifying and tracking user identity.”

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to the Unique User ID as outlined below.

Statement of Intent

All users that require access to any network, system, or application will be provided with a unique user identification.

Confidentiality

Users shall adhere to Rewarding HealthyHabits's Password Management policy. Users will not share their unique user identification or password with anyone.Users must ensure that their user identification is not documented, written, or otherwise exposed in an insecure manner. If a user believes their user identification has been comprised, they must report that security incident to the HIPAA Security Officer.

Emergency Access Procedure

Effective	Revised
1/9/2020 2:05:33 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented integrity controls.

Specification Language

§ 164.312(a)(2)(ii) "Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."

Policy Procedure

Rewarding HealthyHabits will take reasonable and appropriate steps to establish, implement, and document an emergency access procedure delineating the necessary steps to enable authorized workforce members to obtain access to necessary ePHI during a disaster or other emergency.

Statement of Intent

Rewarding HealthyHabits will provide appropriate workforce members with a current copy of the emergency access procedure and keep an appropriate number of copies at a secure off-

site location in conjunction with the Disaster Recovery Plan and the Emergency Mode Operation Plan.

Emergency Access Credentials

Appropriate workforce members shall be provided with separate emergency access log-in credentials. An electronic and auditable log of will be maintained indicating who, when and purpose for using the emergency access credentials.

Automatic Logoff or Locking

Effective	Revised
12/5/2019 2:39:52 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Automatic Logoff implementation standard of the Rule requires business assoiciates to implement policies and procedures to ensure user or entity authorized access to ePHI is not left unsecured during extended idle time [45 CFR 164§.312(b)(2)(iii)]. Business Associates that implement the Automatic Logoff specification will increase the security of their ePHI.

Policy Purpose

The purpose of this policy is to comply with HIPAA's Security Rule requirements pertaining to automatic logoff procedures. As a general practice, users should logoff the system they are working on when their workstation is unattended. However, there will be times when workers may not have the time or will not remember to log off a workstation. Automatic logoff is an effective way to prevent unauthorized users from accessing ePHI on a workstation when it is left unattended for a period of time.

Specification Language

§ 164.312(a)(2)(iii) "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to Automatic Logoff as outlined below.

Timing

Servers and workstations that stores or accesses ePHI will have the password protected

screensaver turned on. The system will be configured to lock the server or workstation after 30 minutes of inactivity.

Any servers or workstations that are located in locked or secure environments need not implement inactivity timers (such as automatic logoff) if determined by a security risk analysis.

Encryption and Decryption

Effective	Revised
8/6/2021 1:36:14 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 *(HIPAA)* requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI *(ePHI)* data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information *(IIHI)* pertaining to each patient or client.

Encryption and Decryption can be used as a form of Access Control.

Policy Purpose

The purpose of this policy is to comply with HIPAA's Security Rule requirements pertaining to encryption and decryption.

Specification Language

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

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to the Access Control Standard as outlined below.

Statement of Intent

Rewarding HealthyHabits will abide by encryption and decryption policies and procedures as outlined elsewhere in its Security policies and procedures.

Rewarding HealthyHabits will ensure encryption and decryption is reasonable and appropriate as related to its security risk analysis, to be conducted or reviewed on an annual basis.

Media which cannot be protected by other methods of access control shall utilize encryption and decryption to protect ePHI from unauthorized disclosure. Encryption and Decryption may also be utilized in combination with other access controls where indicated by risk analysis.

Inventory

Rewarding HealthyHabits will identify systems that will contain ePHI and will need to be encrypted.

Methodology

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application.

1. Symmetric cryptosystem key lengths must be at least 56 bits.

2. Asymmetric crypto-system keys must be of a length that yields equivalent strength.

3. Rewarding HealthyHabits's key length requirements will be reviewed annually and upgraded as technology allows. All keys generated will be securely escrowed.

4. Rewarding HealthyHabits will consider the use of automated encryption tools as recommended by their IT vendor.

Risk Assessment

Rewarding HealthyHabits will seriously review the viability of securing critical database, file servers as well as ePHI on mobile devices such as laptops and PDAs. Rewarding HealthyHabits will need to balance the challenge of protecting "data at rest" such as that defined in the Access Control standard of the HIPAA Security Rule against the increase in security technology complexity and administrative overhead including performance considerations and usability.

Assigned Security Responsibility

The Assigned Security Responsibility Standard of the Security Rule requires that covered entities “identify the security official who is responsible for the development and implementation of the policies and procedures required. The purpose of this standard is to identify who in Rewarding HealthyHabits will be responsible for assurance with complying with the Security Rule.

Assigned Security Responsibility

Effective	Revised
1/9/2020 2:15:09 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The Security Officer will have overall responsibility for compliance with the Security Rule generally and, in particular, for implementing policies and procedures. The Security Officer may delegate tasks and responsibilities, but, is ultimately responsible for compliance with the Security Rule.

Policy Procedures

The Assigned Security Responsibility Standard of the Security Rule requires that covered entities “identify the security official who is responsible for the development and implementation of the policies and procedures required. The designation of the Security Officer should rest with one individual to ensure accountability within each covered entity for the security of the electronic systems that contain ePHI. Qualifications of the Security Official should include the following:
• Knowledgeable about technological and business applications
• Good oral and written communication skills with ability to discuss technical terms in plain language
• Ability to compile, update, and maintain documentation of policies, procedures, actions, and assessments pertaining to implementation specifications of the security standards
• Good people management skills inside the practice and with business associates such as electronic system vendors

• Ability to enforce security policies, procedures, and sanctions
• Ability to lead risk analysis processes and training programs

Specification Language

§ 164.308(a)(2) "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

Statement of Responsibility

Rewarding HealthyHabits will assign final responsibility of security to one individual who will be referred to as the Security Officer. Responsibilities of the Security Officer include, but are not limited to:

Budget Responsibility

Prepare and manage the budget allocated to the security program and be responsible for protecting the information system assets, including an up-to-date record of inventory of hardware and software.

Policy and Procedure Implementation Responsibility

Develop and implement security policies, procedures, and guidelines to direct and carry out the objectives of the security program; research and recommend new security measures; monitor and test the security program for effectiveness.

Policy Adherence Responsibility

Ensure that the following policies and procedures are in place: security policies and procedures; baseline security safeguards; security risk management; security administration; security of computer network; security of servers; security of personal computers; physical security; disaster recovery plan; security awareness training.

Documentation Responsibility

Maintain documentation regarding levels of access granted to each information system user in the practice and review these levels of access periodically and when the status of a workforce member changes-controlling appropriate access.

Investigative Responsibility

Investigate, respond to and remedy security incidents.

Supervisory Responsibility

Supervise personnel of vendors or subcontractors who perform technical system maintenance activities and provide and document that such personnel have security awareness training, as appropriate.

Monitor Legislation Responsibility

Monitor changes in legislation that may affect Rewarding HealthyHabits and its security position.

Monitor Technology Advances Responsibility

Monitoring changes and advances in technology that may affect Rewarding HealthyHabits and its security position.

Spokesperson Responsibility

Acting as an internal consultant and external spokesperson for Rewarding HealthyHabits in all issues related to security. This includes managing Business Associates as well as communicating security related issues to workforce members and reporting of breaches as required under the Breach Notification Rule.

Assignment of Security Responsibility

Rewarding HealthyHabits has assigned these responsibilities to Paul Alfonso. If the Security Officer is not able to meet the requirements of this policy or is no longer affiliated with Rewarding HealthyHabits, these responsibilities will be assigned to a new Security Officer.

Job Description

Effective	Revised
1/9/2020 2:17:07 PM	

Job Purpose

The purpose of this position is to support the work of Rewarding HealthyHabits by being responsible for all Security related issues including, but not limited to, training, compliancy, policy development and implementation, and day-to-day administration and oversight of the HIPAA Security compliance program. The HIPAA Security Officer will be responsible for ensuring Rewarding HealthyHabits's policies and procedures are in compliance with HIPAA to ensure the confidentiality, integrity, and availability of all systems and networks. The HIPAA Security Officer is also responsible for coordinating HIPAA security activities with HIPAA Privacy and Breach Notification activities.

Job Duties: Security

- Prepare, and manage the budget allocated to the practice's security program and be responsible for protecting the practice's information system assets, including an up-to-date record of inventory of hardware and software
- Develop and implement security policies, procedures, and guidelines to direct and carry out the objectives of the practice's security program
- Research and recommend new security measures for the practice
- Monitor and test the practice's security program for effectiveness
- Ensure that the following policies and procedures are in place
    - Security policies and procedures
    - Baseline security safeguards

    - Security risk management
    - Security administration
    - Security of the computer network
    - Security of servers
    - Security of personal computers used to store, transmit or access ePHI
    - Physical security
    - Disaster recovery plan
    - Security awareness training
    - Any other policies and procedures required by the Federal and/or State governments or as required to interact with client systems containing ePHI
- Maintain documentation regarding levels of access granted to each information system user and review these levels of access periodically and when the status of a workforce member changes controlling access as appropriate
- Investigate, respond to, and remedy security incidents
- Supervise personnel of vendors or subcontractors who perform technical system activities, physical maintenance activities, or any other activity which could affect the security of systems and provide and document that such personnel have security awareness training, as appropriate
- Develop a training program
- Any other security compliance activity required by Rewarding HealthyHabits or any governing authority

Required Qualification and Experience

Education of Formal Training

- Bachelor's Degree
- 2 years of experience in healthcare, particularly in dealing with Security and HIPAA compliance

Required Skills and Knowledge

- Knowledgeable about technological and business application of the practice
- Good written and oral communication skills with ability to discuss technical terms in plain language
- Ability to compile, update, and maintain documentation of policies, procedures, actions, and assessments pertaining to implementation specifications of the security standards and privacy rule
- Good people management skills internally and externally
- Ability to enforce security policies, procedures and sanctions in the practice
- Ability to lead risk analysis processes and training programs in the practice
- Familiar with regulatory development and compliance, including federal and state laws and regulations concerning information security and privacy
- Have strong organizational and problem-solving skills, and work in a team environment

Audit Controls

The Audit Controls Standard of the Security Rule requires that covered entities to examine, review, and report on information system activity in order to determine if a security violation has occurred. Most electronic health records, practice management systems, and other electronic systems which store, access, or transmit ePHI provide some level of audit controls with a reporting method, such as audit reports. It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.

Audit Controls

Effective	Revised
1/9/2020 1:57:14 PM	

Policy Background

The Audit Controls Standard of the Security Rule requires that covered entities to examine, review, and report on information system activity in order to determine if a security violation has occurred. Most electronic health records, practice management systems, and other electronic systems which store, access, or transmit ePHI provide some level of audit controls with a reporting method, such as audit reports. The Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed; however, Rewarding HealthyHabits must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented integrity controls.

Specifcation Language

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

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to the Audit Controls Standard as outlined below. Rewarding HealthyHabits shall implement policies and procedures that require a documented process for examining and reporting information system activity.

Audit Control Mechanism

1. Information Systems will enable system logging mechanisms for all system that contain PHI.
2. Each system's audit log will include at least User ID, Login Date/Time, and Logout Date/Time.
3. System audit logs will be reviewed on a regular basis

Audit Control and Review Plan

An Audit Control and Review Plan will be developed by Information Systems. The plan will include:

1. Systems and applications to be logged;
2. Information to be logged for each system;
3. Log-in reports for each system;
4. Procedures to review all audit logs and activity reports.

Breach Notification Rule

The Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. A breach is, generally, unauthorized acquisition, access, use or disclosure of unsecured PHI which compromises the security or privacy of the PHI, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment. Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. A breach is considered discovered when the incident becomes known to the covered entity, not when the covered entity concludes its analysis

Breach Notification Rule

Effective	Revised
1/9/2020 1:44:09 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI). According to the law, all Rewarding HealthyHabits officers, providers and staff must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient.

Policy Purpose

The purpose of this policy is to set forth requirements for reporting data breaches to the HIPAA Security Officer. It is the policy of Rewarding HealthyHabits that all data breaches (as defined below) shall be reported to the HIPAA Security/Privacy Officer as outlined below. In addition, data breaches shall be reported to the affected individual and to the Secretary of HHS as outlined below.

Reporting of Breach to Privacy Officer

All breaches of unsecured PHI shall be reported to the HIPAA Privacy Officer immediately upon discovery. This includes reporting the loss or theft of any portable devise (laptop, PDA, smartphone,etc…) that may contain confidential company information or PHI. Breaches involving encrypted information while not considered a breach should still be reported to the

privacy/security officer for analysis, record keeping, and remedial training if required.

A business associate who becomes aware of a breach of unsecured PHI shall notify the covered entity, or business associate in the case of a sub-contractor, as soon as feasible.

A breach of PHI shall be treated as "discovered" as of the first day on which an incident that may have resulted in a breach is known to Rewarding HealthyHabits, or by exercising reasonable diligence would have been known to Rewarding HealthyHabits.

A breach by a business associate is considered discovered at the time the business associate reports the breach to the covered entity. If the business associate is an agent of the covered entity, the date of discovery for the covered entity is the same date the business associate discovered the breach.

Breach Definitions

Protected Health Information (PHI): Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary.

Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the privacy rule which compromises the security and privacy of the PHI.

An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach unless a breach assessment demonstrates that there is not a greater than low probability that the PHI has been compromised.

Internal Responsibility

Following the report of any data breach, the HIPAA Privacy Officer shall notify (name other individuals/position in the organization responsible for investigating breaches) and begin an investigation to determine whether further notifications are necessary.

a. Determine whether the use/disclosure violates the privacy rule (an impermissible use or disclosure of PHI under the privacy rule)

b. Determine if the use/disclosure was of secured (encrypted) information which means no breach occurred.

c. Perform a breach risk assessment to determine whether breach assessment demonstrates that there is not a greater than low probability that the PHI has been compromised, therefore not requiring notification to the affected individual(s).

1. Determine whether the incident falls under one of the three exceptions described below which means no breach occurred, and if not;

2. Use the four factors to determine if a breach occurred.

d. Document the breach risk assessment such that it can be demonstrated, if necessary, that

no breach notification was required following the impermissible use/disclosure of PHI. Breach Risk assessments shall be maintained for 6 years.

Conducting the Breach Risk Assessment (Exceptions to a Breach)

When conducting a breach risk assessment, the first thing to consider are the *three exceptions* to a privacy/security breach. If any of the three exceptions to a breach applies, no breach has occurred. However, the incident should be recorded for analysis, record keeping, and remedial training if required.

The following are exceptions to a breach:

a. Unintentional acquisition, access, or use of PHI by a workforce member, or a person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in manner not permitted under the privacy rule.

b. Any inadvertent disclosure of PHI by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the privacy rule.

c. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Conducting the Breach Risk Assessment (Review Four Factors to Make Determination)

When the initial review of the breach indicates that none of the three exceptions apply, then Rewarding HealthyHabits will review the following *four factors* to determine if a greater than low risk of compromise to the PHI exists which constitutes a breach:

Factor 1: The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.

Factor 2: The unauthorized person who used the protected health information or to whom the disclosure was made.

Factor 3: Whether the PHI was actually acquired or viewed.

Factor 4: The extent to which the risk to the PHI has been mitigated.

Rewarding HealthyHabits will weigh each of these factors together to make a conclusion as to whether or not the risk of compromise is greater than low. If so, then notification procedures must begin.

Media Notice- for Breaches Affecting 500+ Individuals

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. A prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire

state. Rewarding HealthyHabits will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like the individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and will include the same information required for the individual notice.

Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), Rewarding HealthyHabits must notify the Secretary of breaches of unsecured protected health information. Rewarding HealthyHabits will notify the Secretary by visiting the HHS web site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html) and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, Rewarding HealthyHabits will notify the Secretary without unreasonable delay and in no case later than 60 days following a breach (at the same time notification is made to the individuals affected by the breach).

If, however, a breach affects fewer than 500 individuals, Rewarding HealthyHabits may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

Notification to Individuals

When the risk assessment reveals that a breach has in fact occurred, the covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of such breach. Such notification shall be made without unreasonable delay and in no case later than 60 days after discovery of the breach incident. Therefore, all Rewarding HealthyHabits staff and subcontractors are required to report known or suspected data breaches to the HIPAA Security/Privacy Officer immediately. NOTE: State notification procedures may shorten the reporting period to the affected individuals.

