HCBS Provider
8334986001
1467 Hark A Way Rd
Chester Springs, PA 19425
Generated Date: 12/7/2021

Security Policy Manual

Table of Contents

1 s - Security Risk Assessment Policy ..... **Error! Bookmark not defined.**
101 s - Authorization to Access PHI ..... **Error! Bookmark not defined.**
102 s - Workforce Security Clearance ..... **Error! Bookmark not defined.**
103 s - Workforce Termination ..... **Error! Bookmark not defined.**
104 s - Physical Security Policy ..... **Error! Bookmark not defined.**
105 s - Malware Protection ..... **Error! Bookmark not defined.**
106 s - Login Monitoring ..... **Error! Bookmark not defined.**
108 s - Management of Reported Security or Privacy Events ..... **Error! Bookmark not defined.**
107 s - Password and Logon Management ..... **Error! Bookmark not defined.**
109 s - Business Continuity Data Criticality Backup and Disaster Recovery ..... **Error! Bookmark not defined.**
110 s - Emergency Access ..... **Error! Bookmark not defined.**
111 s - Hardware and Device Management ..... **Error! Bookmark not defined.**
112 s - Automatic Log-off ..... **Error! Bookmark not defined.**
113 s - Workstation Security and Use ..... **Error! Bookmark not defined.**
115 s - Access Controls ..... **Error! Bookmark not defined.**
114 s - Authentication and Unique ID ..... **Error! Bookmark not defined.**
116 s - Emergency Plan Testing and Update ..... **Error! Bookmark not defined.**
117 s - Integrity Controls Including Encryption ..... **Error! Bookmark not defined.**
118 s - Maintenance Records Related to Security ..... **Error! Bookmark not defined.**
123 s - Record Retention and Destruction ..... **Error! Bookmark not defined.**

Security Risk Assessment (SRA) Policy

A. Coverage

Home Community Based Services Provider, Inc, LLC (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on the process of initial and ongoing assessment of the Organization's security risk analysis which will create items for remediation. The stated purpose for this security risk analysis is to reduce the risk level of identified threats and vulnerabilities to an acceptable level, while assisting with HIPAA security and privacy rule compliance.

D. Policy

This policy is intended to provide the basis for assessment of security risks within the Organization and to provide a list of items that need to be addressed through remediation of the identified security risks, in a reasonable and appropriate manner. Note: In this Organization the term 'Security Risk Assessment' may also be interchanged with 'Security Risk Analysis' or 'Gap Assessment'.

Assessment of security risks and compliance with HIPAA Security Rules is an ongoing process, with continued assessment, audit and monitoring as computer networks, software and *'System'* technology is updated or changed. The entire assessment routine should be reviewed and re-assessed yearly to ensure maximum compliance.

The results of our Organization's Security Risk Assessment will be incorporated into our risk management plan (program). Periodic reviews of our Organization's security policies, procedures and technologies will be included within our ongoing risk management and assessment process. This may include vulnerability scans and penetration testing for switches and routers that transmit and receive ePHI (enter "x" for any/all that apply):

Our Security Risk Assessment protocols are intended to complete the requirements contained within 45 CFR 164.308(a)(1). This also meets criteria 15 for the 2012 Stage 1 compliance with incentive payments and as a part of the Meaningful Use program for certified EHRs.

The Security Rule has two types of implementation specifications, 'required' and 'addressable'. The addressable standards have to be implemented, but how they are implemented is more flexible. There are three avenues the Organization can take to comply with an addressable standard. The Organization can decide to implement a specification, implement an alternate equivalent, or not implement it at all. Each organization must determine how to implement these addressable standards according to their size and depth of Information technology expertise. If the decision is

made to implement an alternative or to not implement it at all, it is required to document the reasoning and support why an alternative method or not to implement it at all was chosen. This documentation should be kept, as with all HIPAA documentation, for six (6) years from its creation or last revision date, whichever is later.

It is the policy of this Organization to conduct a regular Security Risk Assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI we create and maintain. Whenever changes to technology or procedures occur there also may be changes to security risks and vulnerabilities. This Organization will reassess and update policies and procedures according to the results of the assessments and may include new/additional employee training if deemed necessary.

E. References

- Stericycle Online Security Risk Assessment tool (SRA)
- 45 CFR §164.308(a)(1), §164.308(a)(8)
- NIST 800-30
- HHS Series 6 Security Risk Analysis
- 2s – Documentation for Security and Privacy Compliance
- 19as – HIPAA Privacy and Security Compliance Program Master Policy
- SRA Items B1, B4, B7, B9, B96, B97, B98, B99, B101, D29
- List Any Additional References: none

Authorization to Access Electronic PHI (ePHI)

F. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential, individually identifiable, electronic protected health information (ePHI).

G. Create / Revision Date

10/21/2024

H. Purpose

The purpose of this policy is to provide guidance in relation to authorization to access electronic PHI (ePHI) and supervision of workforce members given this access.

I. Policy

All Organization workforce members, Business Associates and Contractors must comply with HIPAA regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, as delineated in § 164.308(a)(3). Authorization and supervision of appropriate access, use and disclosure of ePHI assists in reducing overall organizational risk, and reduces HIPAA violations and breaches.

The Organization only permits workforce members who have been appropriately authorized to have access to ePHI. These workforce members must be appropriately supervised. All workforce members shall have access to only to the minimum amount of ePHI/PHI needed to perform their roles. All of these authorizations and supervision will be documented and retained for the minimum six (6) year HIPAA documentation retention period.

J. Related Polices

- 8s -- Minimum Necessary
- 6s -- Appropriate Access to PHI by Workforce
- List Any Additional Related Policies: none

K. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: B39, B41, B42, B43, B44, B62, B68, C2, C9, C11
- 45 CFR § 164.302 - § 164.318, § 164.308(a)(3)
- List Any Additional References: none

Workforce Security Clearance

K. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential protected health information (PHI). Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

L. Create / Revision Date

10/21/2024

M. Purpose

The purpose of this policy is to provide guidance in reference to security background checks and clearance as relates to Information Technology (IT) security.

N. Policy Statement

Screening and assigning specific access controls to IT systems containing electronic PHI (ePHI) within the Organization's workforce can reduce the likelihood of HIPAA violations and breaches by controlling inappropriate access, use and disclosure of ePHI. This Organization provides appropriate levels of access to PHI/ePHI to all members of the workforce. These access levels are based on the nature of each workforce member's duties and responsibilities. Workforce members shall have access to the entire set of PHI/ePHI that they need to do their jobs, but no more access than that. HIPAA Minimum Necessary principals will always apply. No member of the workforce shall have access to a higher level of PHI/ePHI than the level for which they have been approved, including review of their background and clearance from Human Resources.

Human Resources makes use of various levels of background screening to ensure that persons with criminal records or histories of financial or legal difficulties do not have inappropriate access to PHI. Human Resources coordinates with the Security Officer, and legal counsel as appropriate, to ensure background screening requirements are established and complied with. These requirements are fully documented and kept for the retention time mandated by applicable regulations.

O. Related Polices

- 6s - Appropriate Access to PHI by Workforce
- 8s - Minimum Necessary
- List Any Additional Related Policies: none

P. Related Procedures

- List HR Procedures: Home Community Based Services Inc. requires PA Criminal Record Checks, FBI Clearances and Child Abuse Clearances allowing, disabling and deprovisioning workforce access to PHI/ePHI

- List Any Additional Related Procedures: none

Q. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Number: B24, B25, b26, B27, B28, B29, B42, B43
- 45 CFR § 164.302 - § 164.318, § 164.308(a)(3)
- none

Workforce Member Termination of Access Policy

R. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

S. Create / Revision Date

10/21/2024

T. Purpose

The purpose of this policy is to provide guidance on the requirements for removing/terminating access to PHI when employment ends or access is no longer appropriate.

U. Policy Statement

Access to protected health information must be revoked when it is no longer needed. Access to PHI will be eliminated or immediately restricted upon distinct triggering events: (1) when a workforce member's employment is terminated, (2) a workforce member leaves the Organization, (3) there is a change in position such that the workforce member no longer requires access, or (4) upon determination of appropriate mitigation or sanctions against a workforce member. In no case shall the termination of access to PHI be delayed more than the maximum timeframe(s) outlined below. The Organization will document all access termination (deprovisioning) activities, in accordance with our Documentation for Privacy and Security Compliance Policy. Documentation of these activities will be maintained for a minimum of six (6) years.