Elements of Notification

Breach notification notice shall be written in plain language, to the extent possible, and must include the following:

a. A brief description of what happened, including the date of the breach, and date of the discovery of the breach, if known

b. A description of the types of unsecured PHI that were involved in the breach (such as full name, social security number, date of birth, home address, diagnosis, disability codes, or other types of information were involved.

c. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

d. A brief description of what the organization is doing to investigate the breach, to mitigate the harm to individuals, and to protect against further breaches.

e. Contact procedures for individuals to ask questions or learn additional information, which

includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Method of Notification

The method of individual notification for breaches shall be as follows:

a. In written form by first class mail

b. As outlined in the Business Associate Agreement or Services Contract with the Covered Entity

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. If Rewarding HealthyHabits knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out.

Law Enforcement Delay

Law enforcement may notify Rewarding HealthyHabits that a notification, notice, or posting would impede a criminal investigation or cause damage to national security. In this case Rewarding HealthyHabits will:

a. If the statement from law enforcement 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.

b. If the statement is made verbally, 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 verbal request, unless a written statement follows.

Substitute Notice

In the cases where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided.

A 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.

a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

b. In a case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization's website, or a conspicuous notice in a major print or broadcast media in the organizations' geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

If Rewarding HealthyHabits determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

Miscellaneous - Breaches

Training: All staff members will be trained on the breach notification rule. This will include watching the breach notification training video as well as reviewing this breach notification policy. Training completion will be documented in HIPAAtrek.

Complaints: Individuals who wish to file a complaint about the organization's compliance with the breach notification rule will be allowed to file a complaint locally with our organization or with Health and Human Services, Office for Civil Rights. See Privacy Complaints Policy for more details.

Sanctions: Staff members whose actions fail to comply with the Breach Notification Rule will be sanctioned as appropriate. The level of sanction will be based on the type of infraction. See Sanctions Policy for more details.

Refraining from Retaliatory Acts: Rewarding HealthyHabits prohibits retaliation against any staff member exercising a right, participating in the process of an investigation, filing a complaint, or for opposing an act or practice that the staff member believes in good faith violates the Breach Notification Rule.

Waiver of Rights: Rewarding HealthyHabits will not require individuals to waive any right under the Breach Notification Rule as a condition of the provision of treatment, payment, or eligibility for benefits.

The Breach Notification Rule is codified in CFR Part 164, § 164.400 to 412.

Business Associate Contracts

The Business Associates Contracts and Other Arrangements is a standard in the Administrative Safeguards of the HIPAA Security Rule. Business Associate Contracts and Other Arrangements is also addressed in the Privacy Rule and Organizational Requirements of HIPAA. This standard provides specific criteria required for written contracts or other arrangemnets between Rewarding HealthyHabits and its business associates, vendors, clients, and/or sub-contractors. It is possible for a covered entity to be a business associate. For example, a clearinghouse may be a business associate to a provider; however, it is a covered entitiy as defined in HIPAA. If you have any questions or concerns on who your business associates are or whether or not you are a business associate, it is best to consult the advice of your attorney.

Written Contracts or Other Arrangement

Effective	Revised
8/6/2021 1:38:10 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

It is the intention of Rewarding HealthyHabits to protect the integrity, availability, and confidentiality of PHI by ensuring every Business Associate or sub-contractor, external vendor, or consultant has a written agreement in place to serve as satisfactory assurance that the business associate will appropriately safeguard Rewarding HealthyHabits's PHI. § 164.308(b)(3)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE

1. 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 covered entity;
2. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
3. Report to the covered entity any security incident of which it becomes aware;

4. Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract."

Business Associate Agreements - Required Content

A Business Associate Agreement of Rewarding HealthyHabits:

- Must establish the permitted and required uses and disclosures of PHI by the business associate
- May not authorize the business associate to use or disclose information in a manner that would violate the Privacy or Security Rule
- Will include provision that the business associate will not use or further disclose Rewarding HealthyHabits's information other than as permitted or required by the contract or as required by law
- Must establish requirements for the business associate to comply with all federal, state, and local regulations governing the information being disclosed
- Must include requirements for the business associate to report to Rewarding HealthyHabits any use or disclosure of the information not provided for by its agreement of which it becomes aware, including breaches of unsecured PHI.
    - Reporting requirements should reflect the requirements in the Breach Notification Rule as well as any state or local regulation
- Will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate
- Must require that PHI be made available as required by the Privacy Rule, including provisions to ensure information required for Rewarding HealthyHabits to provide an accounting of disclosures

- Shall require the business to make its internal practices, books, and records relating to the use and disclosure of PHI received from, created by, or received by the business associate on behalf of Rewarding HealthyHabits available to any third party auditor or governmental agency for purposes of determining the Rewarding HealthyHabits's compliance
- Must include provisions for the return or destruction of PHI at termination of the agreement, if feasible,
    - The business associate may not retain copies of such information
    - If return nor destruction are infeasible, the business associate must extend the protections of the agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information feasible.
- Authorize termination of the business associate agreement by Rewarding HealthyHabits, if Rewarding HealthyHabits determines that the business associate has violated a material term of the agreement

Prior to Granting Access

Rewarding HealthyHabits assesses all business associates or subcontractors prior to granting access to PHI for compliance with the Security and Privacy Rules.

Rewarding HealthyHabits may still grant access to PHI if the business associate is found to be in non-compliance, if: Rewarding HealthyHabits enforces a strict remediation plan with deadlines for compliance and Rewarding HealthyHabits has no other reasonable alternative for the function being outsourced

Rewarding HealthyHabits may not grant access to PHI if the business associate is found to be in non-compliance and: A reasonable alternative exists The business associate is unwilling or unable to adhere to a remediation plan to mitigate identified threats and/or vulnerabilities in its Privacy or Security practices

During the Contract Term

Rewarding HealthyHabits will conduct periodic reviews of its business associates. Rewarding HealthyHabits reserves the right to conduct more frequent reviews based on its own security assessments, assessments of the business associate, material changes in federal, state, or local regulations, or as deemed necessary by the Security or Privacy Officer of Rewarding HealthyHabits.

Documentation

Rewarding HealthyHabits will retain business associate agreements, contracts, and/or other arrangements as required for a period of six (6) years from the termination date of the agreement. Rewarding HealthyHabits will also maintain all records of assessment, remediation plan/tracking, and other compliance-related documentation for a period of six (6) years.

Contingency Plan

The Security Incident Procedures Standard of the Security Rule requires that covered entities implement policies and procedures to ensure the confidentiality, integrity, and availability of data and resources, the Contingency Plan Standard requires that appropriate policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI. In order to safeguard ePHI, Rewarding HealthyHabits must make efforts to plan for operational continuity in the event of an emergency or disaster as required under the HIPAA Security Rule. There are five implementation specifications for this standard to illustrate the concept of addressability, especially with regard to high-risk analyses pertaining to Rewarding HealthyHabits. The implementation specifications are: • Data Backup • Disaster Recovery Plan • Emergency Mode of Operation Plan • Testing and Revision Procedure • Application and Data Criticality Analysis PURPOSE: Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented emergency response procedures in order to prepare for and respond to emergencies and disasters that may damage or otherwise disable ePHI systems and by taking reasonable and appropriate steps to ensure that critical data including applications, operating systems, database software, and other software supporting packages and tools will survive a disaster or other emergency. POLICY: It is the policy ofRewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to Contingency Plan as outlined below. Rewarding HealthyHabits shall implement policies and procedures that require a documented process for planning for operational continuity in the event of an emergency or disaster.

Data Backup Plan

Effective	Revised
8/6/2021 1:33:52 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to Data Backup.

Specification Language

§ 164.308(a)(7)(ii)(A) "Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

Policy Procedure

It is the policy of to comply Rewarding HealthyHabits with Data Backup Plan as outlined below:

Specify Systems to be Backed Up

Rewarding HealthyHabits shall create and maintain retrievable exact copies of the following systems:

- Essential Servers
- Virtual Servers
- Network Storage Servers
- Workstations not networked
- Mobile Devices

Data Backup Responsibility

Responsibility of creating and maintaining retrievable exact copies ofRewarding HealthyHabits's ePHI systems:

- HIPAA Security Officer
- Disaster Recovery Team Information Systems Department or
- Business Associate

Backup Schedule

Backup Schedule:

- Daily incremental back up
- Weekly full back up

Backup Storage

Define where backup media is to be stored and which workforce members may access the stored ePHI

- Backup media will be stored at an offsite storage facility at least 60 miles from the main site
- Multiple cloud-based back up managed by IT Department/Vendor

Data Backup Access

Workforce Members with access to stored ePHI

- HIPAA Security Officer
- IT Department/Vendor

Testing of Backup Procedures

Complete periodic testing of restoration procedures to confirm the effectiveness of those procedures and that the ePHI can be restored in the event that ePHI systems are damaged by or during a disaster or other emergency

- Conduct annual testing of procedures and provide feedback to its successes and failures to the appropriate management and/or workforce member
- Ongoing monitoring of system backup shall be conducted by HIPAA Security Officer. Any issues are to be brought to the immediate attention of the appropriate management and/or workforce members.

Backup Retention

Document the retention period for backup media and contain backup copies of ePHI

- Rewarding HealthyHabits shall determine when to retire external hard drives. This should be a time that is pre-determined in an effort to protect the stored ePHI's confidentiality, integrity and availability
- External hard drives, though not commonly used, will be retired after a period of no longer than 3 years.
- Retired external hard drives shall be stored for a period of 6 years at the offsite storage facility

Disaster Recovery Plan

Effective	Revised
8/6/2021 1:38:39 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to Disaster Recovery

Specification Language

§ 164.308(a)(7)(ii)(B) "Establish (and implement as needed) procedures to restore any loss of data."

Policy Procedure

It is the policy of Rewarding HealthyHabits to comply with Disaster Recovery Plan as outlined below:

Statement of Intent

Rewarding HealthyHabits will take reasonable steps to maintain a documented and detailed disaster recovery plan to recover ePHI that is lost, damaged, or corrupted in the event of a disaster or other disaster.

Conditions of Activation

The conditions under which the Disaster Recovery Plan may be activated

- Environmental Factors such as fire, tornado, earthquake, lightening strike, extreme winter weather, and other acts of God causing loss of data access
- Data Storage Failure or Server Failure
- Criminal Activity such as theft or vandalism
- Sudden, unexpected loss of staff
- Loss of Data access due to network outage, power outage, denial of service attacks, or compromised account

Define Responsibility

Define workforce members' roles and responsibilities in executing the Disaster Recovery Plan:

All workforce members:

1. Are responsible for reporting to the HIPAA Security Officer any condition triggering this Disaster Recovery Plan
2. Taking necessary and reasonable steps to protect ePHI's confidentiality, integrity, and availability

HIPAA Security Officer:

1. Entire process oversight
2. Notify necessary clients of issues
3. Interview employees to ensure all time keeping methods for payroll are in tact and accurate, make necessary adjustments

Timeframe

Timeframes for recovery are documented on the Rewarding HealthyHabits's Application and Data Criticality Analysis.

Testing and Maintenance

Rewarding HealthyHabits regularly tests and modifies, as necessary, its data backup and disaster recovery plans as defined below:

System	Timeframe for testing
Example: Essential Server	Monthly

Training

Documented training and awareness on the Disaster Recovery Plan for workforce members.

Emergency Mode of Operations Plan

Effective	**Revised**
8/6/2021 1:39:12 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to Emergency Mode of Operations.

Specification Language

§ 164.308(a)(7)(ii)(C) "Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."

Policy Procedure

It is the policy of Rewarding HealthyHabits to comply with Emergency Mode of Operations as outlined below:

Statement of Intent

In an effort to ensure the continuation of operation, Rewarding HealthyHabits will take reasonable steps to ensure the confidentiality, integrity, and availability of ePHI by continuing operations and protecting ePHI during and immediately following a disaster or other emergency.

Define Forseeable Emergencies

Define and Categorize Reasonable and Foreseeable Emergencies

- Environmental factors such as fire, tornado, earthquake, lightening strike, extreme winter weather, and other acts of God causing loss of data access.
- Data Storage failure or Server Failure
- Criminal Activity such as theft or vandalism
- Sudden, unexpected loss of staff
- Loss of Data Access due to network outage, power outage, denial of service attacks, or compromised accounts

Testing and Revisions

Testing to be performed annually

- Classroom style and unannounced testing will be performed at a time that will not affect patient care
- Revisions will be made appropriately as a result of the testing procedures. It is possible that each site will have different Emergency Mode of operations after testing is performed

Testing and Revision Procedure

Effective	Revised
8/6/2021 1:38:53 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

This policy reflects Rewarding HealthyHabits's commitment to effectively prepare for and respond to emergencies or disasters in order to protect the confidentiality, integrity and availability of its information systems.

Specification Language

§ 164.308(a)(7)(ii)(D) "Implement procedures for periodic testing and revision of contingency plans."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to Testing and Revision as outlined below:

Statement of Intent

Rewarding HealthyHabits must conduct periodic, at least annual, testing of its contingency plan to ensure that it is current and operative.

Methodology: Paper Test

Paper Test: A detailed walk through of the plan including tasks such as validating notification call lists of both key workforce members and vendors. The paper test will also include reviewing end user procedures of the data backup plan, disaster recovery plan, and the emergency mode of operations, ensuring the application and criticality analysis is complete and up to date.

Methodology: Limited Scope

Limited Scope Test: A test of one or more components of the disaster recovery plan. This should include using the data back up to restore selected information systems at in a test environment. The limited scope test should also include a testing of communications.

Methodology: Simulated Full-Scale Disaster

Simulated Full-Scale Disaster: A complete test of the disaster recovery plan. The test will likely interrupt Rewarding HealthyHabits's operations and should only be attempted after a significant limited scope testing and after determination that such a test would not impact care. The simulated full-scale disaster requires planning and should only be conducted when deemed crucial to the testing process.

Documentation

Document the Results of Testing: Rewarding HealthyHabits must formally document the testing procedures and results of the test. A plan must be derived for addressing any identified gaps or issues in the contingency plan.

Change Management

Rewarding HealthyHabits's contingency plan must be kept current through a formal change management process. Examples of events that must result in an update of the plan include, but are not limited to:

1. Change in disaster recovery plan personnel or vendors
2. Change in contact information for disaster recovery personnel
3. Significant changes to Rewarding HealthyHabits's technical or physical infrastructure

Does Not Apply

This is an Addressable Implementation Specification of the Security Rule. "Addressable" does not mean optional. Rewarding HealthyHabits must make every effort to comply with addressable implementation specifications.

Rewarding HealthyHabits has conducted an assessment and has determined that the Testing and Revision policy does not apply to Rewarding HealthyHabits for the following reasons:

List the determining factors here as to why you believe this policy does not apply to Rewarding HealthyHabits.

Application and Data Criticality Analysis

Effective	Revised
8/6/2021 1:40:40 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to implement an application and criticality analysis process of evaluating Rewarding HealthyHabits's information systems and the data contained within them.

The purpose of this analysis is to prioritize information systems based on the impact to Rewarding HealthyHabits's services, processes, and business objective if disasters or emergencies cause specific information systems to be unavailable for periods of time. The criticality analysis must be conducted at least annually or with every change or anticipated change to the information systems.

Specification Language

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

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Application and Criticality Analysis as outlined below:

Statement of Intent

Rewarding HealthyHabits must have a formal, documented process for defining and identifying the criticality of its information systems and the data contained within them.

Inventory

An inventory of all Rewarding HealthyHabits information systems is maintained:

- Servers
- Workstations
- Mobile Media
  - Laptops
  - USB Drives
  - Smart Phones
  - Cassette Tapes
  - Any other portable media
- Scanners or Copiers with hard drives
- Software
  - Operating Systems
  - Electronic Medical Records
  - Practice Management Systems
  - Other Software

Prioritization

The prioritization of Rewarding HealthyHabits information systems must be based on an analysis of the impact to Rewarding HealthyHabits services, processes, and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time. The documentation of the systems prioritization can be incorporated into the inventory or maintained separately.

Responsibility

The criticality analysis must be conducted with significant involvement from the administrators, users and owners of Rewarding HealthyHabits information systems and processes.

The criticality analysis can be conducted by either Rewarding HealthyHabits employee(s) or by a qualified third-party firm. Those conducting the analysis should understand the inter-dependencies among Rewarding HealthyHabits's information systems and processes.

Frequency

The criticality analysis must be conducted at least annually. Results from the analysis must be documented and presented to appropriate Rewarding HealthyHabits management. The criticality analysis report must be securely maintained. Any change in status of information systems and/or the data contained within them must be reflected in Rewarding HealthyHabits's disaster recovery plan.