The timely deprovisioning of a workforce member's access to ePHI is paramount for effective security compliance. The designated Security Officer shall ensure this process is accomplished routinely and in all cases when appropriate. Metrics on average deprovisioning times for common trigger events should be reported to the governance structure for the Organization's compliance program on a routine basis.

Deprovisioning procedures and timelines are documented for different types of termination events (voluntary, delayed, involuntary, instant, etc).

V. Related Procedures

- List Appropriate Procedures: Independent contractors are notified by phone that they will be terminated from Home Community Based Services by HR Director. After the initial contact is made an official termination letter is sent. The HR Director coordinates with Administrative Director to terminate access to all PHI, log in and password are pulled immediately.
- List Any Additional Related Procedures: none

W. Related Polices

- 18s – Audit Controls, Access and Privacy Monitoring
- 19as – HIPAA Privacy and Security Compliance Program Master Policy
- 2s – Documentation for Privacy and Security Compliance
- List Any Additional Related Policies: none

X. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: B24, B27, B31, B32, B33, B34
- 45 CFR §164.302 - §164.318, § 164.308(a)(3)
- List Any Additional References: none

Physical Security Policy

Y. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

Z. Create / Revision Date

10/21/2024

AA. Purpose

The purpose of this policy is to provide guidance related to physical security measures that are undertaken by the organization.

BB. Policy

Stringent physical security policies, procedures and safeguards are a mandatory part of our Organization's comprehensive security strategy. These physical security measures work in tandem with technical and administrative safeguards to protect individually identifiable patient information, including Protected Health Information (PHI). The Security Officer has overall responsibility for physical security compliance and documentation under the HIPAA Security Rule and any other applicable regulations.

Maintenance will be performed as needed for all physical security components listed below, including hardware, walls, doors and locks.

Areas we address and monitor regularly in relation to physical security include:

- Hardware, walls, doors and locks
- Locks and keys for windows and doors and / or electronic access controls
- Physical security ingress and egress access points, including rooftop access
- Drawers, cabinets, files where PHI is stored
- Alarms, video cameras, audio-video surveillance systems and media recording
- Workforce member, vendor and guest access to computing devices that contain PHI
- Paper records (medical, billing, any others that contain PHI or sensitive information)
- Parking lot and vehicle security
- Routine and non-routine deliveries
- Physical devices for prevention of theft, equipment logs
- Telecom, server/ network equipment room; desktop computers, laptops and mobile devices
- List additional items as applicable: none

CC. Related Procedures

- List Appropriate Procedures: none
- List Any Additional Related Procedures: none
-

DD. Related Polices

- 19as – HIPAA Privacy and Security Compliance Program Master Policy
- 2s -- Documentation for Privacy and Security Compliance
- List Any Additional Related Policies: none

EE. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Number: C4, C5, C6, C8, C9, C13, C24
- 45 CFR §164.302 - §164.318, § 164.310(a)(1-2)
- List Any Additional References: none

Malware Protection

FF. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

GG. Create / Revision Date

10/21/2024

HH. Purpose

The purpose of this policy is to provide guidance on methods for protecting the Organization's IT network, software and hardware from internal and external malicious software (malware) that can cause damage to these systems and the data on them. Malware can include viruses, Trojan horses, spyware, root kits and innumerable, ever-changing threats that do harm or cause wrongful disclosure of all types of information, including ePHI.

II. Policy Statement

The Organization's policy is to maintain a rigorous program of security measures and technologies to prevent, detect and mitigate malicious software. The designated Security Officer has responsibility for malware detection, prevention and reporting to ensure that current and appropriate technologies are installed and continuously updated to protect information systems and the individually identifiable information/PHI they contain. It is the policy of this Organization that all software, network computers, laptops and servers (whether they contain PHI or not) shall be protected from malware. Documentation of security procedures for malware protection, detected events (incidents), mitigation and remediation are kept for the minimum six (6) year HIPAA documentation retention period. Vulnerability scans and penetration testing as required by the HIPAA Security Rule may also be documented.

JJ. Related Procedures

- List Related Procedures: none

KK. Related Polices

- 2s – Documentation for Privacy and Security Compliance
- List Any Additional Related Policies: none

LL. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Number: B57, B58, B59, B97, B98, B99, B101, D22

- 45 CFR §164.302 - §164.318
- 45 CFR § 164.308(a)(5)
- List Any Additional References: none

Login Monitoring

A. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to ensure appropriate measures are implemented for verifying access to electronic protected health information (ePHI) and to provide guidance on medical computer Systems monitoring and reporting of log-in discrepancies.

D. Policy Statement

Log-in monitoring is the process of logging or recording all successful and unsuccessful log-in attempts in order to monitor hacking or other inappropriate activity. Log-in monitoring is an element of the Organization's wider-scoped Security and Privacy monitoring. Under the direction of the Security Officer, this Organization maintains a documented process for monitoring log-in attempts to ePHI *Systems* and reporting of log-in discrepancies/related security incidents. Possible violations or breaches of ePHI, along with other potentially inappropriate or illegal activities, shall be immediately reported to the Security/Compliance Officer chain of command. All monitoring procedures for secure login (including time limits for log-in procedure and limitations on the number of unsuccessful log-in attempts); the reporting of discrepancies; and investigations of Security events (incidents) shall be documented and retained for the required regulatory time frame.

List Any Additional Applicable Information: Independent Contractors are assigned clients and are only able to access that client's information on line, by password protection. Email encryption is also implemented anytime PHI is sent to Independent Contractors.

E. Related Procedures

- List Appropriate Procedures: none
- List Any Additional Related Procedures: none

F. Related Polices

- 18s – Audit Controls, Access and Privacy Monitoring
- 2s – Documentation for Privacy and Security Compliance
- List Any Additional Related Policies: none

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Number: B14, B15, B16, B25, B32, B64, B65
- 45 CFR §164.302 - §164.318
- 45 CFR§ 164.308(a)(5)
- List Any Additional References: none

Management of Reported Security or Privacy Events (Incidents)

H. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

I. Create / Revision Date

10/21/2024

J. Purpose

The purpose of this policy is to provide guidance for prompt response, reporting, investigating and documenting of security or privacy events which also may be referred to as 'incidents' or 'suspected violations.'

K. Policy Statement

This Organization will appropriately respond in a timely manner to all privacy and security events, regardless of their severity. Any event, suspected event or discovery of a vulnerability that could pose a threat to the confidentiality, integrity or availability of supporting *Systems*, applications or information is considered an information systems security incident. All security or privacy events which rise to the level of investigation must be documented.

Appropriate responses to reported security incidents include, but are not limited to:

- Timely determination of event type and implementation of process workflow and plan of action by workforce members or department/organizational responsibility
- Prompt assessment on the severity of the threat (vulnerability and risk to PHI or other organizational information) and determination if information can be retrieved/ recovered
- Prompt containment, eradication and recovery which may include preserving evidence, securing affected systems and all related media; repairing, patching or changing related procedures
- Timely investigation of the incident to confirm the root cause and determine if PHI was wrongfully disclosed as a result of the security incident and whether a HIPAA violation or breach has occurred
- Final determination as to whether a HIPAA violation or reportable breach under HIPAA regulations has occurred. (if so, take appropriate action for reporting)
- Providing for security event prevention, through analyses of security events and lessons-learned, subsequent remediation, mitigation and workforce member training
- New Hire and ongoing Security and Privacy Training and awareness programs for workforce members must include security and privacy event/incident reporting

Responsibility for management oversight and a prompt coordinated response to security or privacy events (incidents) resides with the Organization's Security and/or Privacy Officer(s). Specific procedures and responsibilities for incident response and reporting have been established to limit damage, mitigate harmful effects and document security incidents and their outcomes.

All reported information systems security incidents and privacy events will be documented on the appropriate Security or Privacy Event Reporting Form(s) and maintained/archived for a minimum of six (6) years.