Does Not Apply

This is an Addressable Implementation Specification of the Security Rule. "Addressable" does not mean optional. Rewarding HealthyHabits must make every effort to comply with addressable implementation specifications.

Rewarding HealthyHabits has conducted an assessment and has determined that the Application and Data Criticality Analysis policy does not apply to Rewarding HealthyHabits for the following reasons:

List the determining factors here as to why you believe this policy does not apply to Rewarding HealthyHabits.

Criticality Analysis Table

Use the below table to complete the requirements of this policy: Review as defined in "Frequency"

Application/Data	Function	Supporting IT Systems	Location	Consequences of Disruption	Workarounds/Alternatives	Maximum Downtime	Criticality/Impact Level (See NIST Risk Management Framework - Categorization of Systems)
Example: Email	Communication with staff, patients, and treatment providers	Email server and application	Hosted Cloud-based server (physical location of server)	More difficult and less timely communications	Telephone, faxes, person to person	50 hours	Moderate (Overall impact defined on Categorization of Systems)

Device and Media Controls

The Device and Media Controls Standard of the Security Rule requires that covered entities implement policies and procedures to ensure the confidentiality, integrity, and availability of data and resources. The Device and Media Controls Standards requires is an important Standard under the Physical Safeguard of the HIPAA law. The Physical Safeguards of the Security Rule were developed to protect electronic protect health information (ePHI). The Device and Media Controls standard requires covered entities to: “Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.” As referenced here, the term “electronic media” means, “electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card…” This standard covers the proper handling of electronic media including receipt, removal, backup, storage, reuse, disposal and accountability. In order to safeguard ePHI Rewarding HealthyHabits must make reasonable and appropriate effort to ensure the physical safeguard of information systems and related equipment and facilities. There are four implementation specifications for this standard to illustrate the concept of addressability, especially with regard to high risk analyses pertaining to Rewarding HealthyHabits. The implementation specifications are: Disposal, Media Reuse, Accountability, and Data backup and storage. Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented media device control policies and procedures regarding the physical receipt and removal of hardware, software, and electronic media that contain ePHI into and out of a facility, and the movement of those items within the facility, ensuring access to ePHI; while limiting the minimum necessary rights for a person to perform their duties. Media controls are established to prevent the loss of confidentiality, integrity, or availability of ePHI. The design and implementation of the media control depends on many factors, including types and classification of data, the quantity of media, and Rewarding HealthyHabits’s environment.

Disposal

Effective	Revised
8/6/2021 1:42:02 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable and appropriate steps to establish

and implement documented media disposal policies and procedures, ensuring that electronic media containing ePHI is rendered unusable and/or inaccessible.

Media disposal procedures are established to prevent the loss of confidentiality, integrity, or availability of ePHI. The destruction of the media depends on many factors, including types and classification of data, the quantity of media, and Rewarding HealthyHabits's environment.

Specification Language

§ 164.310(d)(2)(i) "Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

Policy Procedures

Rewarding HealthyHabits shall dispose of electronic media as outlined below.

Approved Methods

Rewarding HealthyHabits shall dispose of unused, retired, or otherwise non-essential media through the following methods:

Degaussing;
Shredding

Backup

Rewarding HealthyHabits will ensure a complete backup, exact, and retrievable replica of all ePHI and essential business information is made prior to the destruction of media.

Outsourcing

Rewarding HealthyHabits may use Business Associates or subcontractors to assist with the disposal of unused electronic media. If using a Business Associate or subcontractor for media destruction, Rewarding HealthyHabits shall request a certificate of destruction from the Business Associate or subcontractor.

Documentation

A log of destroyed media shall be kept for a period of 6 years. The log shall include:

- Name of media destroyed
- Method of destruction
- Date of destruction
- Person or Organization destroying media
- Location of backup

Media Re-Use

Effective	Revised
8/6/2021 1:43:38 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented media re-use policies and procedures, ensuring that electronic media containing ePHI is appropriately sanitized before it is re-used internally or externally.

Specification Language

§ 164.310(d)(2)(ii) "Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."

Policy Procedures

Rewarding HealthyHabits shall sanitize electronic media as outlined below before it is issued out for re-use.

Approved Methods

The HIPAA security officer will make a decision on how and when to sanitize the device or media. Before sanitization and reuse of media is considered, the HIPAA security officer must verify that the data stored on the device or media is completely known and if required, available elsewhere.

If it can be reused by individuals with authorization to access the information that it holds, or the device may be reused immediately with any restriction on use communicated to the new user.

If the device is to be reused within the organization, but the authority of users to access the information that might be present on it is not assured, then the device and media must be sanitized and all ePHI rendered irretrievable.

If the device and media is to be sold or otherwise continued in service outside of the organization, it must be sanitized and all data stored in it must be carefully and completely rendered irretrievable.

Rewarding HealthyHabits shall ensure that all data and ePHI that must be removed from the media prior to reuse will be accomplished through the following methods: degaussing, shredding, and disk wipe software.

Documentation

A record of how the media is being re-used, as well as if it is being reused within a different location, client's office, or for personal use ,will be maintained for a period of 6 years (see hardware/media inventory).

A record of reuse is not required if the media is being reused for internal purposes.

Accountability

Effective	Revised
8/6/2021 1:44:34 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access

to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law,Rewarding HealthyHabitsmust preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented accountability policies, and procedures that ensure an accurate record of the movement of electronic media containing ePHI is maintained and monitored.

Media accountability procedures are established to prevent the loss of confidentiality, integrity, or availability of ePHI. All portable media will be accounted for at all times.

Portable media would be defined as media that is transferred between users in a facility, transferred between facilities, and/or is transferred out of the practice setting to a personal setting.

Specification Language

§ 164.310(d)(2)(iii) "Maintain a record of the movements of hardware and electronic media and any person responsible therefore.."

Policy Procedures

Rewarding HealthyHabits shall account for portable electronic media as outlined below.

Inventory

Identify portable media that contains ePHI

- Laptops;
- External Hard drives;
- Thumb Drive;
- Cassette Tapes;
- Back Up Tapes;
- Any other portable media that stores, access, or processes ePHI.

Log

Maintain a Check Out/In log for portable media. Periodically review the log to ensure all portable media is properly accounted for.

Data Backup and Storage Procedures

Effective	Revised
8/6/2021 1:45:33 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be

managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable steps to backup and store ePHI prior to the movement of equipment.

Specification Language

§ 164.310(d)(2)(iv) "Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment".

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Data Backup and Storage as outlined below.

Moving Equipment

In the event that equipment containing ePHI is being moved, Rewarding HealthyHabits shall:

- Document the movement according to the Accountability Policy of Rewarding HealthyHabits's Device and Media Controls
- Backup the data according to the procedures outlined in the Data Backup policy of Rewarding HealthyHabits's Contingency Plan
- Store the backup according to the procedures outlined in the Data Backup policy of Rewarding HealthyHabits's Contingency Plan

Data Restoration

In the event the data needs to be restored after the equipment has been moved, Rewarding HealthyHabits will restore the data according to the Disaster Recovery Plan.

Evaluation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Practice Name must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. The Evaluation Standard of the Security Rule requires that covered entities perform a periodic technical and nontechnical evaluation that establishes the extent to which the security policies and procedures meet the minimum requirements under the Health Insurance Portability and Accountability Act (HIPAA) as well as the Health Information Technology for Economic and Clinical Health Act (HITECH). These evaluations will be initially based on the standards implemented under the Security Rule and subsequently based on response to environmental or operational changes affecting the security of ePHI.

Evaluation

Effective	Revised
8/6/2021 1:46:35 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 *(*HIPAA*)* requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

The Evaluation Standard of the Rule requires formal and documented policies and procedures that address how a covered entity addresses the evaluates the ePHI safeguards [45 CFR 164.308(a)(8)(i)].

Policy Purpose

The purpose of this policy is to implement an evaluation process for evaluating Rewarding HealthyHabits's Security Policies and Procedures. The purpose of this evaluation is to determine the effectiveness of those policies and procedures as well as to ensure compliance with federal and state regulations.

Specification Language

§ 164.308(a)(8) "Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that

establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to Evaluation as outlined below.

Statement of Intent

Rewarding HealthyHabits's Security Compliance Officer and Privacy Compliance Officer will determine in advance the programs, departments, and/or staff that will participate in the evaluation. At a minimum, all HIPAA-covered components will be addressed in the evaluation. Rewarding HealthyHabits may choose to include other parts of the organization that are not impacted by HIPAA.

Frequency of Evaluation

Rewarding HealthyHabits will establish the frequency of evaluations, taking into account the sensitivity of the confidential of sensitive electronic information, including ePHI, controlled by Rewarding HealthyHabits. In addition to periodic evaluations, Rewarding HealthyHabits will consider repeating evaluations when environmental and operational changes are made to the organization that affects the security of the confidential or sensitive electronic information, including ePHI.

Subsequent Evaluation

Rewarding HealthyHabits will establish criteria that will trigger subsequent evaluations. When establishing such criteria, Rewarding HealthyHabits takes into consideration the following factors:

1. The history of significant changes to business practices and IT systems.
2. The size of changes that have occurred.
3. Major law or regulation changes, e.g., HIPAA security regulation changes, etc.
4. The addition of new systems.
5. Implementation of new software.
6. Major security incidences within the organization, such as, the system is hacked into and ePHI is accessed, a laptop with ePHI is stolen, etc.
7. A subcontractor is added.
8. The organization makes a major physical move.
9. The organization implements a new program, major program changes, or new business practices.
10. The budget constraints that may exist limiting Rewarding HealthyHabits's ability to conduct the evaluation.
11. The staff availability to conduct the evaluation.

Components of Evaluation

Each evaluation shall include reasonable and appropriate activities, such as:

- A review of Rewarding HealthyHabits's security policies and procedures to evaluate their

appropriateness and effectiveness at protecting against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of ePHI.

- A gap analysis to compare Rewarding HealthyHabits's security policies and procedures against actual practices.
- An identification of threats and risks to ePHI Systems, as set forth in Rewarding HealthyHabits's Risk Analysis implementation specification.
- An assessment of Rewarding HealthyHabits's security controls and processes as reasonable and appropriate protections against the risks identified for ePHI Systems.
- Testing and evaluation of Rewarding HealthyHabits's security controls and processes to determine whether they have been implemented properly and whether those controls and processes appropriately protect ePHI.

Internal vs. External

Determine whether internal or external evaluation is most appropriate. Rewarding HealthyHabits shall determine whether the evaluation will be conducted with internal staff resources or with the aid of external consultants. Rewarding HealthyHabits will engage external expertise when additional skills and knowledge are determined to be reasonable and appropriate. Internal resources should be used to supplement the external source of help.

Conduct Evaluation

In conducting the evaluation, Rewarding HealthyHabits shall determine, in advance, which staff and external consultants will participate in the evaluation. All needed information shall be collected and documented. Collection methods may include interviews, surveys, and outputs of automated tools, such as system auditing tools and/or logs. It is reasonable and acceptable to complete the evaluation process in conjunction with the Security Risk Analysis, so long as the Risk Analysis policies and procedures are also reviewed for their effectiveness and the results documented.

Document Results

Rewarding HealthyHabits shall document each evaluation finding, remediation options and recommendations, and remediation decisions. Rewarding HealthyHabits shall document known gaps between identified risks and mitigating security controls, and any acceptance of risk, including justification.

Facility Access Controls

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. SECURITY REGULATION STANDARD LANGUAGE: “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.” The Facility Access Controls Standard of the Security Rule requires that covered entities implement policies and procedures to ensure the confidentiality, integrity, and availability of data and resources, the Information Technology Security Incident Procedures Standard require that appropriate procedures and protocols be developed to identify and report information security incidents and those protocols and procedures be implemented. There are four implementation specifications for this standard to illustrate the concept of addressability, especially with regard to high risk analyses pertaining to Rewarding HealthyHabits. The implementation specifications are: Contingency Operations Facility Security Plan Access Control and Validation Procedures Maintenance Records

Contingency Operations

Effective	Revised
8/6/2021 1:47:45 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, all Rewarding HealthyHabits officers, employees and agents must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

It is the intention of Rewarding HealthyHabits to protect the integrity, confidentiality, and availability of ePHI during and after an emergency that triggers the contingency plan by securing the physical access to Rewarding HealthyHabits's facility.

Specification Language

§ 164.310(a)(2)(i) "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".

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Contingency Operations as outlined below.

Statement of Intent

Rewarding HealthyHabits will take reasonable steps to ensure that in the event of a disaster or emergency, while operating in emergency mode, appropriate workforce members can enter its facilities to take the necessary actions as indicated in its respective procedures as set forth in the Disaster Recovery Plan and Emergency Mode Operation Plan.

Disaster Recovery

Based on its respective Disaster Recovery Plan, Rewarding HealthyHabits will develop, implement, and periodically review a documented procedure to allow authorized workforce members or business associates access to its facilities to support restoration of lost data

Rewarding HealthyHabitsshall define workforce members' roles in its Disaster Recovery Plan, and address facilities, ePHI Systems and electronic media involved. The Disaster Recovery Plan should define how the actions taken by such workforce members are tracked and logged, and how unauthorized accesses can be detected and prevented.

Emergency Mode of Operations

Based on its respective Emergency Mode Operations Plan, Rewarding HealthyHabits will develop, implement, and periodically review a documented procedure to allow authorized workforce members to enter its facilities to enable continuation of processes and controls that protect the confidentiality, integrity and availability of ePHI while operating in emergency mode. Rewarding HealthyHabits will define workforce members' roles in its Emergency Mode Operations Plan. Its Emergency Mode Operations Plan should define how the actions taken by such workforce members are tracked and logged, and how unauthorized accesses can be detected and prevented.

Facility Security Plan

Effective	Revised
8/6/2021 1:48:38 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, all Rewarding HealthyHabits officers, employees and agents must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement policies and procedures that safeguard the facility and equipment therein from unauthorized entry, tampering and theft.

Specification Language

§ 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 Procedures

Rewarding HealthyHabits shall safeguard its facility as outlined below. Rewarding HealthyHabits shall conduct a security risk analysis in the event a facility is compromised, moved, and/or before acquiring an additional location to ensure this policy and its procedures can be properly implemented.

Facility Access Log

Rewarding HealthyHabits shall maintain a log of all workforce members and other individuals with authorization to access the facility and the level to which access is permitted:

1. Log will state type of access
2. Log will include access method (key, access cards, punch lock code access, etc)
3. Log will state whether individual is permitted to have after-hours access
4. Log will state whether individual is permitted Emergency Mode of Operation access

Access Type

Rewarding HealthyHabits will maintain a list of all facilities and the methods of entry as well as protection implemented at each facility:

1. Keyed locks
2. Code punch lock

Visitor Log

Rewarding HealthyHabits will maintain a visitor access log:

1. Name of visitor
2. Purpose of visit
3. Date of visit
4. Visitor Badge

Workforce Responsibility

Workforce members will receive training on the Facility Security Plan to ensure all workforce

members are aware of Rewarding HealthyHabits's policies and procedures for protecting the physical security of its facilities and PHI held within its facilities. Workforce members will also be trained on their specific role and responsibilities within the Facility Security Plan.

Access Control and Validation Procedures

Effective	Revised
8/6/2021 1:49:43 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable and appropriate steps to establish and implement policies and procedures that safeguard the facility and equipment, therein by controlling and validating a person's access to the facility based on their function and/or role, including visitor, vendor, and/or consultant access and access to software programs for testing and revision.

Specification Language

§ 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 Procedures

Rewarding HealthyHabits shall safeguard its facility as outlined below:

Statement of Intent

Rewarding HealthyHabits will define, document, and implement a procedure for controlling and validating physical access to facilities that house ePHI Systems, to include the following elements:

- Provide workforce members access rights to highly sensitive areas only as needed in order to accomplish a legitimate business task
- Define and document roles or functions that require physical access rights to the facilities
- Periodically review and, where necessary, revise access rights to the facilities and ePHI Systems
- Track, log, and maintain in a secure manner physical access to the facilities

Role-based Access

Control and validate an individual's access to the facility based on role or function.

Rewarding HealthyHabits shall monitor individual's access privileges:

1. Evaluate access privileges periodically to ensure need for access still exists
2. Periodic audits of facility access logs to ensure proper access procedures
3. Enforce termination procedures to ensure proper termination of access to facility

Visitor Control

Visitor/Vendor/Consultant identification

1. All non-workforce members are required to check in with the Front Desk.
2. All non-workforce members shall be escorted.
3. All non-workforce members shall be monitored while in the facility.
4. All non-workforce members will be provided a temporary badge.