L. Related Procedures and Responsibilities

NOTE: Outline specific, applicable procedures for reporting and responding to possible incidents. Address both written and verbal notification of a security incident/event. Outline responsibilities and workflow for remediation, recovery, documentation and archival of the incident/event.

- List Appropriate Procedures: After breach is reported to HR Director, Sharon Halteman, Administrative Director, Jennifer Shaffer or Dina Bray proper written documentation will be sent to the security officer. Appropriate action will be taken immediately in response to the type of violation that occurred.
- List Any Additional Related Procedures: none

F. Related Polices

- 2s– Documentation for Security and Privacy Compliance
- 6s – Appropriate Access to PHI by Workforce
- 25s – Mitigation of Improper use or Disclosure of PHI
- 26s – Sanctions, Enforcement and Discipline
- Bs – Security or Privacy Event Reporting Form (if used by this Organization)
- Cs – Security or Privacy Event Management Form (if used by this Organization)
- List Any Additional Related Policies: none

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Number: B71, B72, B73, B74, B75, B76, B77, E17
- 45 CFR §164.302 - §164.318, § 164.308(a)(6) and at § 164.400 to 164.414
- NIST 800-61 Security Incident Handling
- List Any Additional References: none

Password Management

M. Coverage

Home Community Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

N. Create / Revision Date

10/21/2024

O. Purpose

The purpose of this policy is to provide guidance on issuing and maintaining passwords and logon credentials for the Organization's medical computer *Systems*.

P. Policy Statement

Passwords are an important aspect of computer *Systems* security. Workforce members who access electronic PHI or any confidential organizational information are responsible for taking the appropriate steps to select secure passwords and safeguard their logon credentials. The Security Officer has responsibility to maintain all *Systems* and the Organization's password management procedures for creating, changing, and safeguarding passwords used to verify user identity.

The following standards and description of guidelines shall be followed by workforce members to ensure 'strong' passwords/secure logon management:

Password Construction Guidelines

NOTE: "Strong" Passwords are preferred (passwords that are not easily guessable or obtained by using personal information such as names, pets names, license plates, birthdays)

- To be assigned characters required (6 to 8-digit is recommended min)
- To be assigned alpha characters required
- To be assigned numeric characters required
- To be assigned special characters required
- To be assigned capital characters required
- List Any Additional Requirements: none

Password Management

Passwords and logon credentials should not be written down, stored/maintained on a paper record or left in an easily accessible public area, near any workstation or on any laptop/*System* equipment.

When the Organization's Privacy and/or Security Officer determines that data has been compromised (or there is indication of Password or Information System compromise), workforce member passwords and logon credentials will be changed under the direction of the designated Officer(s).

A workforce member who loses, forgets, or experiences any compromise of his/her password or logon credentials shall immediately notify the Organization's Security/Privacy Officer or a designated alternate in the notification chain of command. These parties will then notify the appropriate Information Systems staff.

Notification of password or logon credential compromise must be made immediately, and in no case is notification to be delayed.

Notification Parameters:

- Contact List: Sharon Halteman, Dina Bray & Jennifer Shaffer
- Minimum Notification Timeline: As soon as compromise is recognized
- List Any Additional Details: none

The Organization shall provide its workforce members with training and awareness on appropriately creating, changing and safeguarding passwords. HIPAA training and security awareness programs will include password management as a topic. All Password Management documentation will be kept in accordance with organizational policy and the minimum HIPAA documentation retention period.

Q. Related Procedures for Password Management

- List Any Appropriate Procedures: Administration will ensure password management
- Password Update Frequency: At minimum every 60 days.
- Password-enabled systems are set for automatic reminders every 60 days (or by department based on risk assessment)
- Passwords should not be written down or stored in the office or near your computer
- "Remember password" features should not be used
- Use of "Admin" or "Administrator" as login for administrator accounts is prohibited
- List Any Additional Related Procedures: none

R. Related Polices

- 6s -- Appropriate Access to PHI by Workforce
- 2s -- Documentation for Security and Privacy Compliance
- List Any Additional Related Policies: none

S. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: B24, B25, B27, B42, B43, D2, D4
- 45 CFR §164.302 - §164.318
- § 164.308(a)(5)
- List Any Additional References: none

Business Continuity, Data Criticality, Back-up, and Disaster Recovery

R. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

S. Create / Revision Date

10/21/2024

T. Purpose

The purpose of this policy is to provide guidance on the Organization's data criticality, back-up, emergency operational preparedness and business continuity measures.