Training

Rewarding HealthyHabits will train its workforce members:

- Not to attempt to gain physical access to sensitive facilities containing ePHI Systems for which they have not been given proper authorization to access
- Immediately to report to an appropriate authority, such as the Security Officer, the loss or theft of any device (e.g., card, key) that enables physical access to facilities

Maintain Maintenance Records

Effective	Revised
8/6/2021 1:50:39 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits strives to protect the confidentiality, integrity, and availability of ePHI by taking reasonable and appropriate steps to establish and implement policies and

procedures that safeguard the facility and equipment, therein by documenting repairs and modifications to the physical components of the facility which are related to security.

Specification Language

§ 164.310(a)(2)(iv) "Maintenance Records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)."

Policy Procedures

Rewarding HealthyHabits shall safeguard its facility as outlined below. Rewarding HealthyHabits shall conduct a security risk analysis in the event a facility is compromised, moved, and/or before acquiring an additional location to ensure this policy and its procedures can be properly implemented.

Risk Assessment

After modifications of the physical components of the facility, a security risk assessment should be performed to evaluate risks and vulnerabilities to the physical security.

Log Contents

Rewarding HealthyHabits shall maintain a log of all repairs which could compromise the security of a facility such as repairs to:

1. Doors
2. Windows
3. Locks
4. Walls
5. Alarm System

Maintenance Logs shall be reviewed periodically.

Log Retention

Log of repairs and modifications shall be maintained for a period of six years or greater.

Information Access Management

The Health Insurance Portability and Accountability Act of 1996 requires access to protected health information be managed to guard the integrity, confidentiality and availability of electronic protected health information. In addition, such access shall be limited to the minimum necessary to for a workforce member to perform their duties. The information access management process is a tool in conjunction with other standards in the Privacy/Security Rule as well as the risk analysis that shall be used to accomplish this goal. The information access management process includes one required implementation specification and two addressable: Isolating Healthcare Clearinghouse Functions (required) Access Authorization (addressable), and Access Establishment and Modification (addressable). Together the three aspects of the information access management process help to guard the integrity, confidentiality, and availability of ePHI. SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: “Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E [The Privacy Rule] of this part.” PURPOSE: The purpose of this policy is to ensure workforce security procedures include requirements for authorization and supervision of access to confidential information as well as appropriate clearance procedures to approve and terminate access. These procedures must include reasonable and appropriate safeguards to prevent unauthorized access to confidential information while ensuring properly authorized workforce member’s access is permitted.

Access Authorization

Effective	Revised
8/6/2021 1:56:20 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Determine through risk analysis which Rewarding HealthyHabits workforce members have need for access to client systems containing ePHI and reflect the need for such access in job responsibilities incorporated in job descriptions. Comply with HIPAA requirements in addressing Access Authorization.

Specification Language

§ 164.308(a)(4)(ii)(B) "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 Procedure

It is the policy of Rewarding HealthyHabits to comply with Access Authorization as outlined below:

Guidelines for Accessing PHI

1. Employees may only access PHI for purposes necessary to perform their own job duties.
2. In circumstances where an employee's job requires him/her to access ePHI, the employee must adhere to the minimum necessary guidelines as well as the Privacy guidelines set forth in the Business Associate Agreement or Service Contract.
3. Employees who violate these guidelines will be subject to disciplinary action, up to and including termination.

Protecting PHI from Unauthorized Viewing

1. In areas where PHI is maintained, escort, repair and delivery representatives and any other persons not having a need to view the PHI.
2. When necessary to access systems containing ePHI remotely, do so from secure networks.
3. Ensure workstations are in secure ares to prevent accidental disclosures
4. Workstations that are in high traffic areas implement safeguards to protect from unauthorized viewing

- Higher increment auto logoff (i.e., 30 seconds, 1 minute, etc.)
- Use visual privacy screen

Guidelines for Securing Workstations

1. Establish controls that limit access to PHI to only those persons who have a need for the information
2. Exit any database containing PHI upon leaving work stations so that PHI is not left on a computer screen where it may be viewed by persons who do not have a need to see the information
3. Do not disclose or release to other persons any item or process which is used to verify authority to create, access or amend PHI, including but not limited to, any badge, password, personal identification number, token or access card, or electronic signature
4. Update and change passwords and install security updates

Access Establishment and Modification

Effective	Revised
8/6/2021 1:56:56 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Determine through risk analysis which Rewarding HealthyHabits workforce members have need for access to ePHI. Reflect the need for such access in job responsibilities incorporated in job descriptions. Determine which business associates need access to systems housing ePHI, and consider the implications of such access authorization in the risk analysis. Comply with HIPAA requirements in addressing Access Establishment and Modification.

Specification Language

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

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Access Authorization as outlined below:

Minimum Necessary Use

Access to systems housing ePHI will be granted to workforce members minimally necessary to perform job functions. Minimum necessary access will be determined by job descriptions and analyzed as part of the risk analysis.

Documentation

Access establishment and modification will be documented by HIPAA Security Officer. Records of access will be kept in the employee file.

Modification Appeal Procedure

In the event access modification unreasonably prohibits a workforce member from accomplishing tasks, the workforce member may appeal to the Security Officer. Such an appeal does not guarantee re-establishment of access.

Business Associates and Subcontractors

Business Associates and their Subcontractors needing access to systems will need to request access in writing. Access rules shall be included in the Business Associate Agreement. Business Associate and Subcontractor access shall be as defined in Access Authorization and subject to rules and restrictions just as workforce members.

Bring Your Own Device - BYOD

Effective	Revised
8/6/2021 1:57:27 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, all Rewarding HealthyHabits officers, providers, and employees must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits permits personal devices to access the network as well as to access and create PHI. The purpose of this policy is to establish guidelines and procedures for utilizing a personal electronic device: smart phone, tablet, laptop, or personal computer, on Rewarding HealthyHabits's network or from a non-network location.

Permissions

Workforce members, as defined by the Omnibus Rule, including contract employees (1099), students, volunteers, business associates, and other healthcare providers, must receive permission from the appropriate manager and/or the Security Office prior to utilizing a personal device to access the network or access or create protected health information. Failure to obtain proper authorization will result in a sanction as defined in Rewarding HealthyHabits's Sanction Policy under the Security Management Process standard of the Security Rule.

Should permission be granted, the Security Officer, or other appropriate manager, shall document the device on Rewarding HealthyHabits's inventory of devices, application and criticality analysis, risk analysis, risk management plan, and any other security protocol in place by Rewarding HealthyHabits to protect the confidentiality, integrity, and availability of PHI as defined by the Federal Information Systems Management Act.

Prior to Granting Permission

Prior to granting permission for a personal device to access Rewarding HealthyHabits's network or systems which create, access, maintain, or store protected health information, the granting authority (appropriate manager or Security Officer) will ensure the device:

- Is encrypted according to Rewarding HealthyHabits's protocols as defined in the Transmission Security standard of the Security Rule
- Has anti-malware, anti-virus, anti-spyware, and any other detective softwares properly installed in accordance with Rewarding HealthyHabits's protocols defined in the Security Awareness and Training standard, Protection from Malware implementation specification of the Security Rule
- Meets all other security protocols deemed necessary based on the device type by the granting authority

In addition, the granting authority will obtain written assurance by the workforce member seeking permission to use a personal device on the network or to access systems which create, access, maintain, or store PHI that the workforce member agrees to:

- Surrender the device in the event of a security incident affecting the device, the workforce member, or any system or application on the device or for which the device has access
- Surrender the device, if necessary, for the purposes of a comprehensive security risk analysis or other risk management activities
- Grant permission to Rewarding HealthyHabits for remote wiping in the event of loss or theft of the device or termination of the workforce member
- Grant access to the device to appropriate departments or individuals at Rewarding HealthyHabits for the purposes of periodic review of compliance regarding the device including Audit Controls protocols as defined in the Security Rule
- Prohibit access to the device by non-authorized individuals, including family members, so long as the device has permission to access the network or Rewarding HealthyHabits systems which create, access, maintain or store protected health information

Terminating Access

Rewarding HealthyHabits reserves the right to terminate the device's access to the network and/or systems which create, access, maintain, or store PHI without notice to the workforce member and without cause.

When terminating device access, Rewarding HealthyHabits shall maintain a record of the date, reason, and termination procedures for device access termination.

Rewarding HealthyHabits will adhere to the protocols defined in Device and Media Controls, Media Reuse, when terminating access to ensure all PHI and electronic access permissions have been wiped from the device prior to reissuing the personal device to the workforce member.

Information Blocking

Policies to prevent Information Blocking as required by the CURES Act.

Disclosing PHI with Health Care Providers for Treatment Purposes

Effective	Revised
8/6/2021 1:58:39 PM	

Policy

Rewarding HealthyHabits is committed to ensuring that when another treating provider of a patient requests information about that patient for treatment purposes, Rewarding HealthyHabits discloses the requested protected health information (PHI), when permitted under HIPAA and other applicable law and in a manner that does not constitute information blocking under the 21st Century Cures Act.

Rewarding HealthyHabits's policy on disclosing PHI for treatment purposes permits disclosing PHI with other treating providers without needing a patient's authorization. The minimum necessary standard does not apply to disclosures of PHI made in response to other providers for treatment purposes.

Information blocking is a practice that is likely to interfere with access, exchange, or use of electronic health information (EHI). See also Rewarding HealthyHabits's policy on Information Blocking; Exceptions.

Procedure

If a Rewarding HealthyHabits or a provider employed by Rewarding HealthyHabits receives a request from a health care provider requesting disclosure of PHI for treatment purposes, Rewarding HealthyHabits will make a reasonable effort to determine that the requesting provider is a treatment provider and will provide the PHI in the format requested if Rewarding HealthyHabits has the capability to do so. If Rewarding HealthyHabits does not have the technical capability to provide the PHI in the requested format, Rewarding HealthyHabits will contact the requesting provider to agree upon an alternate format.

Once the requesting provider has been identified as a treating provider and an acceptable and timely transmission format has been identified for disclosing the requested information, Rewarding HealthyHabits shall transmit the requested PHI to the requesting provider as expeditiously as possible but in no event later than 30 days from the original request. Note: unreasonable delay in transmission of requested electronic PHI may constitute information blocking, if Rewarding HealthyHabits delays transmission of the requested information in a manner that Rewarding HealthyHabits knows is unreasonable and/or is likely to or does interfere with access, exchange or use of electronic PHI by the requesting provider or the patient.

Rewarding HealthyHabits shall document name of the provider, the date of the receipt of the request for PHI and the requested PHI in the patient's medical record, along with the format of transmission, date and time of the transmission of the requested records to the requesting provider.

Information Blocking: Exceptions Policy

Effective	Revised
8/6/2021 2:00:46 PM	

Policy

Rewarding HealthyHabits has implemented policies to prevent practices which restrict access, exchange, or use of Electronic Health Information for treatment and other permitted purposes.

Rewarding HealthyHabits's policies to prevent information blocking take into account exceptions permitted under the CURES Act, Information Blocking Rule.

If it is deemed necessary to withhold the information under any of the below exceptions, Rewarding HealthyHabits will document the harm assessment and retain the documentation for no less than 6 years.

Preventing Harm Exception

Rewarding HealthyHabits may deny a request to access, exchange, or use Electronic Health Information if there is a reasonable belief that withholding the information will reduce a risk of harm. Rewarding HealthyHabits will not restrict data beyond what is necessary to prevent harm.

To enact this exception, the restriction must satisfy one condition from each of the following categories:

- Type of risk
- Type of harm
- Implementation basis

The patient has the right to review the individualized determination of risk of harm.

Privacy Exception

Rewarding HealthyHabits may deny a request to access, exchange, or use Electronic Health Information to protect individual privacy if:

- Precondition not satisfied:
  - Rewarding HealthyHabits may deny a request if there is a federal or state regulation which requires a precondition, such as patient consent/authorization. This exception does not include Rewarding HealthyHabits policies which are stricter than a regulation/law.
- Request is not permitted under the HIPAA Privacy Rule:
  - Rewarding HealthyHabits may deny a request for access to PHI under the circumstances provided under 45 CFR 164.524(a)(1)and(2).
    - Psychotherapy Notes
  - Rewarding HealthyHabits recognizes that access, exchange, or use of PHI is permissible under the Treatment, Payment, and Operations provision of the HIPAA Privacy Rule and will not block information nor implement barriers to access for this type of data exchange/access.
- Respecting an individual's request not to share: Rewarding HealthyHabits may choose not to provide access, exchange, or use of an individual's Electronic Health Information if doing so fulfills the wishes of the individual, provided certain conditions are met.

Security Exception

Rewarding HealthyHabits may deny a request to access, exchange, or use Electronic Health Information to protect the security of the data. This exception is meant to cover all legitimate security protocols and practices.

- The denial must be directly related to safeguarding the confidentiality, integrity, and availability of the Electronic Health Information.
- Must be tailored to specific security risks
- Must be implemented in a consistent and non-discriminatory manner
- Must implement a security policy or qualifying security determination

Infeasibility Exception

Rewarding HealthyHabits shall invoke the infeasibility exception to the Information Blocking Rule, when legitimate practical challenges limit Rewarding HealthyHabits from complying with a request to access, exchange, or use Electronic Health Information. Legitimate practical challenges exist when Rewarding HealthyHabits does not have and/or is unable to obtain the technological capabilities, legal rights, or other means necessary to enable the request.

Uncontrollable events such as: natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service disruption, or act of military, civil, or regulatory authority, make complying with the request infeasible.

Electronic Health Information cannot be unambiguously segmented.

Rewarding HealthyHabits demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances.

Rewarding HealthyHabits must provide written notice to the requestor within 10 days of the receipt of the request with the reason as to why the request is infeasible.

Health IT Exception

Rewarding HealthyHabits takes reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met. This exception recognizes that for health IT to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that health IT be taken offline temporarily.

- The practice must:
  - Be implemented for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable or the health IT’s performance degraded;
  - Be implemented in a consistent and non-discriminatory manner; and
  - Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN.
- Rewarding HealthyHabits may take action against a third-party app that is negatively impacting the health IT’s performance, provided that the practice is:
  - For a period of time no longer than necessary to resolve any negative impacts;
  - Implemented in a consistent and non-discriminatory manner; and
  - Consistent with existing service level agreements, where applicable.
- If the unavailability is in response to a risk of harm or security risk, the clinic or hospital must only comply with the Preventing Harm or Security Exception, as applicable.

Content and Manner Exception

This exception provides Rewarding HealthyHabits flexibility concerning content and manner of a response to a request.

Content Condition

For 24 months from the publication date (March 9, 2020) of the CURES Act, Rewarding HealthyHabits must respond to requests for access, exchange, or use of Electronic Health Information identified by the data elements represented in the United States Core Data for Interoperability (USCDI) standard:

- Allergies and Intolerances
- Goals
- Problems
- Assessment and Plan of Treatment
- Health Concerns
- Procedures
- Care Team Members
- Immunizations
- Provenance

- Clinic Notes
- Laboratory
- Smoking Status
- Medications
- Unique Device Identifiers
- Diagnostic Imaging
- Patient Demographics
- Vital Signs
- Encounter Information

After March 9, 2022, Rewarding HealthyHabits, must respond to requests for access, exchange, or use of Electronic Health Information identified by the data elements as defined in §171.102 of the CURES Act:

- Patient Name
- Sex (as defined in §170.207(n)(1)
    - Birth Sex attributed as follows
        - Male
        - Female
        - Unknown
- Date of Birth
- Race
- Ethnicity
- Preferred Language
- Smoking Status
- Problems
- Medications
- Medication allergies
- Laboratory tests
- Laboratory value/results
- Vital signs
- Procedures
- Care team members
- Immunizations
- Unique device identifiers
- Assessment and plan of treatment
- Goals
- Health concerns

Manner Condition

Rewarding HealthyHabits may need to fulfill a request in an **alternative manner** when we are:

- Technically unable to fulfill the request in any manner requested; ***or***
- Cannot reach agreeable terms with the requestor to fulfill the request.

If Rewarding HealthyHabits fulfills a request in an alternative manner, such fulfillment must comply with the order of priority described in the manner condition and must satisfy the Fees Exception and Licensing Exception, as applicable.

Fee Exception

Rewarding HealthyHabits may charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using Electronic Health Information, provided certain conditions are met. This exception enables Rewarding HealthyHabits to charge fees related to the development of technologies and provision of services that enhance interoperability.

Fees must:

- Be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests.
- Be reasonably related to the Rewarding HealthyHabits's costs of providing the type of access, exchange, or use of EHI.
- Not be based on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the actor.

Licensing Exception

Rewarding HealthyHabits is permitted to protect its innovations and to charge reasonable royalties in order to earn returns on the investments we have made to develop, maintain, and update our innovations to support interoperability elements for Electronic Health Information to be accessed, exchanged, or used.

Licensing negotiations must begin within 10 business days of receipt of a request and negotiate a licensing fee within 30 days from receipt of the request.

Licensing conditions must include:

- Scope of rights
- Reasonable royalty
- Non-discriminatory terms
- Collateral terms
- Non-disclosure agreement

Rewarding HealthyHabits may also include additional conditions relating to the provision of interoperability elements.

Designated Record Set and Disclosure Policy

Effective	Revised
8/6/2021 2:01:22 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of PHI. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Purpose

The purpose of this policy is to set forth Rewarding HealthyHabits's Designated Record Set to comply with HIPAA and CURES.

Regulatory Language

§164.501

(1) A group of records maintained by or for a covered entity that is:

i. The medical records and billing records about individuals maintained by or for a covered health care provider;
ii. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
iii. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Policy

It is the policy of Rewarding HealthyHabits to define its designated record sets to identify the information that is subject to the HIPAA Privacy Rule requirements as well as the 21st Century CURES Act. With limited exceptions, the HIPAA Privacy Rule gives individuals the right to access their medical and health information (protected health information) as maintained by healthcare providers and health plans.

Individuals ***do not*** have the right to access protected health information that is not part of the organization's designated record set. This may include peer review records, quality improvement records, safety records, incident reports, and/other information used by the organization in its healthcare operations.

Additionally, individuals do not have the right to access:

- Psychotherapy notes that a mental health professional maintains separately from the individual's health record that document or analyze the contents of a counseling session; and
- Information about the individual compiled in reasonable anticipation of, or for use in, a legal proceeding.

It is critical that the Rewarding HealthyHabits delineates what patient protected health information is and is not part of the Designated Record Set. It is important that there is clarity for staff as to what protected health information (PHI) is not included in the Designated Record Set so that it is not inadvertently disclosed.

The Designated Record Set will include the USCDI data points required for Electronic Health Information (EHI) release in accordance with the 21st Century CURES Act.

Procedures

1. The Rewarding HealthyHabits Health Information Management (HIM) Leader and/or Privacy Officer must inventory the systems and applications that create, maintain, and store its patient protected health information/health records.
2. Upon identification of sources of patient protected health information/health records, the individual documents/items shall be itemized with an indication of what is a component of the Rewarding HealthyHabits's Designated Record Set (DSR) and subject to disclosure.
3. Just as importantly, the Rewarding HealthyHabits shall itemize those documents/items that are not a part of the DSR and not subject to disclosure.
4. Once completed, HIM and Privacy leadership will be responsible for:
    a. Providing administrative support in relation to policies and procedures relating to the designated record set; and
    b. Providing appropriate training to the workforce with an emphasis for more complete training for those departments and functions that routinely disclose patient information (e.g., Release of Information, Patient Financial Services).

USCDI Standard Data Points

1. Allergies and Intolerances
    a. Substance (Medication)
    b. Substance (Drug Class)
    c. Reaction
2. Assessment and Plan of Treatment
3. Care Team Members
4. Clinical Notes
    a. Consultation Note

    b. Discharge Summary Note
    c. History and Physical
    d. Imaging Narrative
    e. Laboratory Report Narrative
    f. Pathology Report Narrative
    g. Procedure Note
    h. Progress Note
5. Goals
6. Health Concerns
7. Immunizations
8. Laboratory
    a. Test
    b. Values/Results
9. Medications
10. Patient Demographics
    a. First Name
    b. Last Name
    c. Previous Name
    d. Middle Name (including middle initial)
    e. Suffix
    f. Birth Sex
    g. Date of Birth
    h. Race
    a. Ethnicity
    j. Preferred Language
    k. Current Address
    ax. Previous Address
    all. Phone Number
    n. Phone Number Type
    o. Email Address
11. Problems
12. Procedures
13. Provenance
    a. Author Time Stamp
    b. Author Organization
14. Smoking Status
15. Unique Device Identifier(s) for a Patient's Implantable Device(s)
16. Vital Signs
    a. Diastolic Blood Pressure
    b. Systolic Blood Pressure
    c. Body Height
    d. Body Weight
    e. Heart Rate
    f. Respiratory Rate
    g. Body Temperature
    h. Pulse Oximetry
    a. Inhaled Oxygen Concentration
    j. BMI Percentile (2-20 years old)
    k. Weight-for-length Percentile (Birth – 36 months)
    l. Occipital-frontal Head Circumference Percentile (Birth – 36 months)

Inventory List for Delineating Status of Designated Record Sets

Designated Record Set	Examples
Medical/Healthcare Record of Organization/Provider *Itemize by system, application, document type.*	▪ The information defined as the legal health record in a paper or computer-based record environment.
Billing Record of Organization/Provider	▪ The content of the patient account file in a paper-based provider office. ▪ The information defined as patient account data in a computer-based record environment.
Enrollment, Payment, Claims Adjudication, and Case or Medical Management Record Systems Maintained by or for a Health Plan	▪ The information defined as enrollment, payment, claims adjudication, and case or medical management information in a health plan information system.
Other Records Used to Make Decisions About the Individual	▪ A history and physical generated by a physician at a hospital and incorporated into the resident's record in a long-term care facility because it will be used to make decisions about the individual. ▪ Copies of reports generated by other providers and used to make decisions about the individual, even when such records are kept in a separate file location or file folder. ▪ E-mail communications that include PHI that an organization stores online and hasn't printed out in its otherwise paper-based health record.
Records Maintained by a Business Associate That Meet the Definition of Designated Record Set That Are Not Merely Duplicates of Information Maintained by the Organization/ Provider	▪ Records maintained by record storage companies that have agreed to manage release of information rather than returning the records to the covered entity to respond.

The following table provides examples of patient PHI that are not considered part of the organization's designated record set.

Outside the Designated Record Set	Examples
Health Information generated, collected, or Maintained for Purposes That Do Not Include	▪ Data collected and maintained for peer review and/or risk management purposes. ▪ Data collected and maintained for performance improvement purposes.

Outside the Designated Record Set	Examples
Decision Making About the Individual	▪ HIPAA breach investigation and compliance issue documentation. ▪ Appointment and surgery schedules. ▪ Birth and death registers. ▪ Surgery registers. ▪ Diagnostic or operative indexes or reports. ▪ Duplicate copies of information that can also be located in the individual's medical or billing record. ▪ Data collected and maintained for research.
Psychotherapy Notes	The notes of a mental health professional about counseling sessions that are maintained separate and apart from the regular health record.
Information Compiled in Reasonable Anticipation of or For Use in a Civil, Criminal, or Administrative Action or Proceeding	Notes taken by a covered entity during a meeting with the covered entity's attorney about a pending lawsuit.
Clinical Laboratory Records	▪ Requisitions for laboratory tests. ▪ Duplicate lab results when the originals are filed in the individual's paper chart.
Employer Records	▪ Pre-employment physicals maintained in human resource files. ▪ The results of HIV tests maintained by the infectious disease control nurse on employees who have suffered needle stick injuries on the job.
Miscellaneous Records	▪ Adoption Records ▪ Guardianship Papers
Quality Improvement/Peer Review Records	▪ Medical Staff Case Reviews
Registry Information	▪ Birth Registers ▪ Death Registers ▪ Surgery Registers ▪ Cancer Registers ▪ Trauma Registers
Research Records	▪ Records Maintained for Research Purposes
Risk Management Records	▪ Incident/Variance Reports
Schedules	▪ Surgery Schedules ▪ Appointment Schedules
Source Data Interpreted or Summarized in the	▪ Pathology slides. ▪ Diagnostic films.

Individual's Medical or Health Record Outside the Designated Record Set	Examples
Working Records – Only if the Information is Available Elsewhere in the Medical/ Healthcare Record and/or Billing Record of the Individual (e.g., Summarized in Notes or Reports).	▪ Electrocardiogram tracings from which interpretations are derived. ▪ Raw test data. ▪ Audiotapes. ▪ Videos/photographs used for educational purposes. ▪ Telemedicine records. ▪ Coding/UR worksheets. ▪ Billing/Accounts Payable staff working notes regarding claim status, patient conversations, claim reviews, etc.

Integrity

The Integrity Standard of the Security Rule requires that covered entities protect the integrity of electronic protected health information by implementing proper electronic mechanisms to ensure that ePHI is not inappropriately destroyed or altered. EPHI that is improperly altered or destroyed can result in clinical quality problems for a covered entity, including patient safety issues. The integrity of data can be compromised by both technical and non-technical sources. Workforce members may make accidental or intentional changes that improperly alter or destroy ePHI. Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures. The purpose of this standard is to establish and implement policies and procedures for protecting ePHI from being compromised regardless of the source. The Integrity standard requires covered entities to: “Implement policies and procedures to protect electronic protected health information from improper alteration or destruction” and “electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.” There is one implementation specification for this standard: Mechanism to Authenticate Electronic Protected Health Information. In order to determine which electronic mechanisms to implement to ensure that ePHI is not altered or destroyed in an unauthorized manner, Rewarding HealthyHabits must consider the various risks to the integrity of EPHI identified during the risk analysis. Once Rewarding HealthyHabits has identified risks to the integrity of their data, they must identify security measures that will reduce the risks. Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented integrity controls.

Mechanism to Authenticate ePHI

Effective	Revised
8/6/2021 2:02:05 PM	

Policy Background

The Integrity Standard of the Security Rule requires that covered entities protect the integrity of electronic protected health information by implementing proper electronic mechanisms to ensure that ePHI is not inappropriately destroyed or altered. EPHI that is improperly altered or destroyed can result in clinical quality problems for a covered entity, including patient safety issues.

Policy Purpose

The purpose of this policy is to establish procedures for protecting ePHI from being compromised regardless of the source by implementing electronic mechanisms to authenticate ePHI.

Specification Language

§ 164.312(c)(2) "Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner."

Policy Procedures

In order to determine which electronic mechanisms to implement to ensure that ePHI is not altered or destroyed in an unauthorized manner, Rewarding HealthyHabits must consider the various risks to the integrity of ePHI identified during the risk analysis. Once Rewarding HealthyHabits has identified risks to the integrity of their data, they must identify security measures that will reduce the risks.

Statement of Intent

Electronic mechanisms used to protect the integrity of ePHI accessed on Rewarding HealthyHabits's systems must ensure that the value and state of the ePHI is maintained, and it is protected from unauthorized modification and destruction.

Approved Mechanisms

Mechanisms must also be capable of detecting unauthorized alteration or destruction of ePHI. Such mechanisms might include:

- System memory
- Hard drives, and other data storage devices with error-detection capabilities
- File and data check sums
- Encryption
- Audit log reviews

Organizational Requirements

Organizational Requirements is a requirement under the Security Rule and further describes responsibilities and duties for policy oversight.

Policy Oversight Documentation

Effective	Revised
8/6/2021 2:02:37 PM	

Policy Purpose

The purpose of this policy is to comply with the Security Rule's Policy and Procedures as well as Documentation requirements.

Specification Language

§164.316(a)" Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b) (2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

§164.316(b)(1)(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

§164.316(b)(2)(i) Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

§164.316(b)(2)(i)(ii) Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

§164.316(b)(2)(i)(ii)(iii) Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Policies and Procedures

Rewarding HealthyHabits will maintain and implement policies and procedures which are reasonable and appropriate to comply with HIPAA's Privacy, Security, and Breach Notification Rule.

Time Limit

Rewarding HealthyHabits will maintain all inactive policies and procedures for a period of six(6) years, or greater if required by state or local law in HIPAAtrek.

Availability

Rewarding HealthyHabits will ensure all documentation of policies and procedures are available to all workforce members. All workforce members have access to HIPAAtrek, a cloud-based software where all Rewarding HealthyHabits's compliance related activity, including policies are maintained.

Updates

Rewarding HealthyHabits will review its policies and procedures annually and make updates as appropriate or required.

Person or Entity Authentication

The Person or Entity Authentication Standard of the Security Rule requires that covered entities protect the confidentiality, integrity and availability of electronic protected health information by implementing appropriate measures to ensure proper authentication of users to network and systems. The Person or Entity Authentication Security standard requires covered entities to: “Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”

Person or Entity Authentication

Effective	Revised
8/6/2021 2:03:07 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The Person or Entity Authentication Standard of the Security Rule requires that covered entities protect the confidentiality, integrity, and availability of electronic protected health information by implementing appropriate measures to ensure proper authentication of users to network and systems.

Specification Language

§ 164.312(d) "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to the Person or Entity Authentication Standard as outlined below. Rewarding HealthyHabits shall implement policies and procedures that require a documented process for authenticating persons or entities

Approved Authentication Methods

Authentication processes may include:

1.Documented procedures for granting persons and entities authentication credentials or for changing an existing authentication method.

2.Uniquely identifiable authentication identifiers in order to track the identifier to a workforce member.

3.Documented procedures for detecting and responding to any person or entity attempting to access ePHI without proper authentication.

4.Removing or disabling authentication credentials in ePHI Systems for persons or entities that no longer require access.

5.Periodic validation that no redundant authentication credentials have been issued or are in use.

6.Protection of authentication credentials (e.g., passwords, PINs) with appropriate controls to prevent unauthorized access.

7.When feasible, masking, suppressing, or otherwise obscuring the passwords and PINs of persons and entities seeking to access ePHI so that unauthorized persons are not able to observe them.

Failed Attempts

Rewarding HealthyHabits shall limit authentication attempts to its ePHI to no more than 3 number of attempts. Authentication attempts that exceed the limit may result, as appropriate, in:

1.Disabling relevant account for an appropriate period of time;
2.Logging of event;
3.Notifying Security Officer.

Approved Access Methods

Rewarding HealthyHabits shall use appropriate authentication methods to confirm that only properly authenticated and authorized persons or entities access ePHI. Appropriate access methods may include:

- Unique user IDs;
- Passwords;
- Personal Identification Number (PIN) systems.

Managing Exceptions

Access methods for authentication to ePHI Systems shall not be built into logon scripts. Exceptions may be made only after review and approval by the ePHI Security Officer.

Security Awareness and Training

The Security Awareness and Training standard of the Security Rule requires that covered entities implement a security awareness and training program for workforce members, including providers, with access to Protected Health Information (PHI). Such workforce members should be made aware of the policies and procedures to safeguard the confidentiality, integrity, and availability of PHI in all forms: oral, written, and/or electronic. All workforce members must complete the security awareness training program, and all must certify that such training has been completed. Completion of the training program is required before access can be granted to PHI. Rewarding HealthyHabits offers annual formal trainings in a group setting as well as semi-annual informal trainings. The security awareness and training program will be updated from time to time and will address topics, including but not limited to, the four implementation specifications for this standard. There are four implementation specifications for this standard to illustrate the concept of addressability, especially with regard to high risk analyses pertaining to Rewarding HealthyHabits. The four implementation specifications are: • Security Reminders • Protection from Malicious Software • Log-In Monitoring • Password Management RESPONSIBILITIES: This policy is the responsibility of the HIPAA Security Officer • Ensuring all workforce members understand and follow security related policies and procedures • Maintaining an ongoing security awareness program • Ensuring all workforce members understand and use the installed anti-virus software • Leading compliance activities that bring Rewarding HealthyHabits into compliance with the HIPAA Security Rule implementation specifications of this standard PURPOSE: The purpose of this policy is to implement security awareness and training program for all Rewarding HealthyHabits's workforce members, including providers. Rewarding HealthyHabits understands that “people”, not necessarily technology, are often the largest threat to the security of sensitive information, such as ePHI in the organization.

Security Reminders

Effective	Revised
8/6/2021 2:10:42 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule’s requirements pertaining

to Security Reminders.

Specification Language

§ 164.308(a)(5)(ii)(A) “Implement: …Periodic security updates.”

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Security Reminders as outlined below:

Resposibility Statement

Rewarding HealthyHabits's Security Officer shall be responsible for the taking reasonable steps to ensure that Rewarding HealthyHabits's workforce members receive security information, awareness reminders, and training on Rewarding HealthyHabits's security policies and procedures periodically and as needed.

Method of Security Reminder

Rewarding HealthyHabits will ensure security reminders are provided to workforce members and other entities with access to Rewarding HealthyHabits's PHI. Security reminders may be in written or in verbal form. Security reminders are to be sent through electronic methods, distributed in newsletters, discussed at staff meetings, displayed on posters, displayed on screen savers, or any other method approved by Rewarding HealthyHabits's Security Officer.

Timeframe Security Reminder

Security reminders are to be communicated at least quarterly to all workforce members. Security reminders should be sent out more frequently in the following events:

1. Substantial revisions are made to Rewarding HealthyHabits's security policies or procedures
2. Substantial new security controls are implemented at Rewarding HealthyHabits
3. Significant changes are made to existing Rewarding HealthyHabits security control
4. Substantial changes are made to Rewarding HealthyHabits's legal or business responsibilities
5. Substantial threats are perceived or risks arise against Rewarding HealthyHabits's ePHI systems or network

Method of Security Training

Rewarding HealthyHabits will ensure security training is provided to all workforce members. Security training is required prior to granting access to PHI to any new workforce member, business associate, or subcontractor. Security training may be delivered in-person classroom style learning sessions, webinars, electronic portals, or any other method approved by Rewarding HealthyHabits's Security Officer, so long as the delivery method chosen complies with the content requirements listed within this policy.

Security Training Content Requirements

Workforce members and others with access to Rewarding HealthyHabits's PHI will be formally trained on information security risks and how to follow Rewarding HealthyHabits's security policies and procedures as well as how to use ePHI systems in a manner that reduces security risks and on selected security topics including:

- Rewarding HealthyHabits security policies and procedures
- Rewarding HealthyHabits security controls and processes significant risks to ePHI systems
- Legal and business responsibilities of Rewarding HealthyHabits for protecting ePHI systems
- Security Best Practices

Basic HIPAA principles, although important, are not sufficient. Rewarding HealthyHabits must train workforce members and other entities with access to Rewarding HealthyHabits's PHI on specific policies and procedures adopted by Rewarding HealthyHabits.

Timeframe of Security Training

1. Security training is to be conducted at least annually to all workforce members.

2. All new workforce members must be trained on Rewarding HealthyHabits's security policies and procedures prior to being granted access to systems containing PHI.

3. All workforce members with a change in position requiring higher level of access to PHI must be retrained on Rewarding HealthyHabits's security policies and procedures prior to the change in access being granted.

4. Any workforce member who is found in violation of a security safeguard implemented by Rewarding HealthyHabits must be retrained on Rewarding HealthyHabits's policies and procedures, if required by the Sanction Policy.

Documentation

All security reminders and security trainings must be documented. This documentation should include:

1. Who distributed the reminder/training

2. Who attended or received the reminder/training

3. What topics were covered in the reminder/training

4. What date was the reminder/training

5. What was the purpose of the reminder/training

Protection from Malicious Software

Effective	Revised
8/6/2021 2:11:20 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to Protection from Malicious Software.

Specification Language

§ 164.308(a)(5)(ii)(B) "Implement: …Procedures for guarding against, detecting, and reporting malicious software."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Protection from Malicious Software as outlined below:

Statement of Responsibility

The Security Officer will develop, implement, and periodically review a documented process for guarding against, detecting, and reporting malicious software that pose risks to ePHI. Rewarding HealthyHabits's malicious software prevention, detection, and reporting procedures shall include:

Anti-Malware Installation

Anti-virus and anti-malware installed and updated on ePHI systems.

Workforce Procedures

Procedures for Rewarding HealthyHabits workforce members to report suspected or confirmed malicious software:

1. Close out of all open applications and power down the workstation
2. Notify the Security Officer

Recovery Plan

Plan for recovering from malicious software attacks:

1. Restoring any lost data following the Disaster Recovery Plan
2. Determine level of lost data due to attack
3. Document data lost

Electronic Attachments and Downloads

Process to examine electronic mail attachments and downloads before they can be used on ePHI systems:

1. Install Anti-Malware software that scans emails as well as email attachments
2. Train workforce on identifying suspicious email
3. Scan all download attempts prior to download being finalized
4. Train all workforce members on the potential dangers of downloading certain types of files (.exe, .dmg, .zip)
5. Limit download capability to only key workforce members

Disabling Anti-Malware

Rewarding HealthyHabits's workforce members shall not bypass or disable anti-malware or anti-virus software installed on ePHI systems unless properly authorized to do so. Sanctions will apply to any workforce member attempting to or successfully disabling anti-malware or anti-virus software.

Workforce Training

The Security Officer will provide periodic training and awareness to workforce members about guarding against, detecting, and reporting malicious software. Training workforce members on protection from malicious software shall include:

a. How to discover malicious software
b. How to report malicious software
c. How to discover malicious software fraud
d. How not to download or receive malicious software including not opening or launching email attachments that may contain malicious software

Log-in Monitoring

Effective	Revised
8/6/2021 2:11:57 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) wil be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, (Organization Name) must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule’s requirements pertaining to Log-in Monitoring

Specification Language

§ 164.308(a)(5)(ii)(C) “Implement: …Procedures for monitoring log-in attempts and reporting

discrepancies.”

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Log-in Monitoring as outlined below:

Log-in Process

The Security Officer will develop, implement and periodically review a documented login process for ePHI systems and reporting log-in discrepancies. The log-in process may include:

1.Ensuring help messages that could assist an unauthorized user are not provided during the log-in process

2.Limitations on the number of unsuccessful log-in attempts to 3 attempts

3.The system does not state which part of the log-in information is correct or incorrect if there is an error

4.Prior to successfully completing the log-in process, information system or application identifying information is not provided

5.Upon completion of a successful log-in, the date and time of the previous log-in by the workforce member are displayed

6.If the system doesn't automatically recognize the IP address that the user is logging in from it will require a second authorization code. The system will automatically text another code to the user's mobile phone.

Monitoring Log-in Attempts

The Security Officer will develop, implement and periodically review a documented process for monitoring log-in attempts to ePHI systems and reporting log-in discrepancies. The log-in process may include:

1.Record failed log-in attempts

2.After the specific pre-determined number of failed log-in attempts, a time period is documented before permitting further log-in attempts, or any further attempts are rejected documented before permitting further log-in attempts, or any further attempts are rejected until the Security Officer or designated workforce member or business associate has given authorization.

Log-in Training

Rewarding HealthyHabits will provide training and awareness periodically and as needed to Rewarding HealthyHabits workforce members regarding procedures for monitoring log-in attempts and reporting discrepancies regarding their log-in attempts. The log-in monitoring training and awareness shall include the following topics:

- How to detect a log-in discrepancy
- How to report a log-in discrepancy
- How to successfully use Rewarding HealthyHabits's log-in process

Password Management

Effective	Revised
8/6/2021 2:12:28 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to Password Management.

Specification Language

§ 164.308(a)(5)(ii)(D) "Implement: ....Procedures for creating, changing, and safeguarding passwords."

Policy Procedure

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to Password Management.

Construction Guidelines

Use a pass phrase which is typically composed of multiple words or acronyms. It should not be a word in any language, slang, dialect, or jargon. It should not be based on personal information. Is at least 8 characters long and should contain at least three of the four characteristics of a good password:

1. Upper case letter (A-Z)
2. Lower case letter (a-z)
3. Contain at least 1 numeric character (0-9)
4. Contain a special character (!#?)

Management Guidelines

1. Passwords, if they need to be written down or stored online, must be stored in a secure place separate from the application or system that is being protected by the password

2. Password vaults are encouraged

3. Users should not use the Remember Password feature of applications unless your system or application has the means to encrypt the remembered password

4. If an account or password is suspected to have been compromised, report the incident to the Security Officer and change all passwords

5. Password cracking or guessing may be performed on a periodic and random basis. If a password is guessed or cracked, the user will be required to change it

Password Management Procedure

The Security Officer shall develop, implement, and review a documented process for appropriately creating, changing, and safeguarding passwords used to verify users' identities and obtain access to ePHI. The password management procedure shall include:

1. Require and force periodic password changes

2.The change interval should not exceed 2 years

3.Use of Password Vault with password history is strongly recommended to be used by all workforce members

4.Require and force the use of individual passwords to maintain accountability

5.Permit workforce members to select and change their own passwords

6. Require unique passwords that meet the standards defined by Rewarding HealthyHabits

7. Reuse history should not include the last five passwords.

Training

Rewarding HealthyHabits shall provide its workforce members with training and awareness on appropriately creating, changing, and safeguarding passwords used to verify users identities and to obtain access to ePHI systems. Password management training and awareness shall include:

1. Rewarding HealthyHabitss password standards and guidelines

2. The process for changing temporary passwords when assigned for a new log-in

3. The importance of avoiding maintaining passwords in a paper record

4. The importance of utilizing password vaults

5. The significance of changing passwords and avoiding reusing passwords

6. The significance of keeping passwords confidential

7. The significance of using different passwords for personal and business accounts

8. The importance of not including passwords in any automated log-in process

9. The importance of changing passwords when there is an indication of password or information system compromise

10. The importance of logging off prior to leaving a workstation

Security Incident Procedures

The Security Incident Procedures Standard of the Security Rule requires that covered entities implement policies and procedures to ensure the confidentiality, integrity, and availability of data and resources. The Information Technology Security Incident Procedures Standard requires that appropriate procedures and protocols be developed to identify and report information security incidents and those protocols and procedures be implemented. There is one implementation specification for this standard to illustrate the concept of addressability, especially with regard to high risk analyses pertaining to Rewarding HealthyHabits. The implementation specification is: • Response and Reporting PURPOSE: Rewarding HealthyHabits strives to protect the confidentiality, integrity and availability of ePHI by instituting and documenting reasonable and appropriate safeguards to identify, track, and respond to security incidents promptly. Awareness of, response to, and creation of reports about security incidents in the context of its operations are integral parts of (Practice Name)'s efforts to comply with the HIPAA Security Rule. POLICY: It is the policy of Rewarding HealthyHabits to comply with HIPAA Security Rule regulations in regards to Security Incident Procedures as outlined below. Rewarding HealthyHabits shall implement policies and procedures that require a documented process for promptly identifying, reporting, tracking, and responding to security incidents.

Response and Reporting

Effective	Revised
8/6/2021 2:04:52 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law,Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to Response and Reporting of security incidents

Specification Language

§ 164.308(a)(6)(ii) "Identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes"

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Response and Reporting as outlined below:

Records of Security Incidents

Rewarding HealthyHabits shall have a process for identifying, documenting, and retaining a record of security incidents. Records of a security incident will be maintained for a period of 6 years from the date the security incident occurred, was discovered, or was mitigated, whichever is the greater timeframe.

Rewarding HealthyHabits will maintain a log of security incidents (name location of log here). The log shall include:

a. A description of the incident
b. The location of the incident
c. Workforce members involved in the incident
d. Workforce members who discovered the incident
e. Number of patients affected by the incident
f. Investigative Process and findings
g. Remediation Plan

Response Procedures

All workforce members are required to report suspicious activities to the Security Officer. The Security Officer shall thoroughly investigate all reported suspicious activities.
Rewarding HealthyHabits will conduct an assessment of all discovered security incidents. Security Incidents that are determined to be a significant risk will require a complete risk analysis around the incident
and deployment of the Security Incident Response Team (SIRT). The SIRT is responsible for:

a. Assemble the necessary SIRT members
b. Properly identifying an incident and the extent of the incident
c. Providing immediate notification to appropriate parties
d. Consider risk assessment specific to the incident
e. Gather data and/or evidence
f. Analyze the available information
g. Determine the extent of access or damage
h. Create an action plan and get-well time frame

Security Incident Types

A security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An incident is the culmination of one or more events with adverse effects. An imminent threat of violation refers to a situation in which the organization has a factual basis for believing a specific incident is about to occur.

Security incidents include the following:

A system or network breach accomplished by an internal or external entity
An unauthorized disclosure
An unauthorized disclosure or destruction of ePHI (i.e., delete dictation, data alterations not following Rewarding HealthyHabits procedures
Physical intrusion/security incident/active shooter
Disaster or enacted threat to business continuity
Denial of Service
Malicious Code
System Hijacking
Unplanned Downtime

Security incidents may also include the following:

Use of another person's individual password and/or account login
Posting passwords on equipment
Leaving workstations unattended while actively signed on
Installation of unauthorized software
Posting of PHI on the internet from a web portal
Discarding of PC hard drives, CD or other devices without appropriate destruction
Terminated workforce member accessing applications, systems, or network

Reporting Procedures

Reporting of security incidents to the Office for Civil Rights:

https://ocrnotifications.hhs.gov/.

Rewarding HealthyHabits shall adhere to its Breach Notification Policy when reporting security incidents.

Rewarding HealthyHabits shall report all incidents affecting fewer than 500 individuals to the Office for Civil Rights annually.

Rewarding HealthyHabits shall report all incidents affecting 500 or more individuals to the Office for Civil Rights within 60 days of the date of incident or date of discovery, whichever is less

Incident Response Team

Rewarding HealthyHabits recognizes that there may be security incidents that require an incident response team. Rewarding HealthyHabits shall deploy a security incident response team (SIRT) to oversee security incidents. The determination of whether or not to deploy an incident response team will be a direct result of the security assessment conducted around the incident itself. The security response team may consist of the following team members:

HIPAA Security Officer
HIPAA Privacy Officer
Senior Management
Information Technology Staff
Facility Manager

Optional Members may include:

Legal Counsel
Contractors
Workforce member(s) involved in the incident

The incident response team may vary from incident to incident, based on complexity, threat level, and mitigation response needs.

Training

Conduct training and awareness for workforce members to include:

a. Documentation process for promptly reporting a security incident

b. Responding to security incidents in accordance to Rewarding HealthyHabits's policies and procedures

No Rewarding HealthyHabits workforce member will prohibit or otherwise attempt to hinder or prevent another workforce member from reporting a security incident

ii. Rewarding HealthyHabits workforce members shall cooperate fully with the Incident Response Team investigations

iii. Rewarding HealthyHabits workforce members are free to report known or perceived

security incidents without fear of retaliation

Ransomware Response and Reporting

Effective	Revised
8/6/2021 2:05:16 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to response and reporting of security incidents which may include a ransomware event.

Specification Language

§ 164.308(a)(6)(ii) "Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner".

Policy Procedures

It is the policy of {{Organization}} to comply with ransomware response and reporting as outlined in this policy. Ransomware management consists of three phases; prevention, response, and recovery.

Ransomware Defined

Ransomware is a type of malware (malicious software) which attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. The ransomware may also destroy or exfiltrate (remove) the data. A ransomware attack is considered a security incident.

Ransomware Prevention

Ransomware prevention begins with proactive steps to prevent the attack or to minimize the effects of a successful attack. Rewarding HealthyHabits will delegate specific staff the responsibility to conduct and document the following preventive measures:

1. Conduct a security risk analysis to reduce risks and vulnerabilities to a reasonable and appropriate level
2. Update firmware of network devices and entities as part of risk analysis and security management process
3. Apply intrusion detection systems (IDS) and other monitoring applications
4. Train users on malicious software protection and detection
    a. Be cautious of clicking directly on links in emails
    b. Be wary of compressed or ZIP file attachments
    c. Attempt to verify web addresses (URL) independently
5. Implement access controls to limit access to e-PHI to only those who are authorized
6. Conduct and maintain frequent backups from which data can be recovered
7. Test restorations of backup to ensure continuity of operations can be restored (maintain backups off line if feasible)
8. Install virus protection software, firewalls, and email filters
9. Ensure patches are updated for your applications, operating systems, and software

Ransomware Response

Ransomware response begins the moment ransomware is indicated to have infiltrated your information systems. Response requires specific steps to identify the malware, contain the malware, eradicate the malware. Afterwards, Rewarding HealthyHabits will move to the recovery phase and then return to normal business operations. The Incident Response Team and/or specific staff are delegated the responsibility to conduct and document the following response measures:

1. Rewarding HealthyHabits will conduct an initial analysis to identify the ransomware
    a. Is it a known malware?
    b. What are the algorithmic steps undertaken by the malware?
    c. What are the characteristics of the attack?
    d. Where did it originate? (who/what/where/when)?
    e. What are industry recommendations for this type of malware?
    f. Contact the following agencies for assistance and to report the crime and seek guidance:
        i. Local Police Department: _____
        ii. Regional FBI Office: _____
            1. Cyber Task Force: www.fbi.gov/contact-us/field
            2. Internet Crime Complaint Center: www.ic3.gov
            3. United States Secret Service: www.secretservice.gov/contact/
            4. Dept. of Homeland Security United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov
2. Rewarding HealthyHabits will attempt to contain the impact and propagation of the ransomware
    a. What systems or hardware have been impacted by the malware?
    b. What systems should be taken off the network (isolated) to prevent further spreading of malware?
3. Rewarding HealthyHabits will attempt to eradicate the ransomware
    a. What steps can the organization take to remove the ransomware if possible?
        i. Try industry ransomware removal solutions, or
        ii. Completely wipe clean all machines and reinstall the operating system
        iii. Consider paying the ransom (communicate with authorities before paying)

Ransomware Recovery

1. Rewarding HealthyHabits will recover from ransomware attack when ransomware is completely removed
    a. Restore data lost during the attack
    b. Use data back-ups that have not been infected (clean data)
        i. Consider off-line backups which should be free of malware
    c. Reconnect the systems that were taken offline
    d. Applications/systems that cannot be cleaned of the ransomware will be permanently removed from the inventory

Breach Risk Assessment

The Office for Civil Rights (OCR) considers all ransomware attacks as breaches of Protected Health Information (PHI). A breach under the HIPAA rules is defined as “the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA privacy rule which compromises the security or privacy of PHI”. When PHI is encrypted by a ransomware attack, a breach is presumed to have occurred because the PHI was acquired by individuals who have taken possession and control of the information.

Rewarding HealthyHabits will conduct a breach risk assessment to determine if the risk of compromise of the ePHI is greater than low. Each ransomware incident is unique in of itself and must be assessed to determine if notification to the affected individuals is warranted. Rewarding HealthyHabits will review the Breach Notification Policy for steps on conducting the breach risk assessment and record the ransomware incident in their security incident log.

Security Management Process

The Security Management Process is a standard in the Administrative Safeguards of the HIPAA Security Rule. There are four Implementation Specifications in this standard: Risk Analysis, Risk Management, Sanction Policy and Information System Activity Review. The security management process forms the foundation upon which Rewarding HealthyHabits's security activities are built. The purpose of this standard is to meet the HIPAA Security Rule which requires Rewarding HealthyHabits to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI” . . . as well as, to “implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply.”

Risk Analysis

Effective	Revised
8/6/2021 2:26:39 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule’s requirements pertaining to the integrity, confidentiality, and availability of ePHI.

Specification Language

§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 Procedures

It is the policy of Rewarding HealthyHabits to conduct or review a Risk Analysis on an annual basis as outlined below.

Identify Potential Vulnerabilities

Develop a list of vulnerabilities (flaws or weaknesses) that could be exploited by threat sources. This list focuses on realistic technical and nontechnical areas where ePHI can be disclosed without proper authorization, improperly modified, or made unavailable when needed.

Assess Security Controls

Determine if the implemented or planned security controls will minimize or eliminate risks to ePHI. A thorough understanding of the actual security controls in place for a covered entity will reduce the list of vulnerabilities, as well as the realistic probability, of a threat attacking (intentionally or unintentionally) ePHI.

Likelihood of a Threat Exposing a Vulnerability

Determine the likelihood, and the potential adverse impact resulting from a threat successfully exploiting a vulnerability. A business impact assessment prioritizes the impact levels associated with the compromise of information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support critical missions.

Determine the Level of Risk

Assess the level of risk to the Information Technology (IT) systems. The determination of risk takes into account the information gathered and determinations made during the previous steps. The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and the resulting impact of threat occurrence.

Scope the Assessment

The first step in assessing risk is to define the scope of the effort. To do this, it is necessary to identify where ePHI is created, received, maintained, processed, or transmitted. Ensure that the risk assessment scope takes into consideration the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).

Gather Information

Identify the conditions under which ePHI is created, received, maintained, processed, or transmitted. This includes identifying the security controls being used to protect the ePHI.

Identify Realistic Threats

Identify potential threat sources and compile a threat statement listing potential threat sources that are applicable to the operating environment. The listing of threat sources includes realistic and probable human and natural incidents that can have a negative impact on the ability to protect ePHI.

Recommend Security Controls

Recommend security controls that could mitigate the identified risks, as appropriate to the organization's operations. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. Security control recommendations provide input to the risk mitigation process, during which the recommended security controls are evaluated, prioritized and implemented.

Document Risk Assessment Results

Once the risk assessment has been completed (threat sources and vulnerabilities identified, risks assessed, and security controls recommended), the results of each step in the risk assessment should be documented.

Risk Management

Effective	Revised
8/6/2021 2:27:05 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to the integrity, confidentiality, and availability of ePHI.

Specification Language

§164.308(a)(1)(ii)(B) "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."

Policy Procedure

It is the policy of Rewarding HealthyHabits to maintain a continuous risk management program to ensure that appropriate security measures are selected and implemented to protect the confidentiality, integrity, and availability of ePHI. Security measures will commensurate with the risks to the information systems that store, process, transmit or receive ePHI, and will be designed to reduce the risks to ePHI to reasonable and manageable levels.

Risk Management Components

Selection, implementation, and operation of safeguards will be based on a formal, documented risk management process and will include the following.

- A formal risk analysis that documents and prioritizes risks to information assets that store,

process, transmit, or receive ePHI. See the Risk Analysis Policy.
- Selection and implementation of reasonable, appropriate, and cost-effective security measures to manage or mitigate identified risks.
- Security awareness training for workforce member and security management training for HIPAA Security Officer.
- A regular patch management program to ensure that systems and software are protected from new software vulnerabilities.

Risk Prioritization

Using information from the risk analysis, risks will be ranked based on the potential impact to information systems containing ePHI and the probability of occurrence. When deciding what resources should be allocated to identify risks, the highest priority will be given to risks with unacceptable risk ratings.

Safeguard Selection

Select the most appropriate security methods to mitigate or manage identified risks to critical information systems and ePHI. Such selections will be based on the nature of specific risks and the feasibility, effectiveness, and cost of specific safeguards.

Security Method Evaluation

Selected security safeguards will be regularly evaluated and revised as necessary.

Results

The results of each of the above steps will be formally documented.

Risk Management Implementation

For the risk management plan to be successful, key members of Rewarding HealthyHabits must be involved. Management will determine which risks uncovered by the risk analysis must be addressed immediately as well as create a timetable for risks that are determined to be a lower priority. Rewarding HealthyHabits Security Officer shall delegate tasks necessary to appropriate team members as well as monitor the completion of the delegated tasks. Steps taken to mitigate risks shall be documented in the Risk Management Plan.

Sanctions

Effective	Revised
8/6/2021 2:27:31 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits

must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client. The Sanction Policy of the rule requires formal, documented policies and procedures that address how a covered entity addresses the security violations of ePHI by it's workforce to include misuse of workstation, breach of security, and disregard for the security environment.

Specification language

§164.308(a)(1)(ii)(C) "Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

Policy Procedures

It is the policy of Rewarding HealthyHabits to ensure that all HIPAA Security policies are followed. Appropriate sanctions will be taken against those who violate HIPAA security policies and/or procedures within the HIPAA Security Manual.

Policy Availability

All staff and workforce members will be provided a copy of the HIPAA Security Manual and will sign a statement confirming receipt.

Staff Policy Awareness

Each employee will be oriented on HIPAA security, its importance, and disciplinary actions for violations.

Policy Adherence Monitoring

The HIPAA Security Officer will monitor to ensure all policies are followed. Employees witnessing violations should report the violations to the HIPAA Security Officer. If there is a breach or a violation of these policies/procedures, the HIPAA Security Officer will address the situation. Employees violating any policy and/or procedure within the HIPAA Security Manual will face disciplinary action as defined.

Level 1 (Least Severe) Violation

Accessing information that you do not need to know to perform your job, sharing computer access codes (user name & password), leaving your computer unattended while you are logged into a ePHI program, changing information without authorization, failing/refusing to cooperate with the Management, Supervisors, and/or the HIPAA Security Officer.

Level 2 (Moderately Severe) Violation

Second occurrence of any Level 1 offense (does not have to be the same offense), unauthorized disclosure or use of PHI, using another person's computer access code, failing/refusing to comply with remediation resolution or recommendation.

Level 3 (Most Severe) Violation

Level 3 Violation: Copying information without authorization, disclosing confidential or patient information with unauthorized persons, discussing confidential information with an unauthorized person (this includes all unauthorized online discussions and social networking posts) ,failure to report security incidents as outlined.

Sanctions

In the event that a member of the Rewarding HealthyHabits's workforce violates the HIPAA Security and Privacy policies/procedures, the following recommended disciplinary actions will apply:

Level 1 (Least Severe) Sanction

Level 1 Sanctions: Verbal or written counseling, retraining on privacy/security awareness, retraining on Rewarding HealthyHabits's privacy and security policies, and/or civil and criminal prosecution, and retraining on the proper use of internal/required forms.

Level 2 (Moderately Severe) Sanction

Final written counseling, retraining on HIPAA awareness, retraining on Rewarding HealthyHabits's privacy and security policies and civil and criminal prosecution, retraining on the proper use of internal/required forms.

Level 3 (Most Severe) Sanction

Termination of employment or other civil penalties as provided under HIPAA or other applicable Federal/State/Local law.

Exceptions

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment with Rewarding HealthyHabits as well as civil penalties as applicable by Federal/State/Local Law.

Disclaimer

The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, Management and/or HIPAA Security Officer shall consult prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

Information System Activity Review

Effective	Revised
8/6/2021 2:27:58 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to the integrity, confidentiality, and availability of ePHI.

Specification Language

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

Policy Procedures

It is the policy of Rewarding HealthyHabits to ensure that all HIPAA Security policies are followed. Rewarding HealthyHabits will make reasonable efforts to regularly review records of activity on information systems containing ePHI. Appropriate hardware, software, or procedural auditing mechanisms should be implemented on Rewarding HealthyHabits's information systems that contain or use ePHI. The level and type of auditing mechanisms that must be implemented are determined by Rewarding HealthyHabits's risk analysis process. Records of activity created by auditing mechanisms should be reviewed regularly.

Review Of IT Records

Rewarding HealthyHabits shall make reasonable efforts to regularly review records of activity on information systems containing ePHI. Records of activity may include but are not limited to:

- Audit Logs
- Access Reports
- Security Incident Tracking Reports

Auditing Mechanisms

Appropriate hardware, software, or procedural auditing mechanisms should be implemented on Rewarding HealthyHabits information systems that contain or use ePHI. At a minimum, such mechanisms should provide the following information:

- Date and time of activity
- Origin of activity
- Identification of user performing activity
- Description of attempted or completed activity

Auditable Events

The level and type of auditing mechanisms that must be implemented on Rewarding HealthyHabits information systems that contain or use ePHI must be determined by (Organization Name)'s risk analysis process. Auditable events can include but are not

limited to:

- Access of sensitive data
- Use of audit software programs or utilities
- Use of privileged account
- Information system start-up or start
- Failed authentication attempts
- Security incidents
- How reviews are documented
- How often a review is performed

Review Of Audit Records

Records of activity created by audit mechanisms implemented on Rewarding HealthyHabits information systems should be reviewed regularly. The frequency of such review must be determined by Rewarding HealthyHabits's risk analysis. At a minimum, the risk analysis should consider the following factors:

- The importance of the applications operating on the information system
- The value or sensitivity of the data on the information system
- The extent to which the information system is connected to other information systems

Document Review

Such review should be via a formal documented process. At a minimum, the process should include:

- Definition of which workforce members will review records of activity
- Definition of what activity is significant
- Definition of which activity records need to be archived and for what period of time
- Procedures defining how significant activity will be identified and reported
- Procedures for preserving records of significant activity

Oversight Of Review

Whenever possible, Rewarding HealthyHabits's workforce members should not monitor or review activity related to their own user account.

Assess Safeguards (Policies)

Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic health information.

Procedure if Safeguard is Reasonable

Implement the implementation specification if reasonable and appropriate.

Procedure if Safeguard is Unreasonable

If implementing the implementation specification is not reasonable or appropriate

- Document why it would not be reasonable and appropriate to implement the implementation specification
- Implement an equivalent alternative measure if reasonable and appropriate

Implementation Accomplished by

Implementation of this specification is accomplished through:

- The Security Officer will develop and implement an internal audit procedure that will provide regular review of records of information system activity.
- The process implemented to provide review will be designed to promote a continuing review of information system activity that will assist in the identification of potential and/or actual security breaches so that immediate corrective action may be taken.

Responsibility of Audit

The internal audit procedure reviewing information system activity will be performed by the Security Officer.

Components of Audits

The internal audit procedure will include:

- Identification of electronic data sites
- Identification of information to be collected from the data sites that will assist in identification of actual and/or potential security issues
- Assimilation of information from the data collection sites into a report format that will be useful for reviewing electronic information system activity and assist in identification of security issues
- As deemed necessary, review designated records or reports of information system activity

Report Responsibility

The Security Officer will develop, implement, and monitor all necessary information system review reports.

- The Security Officer will identify what information or reports are needed by the information system to adequately audit internal electronic security process
- The Security Officer will develop all reports necessary to adequately monitor the electronic security processes
- The Security Officer will, as deemed necessary, review the electronic system activity reports
- The Security Officer, based on review of information system activity reports, will develop parameters for normal or average; activity levels. Normal based on access at a specific site, frequency of access of other relevant criteria

Investigation of Findings

Based on development of normal information system levels, the Security Officer will be responsible for investigating identified abnormalities or unusual information system activities.

Investigation may include:

- Interview of workforce member(s)
- Review of information system activity and/or
- Any other additional information gathering that may be necessary

The Security Officer will be responsible for any necessary response to the identified security abnormality. The response may include:

- Correction of any information system security problem
- Workforce member education of sanction.

The Security Officer will be responsible for collecting, documenting, and maintaining information system activity reports and related activities, including investigation and mitigation.

Documentation of information system activity review, investigation, and/or resolution will be maintained by the Security Officer for a minimum of six years from the date information was created.

Transmission Security

The Transmission Security Standard of the Security Rule requires that covered entities implement policies and procedures to ensure the confidentiality, integrity, and availability of data and resources. The purpose of this standard to ensure electronic Protected Health Information being transmitted is being protected. The Transmission Security standard requires covered entities to: ““Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.” There are two implementation specifications for this standard to illustrate the concept of addressability, especially with regard to high risk analyses pertaining to Rewarding HealthyHabits. The implementation specifications are: Integrity Controls Encryption

Integrity Controls

Effective	Revised
8/6/2021 2:13:49 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with HIPAA’s Security Rule requirements pertaining to the integirty of PHI being transmitted electronically.

Specification Language

§ 164.312(e)(2)(i) "Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Integrity Controls as outlined below.

Approved Protocols

Electronic transmissions will be through secure protocols:

1. Email is permitted if and only if the email is properly encrypted as outlined in Rewarding HealthyHabits's Transmission Security Standard's Encryption Policy.
2. Facsimile is permitted if and only only if a cover sheet is used with {OrgName}}'s privacy statement and contact information clearly visible.
3. Electronic Medical Record Messaging is permitted through Rewarding HealthyHabits's certified EMR system.
4. Other methodologies for transmitting PHI electronically must be reviewed and approved in writing by the Security Officer.

Prior to Transmission

1. All receiving entities will be authenticated before transmission.
2. Any transmissions should include only the minimum amount of PHI.

Encryption

Effective	Revised
8/6/2021 2:14:41 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this document is to define and implement an encryption policy related to creating algorithms and keys that meet or exceed industry standards for data security. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies inside of the United States.

Specification Language

§ 164.312(e)(2)(ii) "Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Encryption as outlined below.

Strength

All encryption mechanisms for electronic transmission are to support a minimum of 128-bit encryption, with 256 or higher being preferred.

Disclaimer

Encryption for the purposes of transmission shall adhere to the Encryption and Decryption policy of the Access Controls Standard.

Transmission Security Procedures

Effective	Revised
8/6/2021 2:15:46 PM	

Policy Background

The Transmission Security Standard of the Security Rule requires that covered entities implement policies and procedures to ensure the confidentiality, integrity, and availability of data and resources. The purpose of this standard to ensure electronic Protected Health Information being transmitted is being protected.

Policy Purpose

In order to comply with the technical security measures of this standard, Rewarding HealthyHabits must specify methods used to transmit ePHI: email, Internet, Peer-to-Peer, VPN, RDP, and any other mechanism used to transmit ePHI. Appropriate means must be taken to protect the confidentiality, integrity and availability of the ePHI being transmitted. In accordance, it is strictly against Rewarding HealthyHabits's policies and procedures to allow transmission of ePHI through unsecure networks such as SMS texting, unapproved applications (mobile or standard), unsecured personal devices, and any other unapproved mechanism.

Specification Language

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

Policy Procedures

Rewarding HealthyHabitsstrives to protect the confidentiality, integrity and availability of ePHI by taking reasonable and appropriate steps to establish and implement documented transmission security controls.

Email: External

Use of E-mail to transmit PHI can be used if the following conditions are met:

i. The PHI data must be in a password protected document.

ii. The sender can authenticate the receiver.

iii. The receiver has given permission to have their PHI sent via E-mail.

iv.The receiver has been made aware of the risks involved through “ePHI Disclosure” statement is included in the signature of every email containing ePHI: “The information contained in this email is confidential and may contain privileged patient information protected under federal and/or state law and is intended only for the use of the individual or entity to which it is addressed. If you are not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received the communication in error, please notify the sender as listed and destroy this message.”

Email: Internal

Use of internal E-mail to send PHI is allowed if the following conditions are met:

i.The PHI data must be in a password protected document.

ii.The minimum amount of PHI is sent.

iii.The E-mail is not forwarded to any parties.

iv.“ePHI Disclosure” statement is included in the signature of every email containing ePHI: “The information contained in this email is confidential and may contain privileged patient information protected under federal and/or state law and is intended only for the use of the individual or entity to which it is addressed. If you are not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received the communication in error, please notify the sender as listed and destroy this message.”

Workforce Security

The Workforce Security standard of the Security Rule requires that covered entities implement policies and procedures to ensure all workforce members have appropriate access to ePHI, as provided by HIPAA, and to prevent those workforce members who do not have access under HIPAA from obtaining access to ePHI. The workforce security process requires covered entities to control access to ePHI and to allow appropriate access to ePHI for workforce members to perform their job responsibilities and to preclude such access to workforce members who do not need such information for conduct of their job responsibilities. There are three implementation specifications for this standard to illustrate the concept of addressability, especially with regard to high risk analyses pertaining to Rewarding HealthyHabits. The three implementation specifications are:• Authorization and/or Supervision• Workforce Clearance Procedure• Termination Procedures. The purpose of this standard is to ensure workforce security procedures include requirements for authorization and supervision of access to confidential information as well as appropriate clearance procedures to approve and terminate access. These procedures must include reasonable and appropriate safeguards to prevent unauthorized access to confidential information while ensuring properly authorized workforce member's access is permitted.

Authorization and Supervision

Effective	Revised
8/6/2021 2:07:30 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to authorization and/or supervision of workforce members to work with ePHI or in locations where it might be located.

Specification Language

§ 164.308(a)(3)(ii)(A) "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."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with the HIPAA Security Rule and

regulations in regards to Authorization and Supervision as outlined below:

As Part of the Risk Analysis

As part of the Risk Analysis:

- Determine which workforce members have need for access to ePHI as part of their job responsibilities
- Describe such needs, corresponding authorization, and supervision responsibilities in job descriptions
- Be sure workforce members understand these needs

Audit Controls

Procedures must be in place for logging and tracking authorized workforce members' access to systems containing ePHI.

Rewarding HealthyHabits has implemented audit controls for all systems containing ePHI including

- Storage locations of estimates and invoices
- Workstations
- Servers

Access Levels

Procedures must be in place for granting different levels of access to ePHI.

Rewarding HealthyHabits has the ability to grant role-based access to systems.

Rewarding HealthyHabits has implemented role-based access to systems containing ePHI. Minimum Necessary Access has been addressed and is noted in the Minimum Necessary Access policy of the Privacy Rule and/or on Rewarding HealthyHabits's job descriptions which are given to workforce members.

Workforce Clearance Procedures

Effective	Revised
8/6/2021 2:09:02 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law,Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to workforce clearance procedures for workforce members who work with ePHI or in locations where it might be located, accessed, or transmitted.

Specification Language

§ 164.308(A)(3)(ii)(B) "Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with Workforce Clearance Procedures as outlined below:

Confidentiality Agreements

All Rewarding HealthyHabits's workforce members with access to confidential information and/or PHI must sign a confidentiality agreement.

Risk Analysis Statement

Clearance will be an outcome of the risk analysis and elaboration of authorization in job descriptions. As part of the risk analysis, Rewarding HealthyHabits shall consider criteria for a background check for each workforce member candidate.

Defining a Position

When defining an organizational position, the HIPAA Security Officer must identify and define both the security responsibilities and the level of supervision required for the position.

New Workforce Member Procedures

The background of all workforce candidates will be adequately reviewed during the hiring process. Verification checks must be made as appropriate, may include but not limited to:

- Character references
- Verification of academic achievements
- Professional license verification
- Credit Checks – for positions with fiscal responsibility including management, billing
- Criminal Background Checks

Termination Procedures

Effective	Revised
8/6/2021 2:09:44 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purposes

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to workforce termination procedures for workforce members who work with ePHI or in locations where it might be located.

ASSUMPTIONS: This Terminal Procedure is based on the following assumptions:

• In any organization, people are the greatest asset in maintaining an effective level of security

• Conversely, people are the greatest threat to data security and confidentiality

• A terminated employee may pose a threat to data security and confidentiality, particularly if dissatisfied with his or her employment or termination

Specification Language

§ 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) [Workforce Clearance Procedure] of this section."

Policy Procedures

When an Rewarding HealthyHabits employee will be ending their relationship with Rewarding HealthyHabits, the HIPAA Security Officer will plan the termination of access to ePHI for the departing workforce member and document the following:

Documentation Requirements for Termination

1. Date and time of notice of workforce member departure received
2. Date of planned workforce departure
3. Description of access to be terminated
4. Date, time, and description of actions taken

Access Termination

When an Rewarding HealthyHabitsemployee will be ending their relationship with Rewarding HealthyHabits, all privileges and access to ePHI systems, including both internal and remote information system privileges will be disabled or removed by the time of departure. Information system privileges include but are not limited to: workstations, server access, data access, network access, email accounts, and inclusion on the group email lists. Physical access to areas where ePHI is located will be terminated as appropriate. Rewarding HealthyHabits will

deactivate or change physical security access codes used to protect PHI.

Removal Statement

A workforce member who ends employment with Rewarding HealthyHabits will not retain, give away, or remove from Rewarding HealthyHabits's premises any information that could compromise the PHI of any client, past or present. At the time of his or her departure, a workforce member will provide information that could access ePHI in his or her possession to his or her supervisor. Rewarding HealthyHabits reserves the right to pursue any and all remedies against workforce members who violate this provision.

Termination Checklist

Rewarding HealthyHabits will track and log the return of equipment and property or having the ability to access ePHI with the workforce member's name, date, and time equipment and property were returned. The equipment and property that may contain, allow or enable the workforce member to access ePHI may include; but is not limited to:

- Portable computers
- Building/Office Keys
- Portable media
- Smart Phones
- Pagers

Voluntary Termination

Voluntary Termination (Resignation)
Steps are as follows:
1. Workforce member notifies HIPAA Security Officer of resignation
2. Supervisor will notify Payroll of termination
3. Supervisor will pull Employee Personnel File and schedule an exit interview
4. Payroll will issue final check including appropriate number of hours worked, vacation payoff, pro-rated PTO payoff.
5. Final paycheck will be issued with the next payroll
6. Termination of accesses will be scheduled for the final date of employment
a. Workforce member will sign an acknowledgement that access will be terminated and that any attempt of access after Rewarding HealthyHabits terminates access will be viewed as a criminal offense and will be prosecuted to the fullest extent of the law
7. The final date of employment, if appropriate, workforce member will be presented with separation package including legal notices regarding COBRA, 401(k), etc

Involuntary Termination

Involuntary Termination (Discharge or Layoff)
Steps are as follows:
1. Supervisor compiles all documentation to support termination
2. Supervisor will total the workforce member's last working day and total hours worked that pay period.
3. Supervisor will notify Payroll of the termination, pull the employee's personnel file and prepare for the termination.
4. Payroll will issue final check including vacation payoff and pro-rated PTO payoff.
5. The Security Officer will terminate all access to Rewarding HealthyHabits's network,

systems, and facilities no later than the date and prior to the time of the termination.
6. On the date of termination, if appropriate, the workforce member will be presented with separation package including legal notices regarding COBRA, 401(k), etc.

Workstation Security

The Workstation Security Standard of the Security Rule requires that all covered entities implement physical safeguards for all workstations that access ePHI and restrict access from unauthorized use.

Workstation Security

Effective	Revised
8/6/2021 2:03:38 PM	

Policy Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IHII) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits is committed to ensuring the security of its computerized clinical and business information systems and equipment. Its computer hardware and software as well as the information and data carried b y the system are the sole property of Rewarding HealthyHabits.

Specification Language

§ 164.310(c) "Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users".

Policy Procedures

It is the policy of Rewarding HealthyHabits to comply with the Workstation Security as outlined below:

Manual Testing

Rewarding HealthyHabits will prevent unauthorized physical access to workstations that can access ePHI and ensure authorized workforce members have appropriate access. Periodic manual testing to ensure proper logoff procedures have been followed will be conducted on all Rewarding HealthyHabits workstations.

Location of Workstations

Rewarding HealthyHabits workstations containing ePHI will be located in locations that minimize the risk of unauthorized access to them.

Portable Devices

All portable workstations will be securely maintained when in the possession of the workforce member issued the device.

Unauthorized Access Prevention

Rewarding HealthyHabits workforce members will take reasonable measures to prevent unauthorized access to ePHI visible on their workstation. Such measure include, but are not limited to:

Locating workstations and peripheral devices (printers, modem, scanners, etc) in secured areas that are not accessible by unauthorized persons

Positioning monitors or shielding workstations so that data on the screen is not visible to unauthorized persons.

Unauthorized Rewarding HealthyHabits workforce members must not attempt to gain physical access to workstations without proper authorization from HIPAA Security Officer.

Risk Assessment

The level of physical protection provided for (Organization Name) workstations containing ePHI will be commensurate with that of identified risks. An assessment of the risks to (Organization Name) workstation that can access ePHI will be conducted at least annually, as outlined in (Organization Name)’s Risk Management Policies. The risk assessment report will be securely maintained.

Workstation Use

The Workstation Use Standard of the Security Rule requires that all covered entities implement policies and procedures to ensure 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 workstations that can access ePHI.

Workstation Use

Effective	Revised
8/6/2021 2:04:09 PM	

Policy Background

The Health Insurance Portability and Accountability act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of PHI. According to the law, Rewarding HealthyHabits must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

Policy Purpose

Rewarding HealthyHabits is committed to ensuring the security of its computerized clinical and business information systems and equipment. Its computer hardware and software as well as the information and data carried by the system are the sole property of Rewarding HealthyHabits. Any misuse of Rewarding HealthyHabits's workstations may result in sanctions as outlined in the Sanction Policy of the Rewarding HealthyHabits.

The intent of Rewarding HealthyHabits's Workstation Use policy is to:

- Ensure that each workstation has the necessary access controls to restrict unauthorized users and programs from accessing ePHI or sensitive business information
- Ensure that software on each workstation on the network is compatible and will not lead to the degradation of the system
- Ensure that users are oriented and trained on workstation use and the maintenance of information integrity, privacy, and resource security
- Establish the security requirements for the appropriate use of mobile computing devices including: smart phones, laptops, notebooks, tablets, iPads and other Personal Digital Assistants or any other device that access ePHI or interface to the network.

Specification Language

§ 164.310(b) "Implement policies and procedures that specify the proper functions to be

performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."

Policy Procedures

User Responsibilities for Rewarding HealthyHabits Workstations

Workforce members are responsible for maintaining the security of Rewarding HealthyHabits's computer resources under their control and for protecting the integrity and privacy of the data maintained on them by the appropriate use of lock down, password controlled access, data encryption, virus protection, and routine backup as outlined elsewhere in Rewarding HealthyHabits's Security Policies and Procedures.

Rewarding HealthyHabits reserves the right to inspect all data and to monitor the use of all its computer systems, and as such, workstation users have no right of privacy with regard to information on or around workstations. Rewarding HealthyHabits's right of access to personally owned computed devices will be limited to Rewarding HealthyHabits's patient or business information and applications important to maintaining security over that information, including, but not limited to anti-virus software, operating systems, etc. Rewarding HealthyHabits reserves the right to remotely access, monitor, control, and configure workstations and any software residing on them. Non-compliance with this policy is subject to disciplinary action as defined in Rewarding HealthyHabits's Sanction Policy or as recommended upon management review.

Statement of Intent

Rewarding HealthyHabits protects ePHI by enforcing workstation use procedures on all workstations that access, store, or process ePHI. All workstations with fixed storage that support more than one user, process critical and/or sensitive information including modems, copiers, and scanners, must be equipped with security that protects hardware and/or restricts access to hardware.

Malware

All workstations must be equipped with updated software for detecting the presence of malware in accordance to Rewarding HealthyHabits's Malicious Software Policy.

1. All computing devices must have the most current versions of anti-virus and anti-malware software enabled.
2. Operating systems must have critical updates installed.

Unauthorized Viewing

All workstations must be positioned or located in a manner that will minimize the exposure of any ePHI or business information from being displayed to any unauthorized individual. When appropriate, privacy screens should be deployed.

Remote Access

Users accessing the Rewarding HealthyHabits network or information from remote locations,

such as connections from home, should employ the appropriate safeguards.

- Do not access ePHI or sensitive business information in a location in which unauthorized viewing is likely, this includes family members
- Do not access ePHI on a device in which the proper software for detecting the presence of malware is not deployed
- Before utilizing a personal computing device to access ePHI or sensitive business information, Rewarding HealthyHabits must first approve its use
- Ensure all Rewarding HealthyHabits's policies and procedures for workstation security are deployed when accessing ePHI or sensitive business information remotely

  Access to Rewarding HealthyHabits's computer systems from remote locations must be approved by the HIPAA Security Officer. All physical safeguards must be observed at the remote access including limiting unauthorized viewing of patient and/or sensitive business information. It is the responsibility of the remote user to ensure that remote access to Rewarding HealthyHabits's computer systems is not used by unauthorized individuals. Users with remote access from personally owned computing devices bear the responsibility of employing security protections such as anti-virus/malware software.

Software Installation

Rewarding HealthyHabits shall have sole discretion in determining which hardware, operating systems, and connectivity solutions will be supported. Users may not independently install connectivity hardware or software to the computing resources or devices of Rewarding HealthyHabits without the proper authorization from Rewarding HealthyHabits management and/or HIPAA Security Officer. All workforce members must comply with Rewarding HealthyHabits policies, state, federal, state, and local laws and regulations regarding the proper acquisition, use, and copying of copyrighted software and commercial software licenses.

Installation of personal software purchased or downloaded, including but not limited to, screensavers and animated GIFs is strictly prohibited on Rewarding HealthyHabits's workstations.

Logoff

Users are required to logoff of applications containing ePHI or sensitive business information as well as the workstation prior to leaving their workstation.

All systems containing ePHI or sensitive business information shall have auto-logoff enabled. The delay is specified at 2-15 minutes. Exceptions must be approved in writing by the HIPAA Security Officer.

Storage Devices

Users are not permitted to store ePHI or sensitive business information to portable media devices without the proper authorization from Rewarding HealthyHabits or the HIPAA Security

Officer.

Accidental Deletion

In the event a critical document or file is inadvertently deleted, contact Rewarding HealthyHabits immediately for help. Do not continue to use the workstation or save additional work as this could further compromise the availability and/or integrity of ePHI or sensitive business information.

Portable Security

All laptops and any other portable computer equipment must be secured when not in use. Proper security may be provided by locking the equipment in a cabinet, desk, office, etc. Where such alternatives are not feasible, keeping the device out of sight may be appropriate. Keeping information stored on a portable computing device secure and current is the responsibility of the person who has the device in his/her possession and control. Workforce members with portable computing devices which access, store or transmit ePHI or sensitive business information are responsible for breaches of security related to devices in their control.

Password Protection

Password Protection: All Rewarding HealthyHabits workstations which access ePHI or sensitive business information, are required to have enabled a password protection. Any exceptions must be approved by HIPAA Security Officer in writing. In cases where password protection is not available, alternative security measures approved by HIPAA Security Officer must be deployed. Passwords must meet Rewarding HealthyHabits minimum security specifications as defined in the Password Management policy of the Security Awareness and Training Standard.

Use Clearance

All workstation users including, workforce members, physicians, vendors, volunteers, students, etc. are required to have appropriate clearance including, but not limited to, a background check and role-based necessity prior to being granted access to workstations.

User Termination

Upon termination or change in of job position, users will have network access removed or modified.

Inventory

All computing devices shall be tagged and tracked. Inventory of all workstations shall be maintained and up-to-date.

Training

Rewarding HealthyHabits will train all workforce members on this policy prior to granting access to a workstation. Periodic training on Workstation Use will be included in Rewarding

HealthyHabits's privacy and security training programs.