U. Policy Statement

Business Continuity

An overarching business continuity strategy is required on a continuous, daily basis to ensure individuals (the patients we treat) have timely access to their health information.

There are a multitude of threats to the integrity, accessibility and security of the Organization's health information: power issues or outages; fire, flood, other natural or manmade disasters; viruses, hackers and improper disclosures/acts by employees or others. All of these introduce risk into the management of key clinical, financial and operational health information.

Responsibility for planning and establishing a Contingency Operation Plan shall reside with the Security Officer who develops, tests, analyzes and updates the Organization's plans and procedures for business continuity, data criticality, back up and disaster recovery. Global testing of all facets of the Plan and its components should be undertaken on a scheduled basis, ideally, every two months with reporting on the results to the Organization's security compliance/governance executives.

The following conditions can destroy or disrupt the Organization's information Systems:

- Power interruption or outage
- Fire
- Water
- Weather and other natural phenomena, such as earthquakes
- Sabotage and vandalism
- Terrorism
- List Any Additional Conditions: none

This Organization has undertaken IT planning to prevent and mitigate these conditions as a part of an overall security risk analysis. This Organization has named staff responsible for taking preventive

measures to prevent and mitigate the conditions that introduce risk or prevent continued business operations. These measures may include, but are not limited to:

- Listing all systems that contain PHI and/or other data crucial to our Organization's operations
- Maintaining network diagrams and listing of connections between Systems, including interfaces
- Listing primary data controllers and servers
- Appointing a data security coordinator for emergency operations
- Defining which data is the most critical and assigning relative weights to data in order to facilitate its relative importance to back-up, emergency preparedness and business continuity operations
- Providing for redundancy of information, off-site back-up, storage, testing and restoration according to a defined plan
- Creating a support plan with phone numbers for customer and technical support of all key IT/ EHR vendors and prominently displaying the key contact list in a redundant fashion so parties can be promptly contacted in the event of an emergency/evacuation
- Color-coding all media as to priority of physical evacuation: red is first priority; yellow is second priority; green is third priority
- Protecting all servers and other critical equipment from damage in the event of an electrical outage or spikes by using appropriate power conditioning and uninterruptable power supplies
- Routinely ensuring that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly; periodically checking these systems and training employees in their use
- Managing servers, hard-drives and network operations from within a secure environment with appropriate locks and physical security
- Locating file servers and other critical hardware in rooms with fire protection systems that limit damage
- Turning off/unplugging electrical equipment in the event of a flood or if contact with water is imminent
- Sealing room(s) to contain fire or water and/or using strategies to protect information and equipment from fire or rising water
- Training appropriate staff and planning for disaster preparation and recovery
- Covering hardware and software under the Organization's property and casualty, and or other appropriate insurance policy or policies
- Applying routine patches and upgrades regularly, especially those addressing security
- Encrypting back-up data "at rest" according to NIST guidelines
- List additional items as applicable: none

Data Criticality

A thorough assessment of the relative criticality of data and the applications that manage this data is essential to emergency preparedness and business continuity. PHI and other sensitive information must be protected during downtimes and emergency operations. As determined by findings in the data criticality analysis, sequencing to support shutdown and data restoration has been determined with the most critical data and applications given the highest priority in terms of investment and emergency protection preparations.

The Security Officer shall be responsible for conducting data and applications analyses, and shall employ technical guidance and recommendations from bodies such as the NIST (National Institute of Standards and Technology), or others, as deemed reasonable and appropriate. This data criticality analysis shall be documented according to the Documentation for Privacy and Security Compliance policy and will be continually updated to remain current. Emergency preparedness and business continuity planning will constantly reflect the changing nature of the data's criticality.

Critical Data Back-up and Recovery

The storage of data backups in a separate location, removed from our normal business operation is an essential element of any successful data backup plan. This Organization has formalized our backup procedures to ensure data is not lost or corrupted when being securely backed up.

Overview of Backup Methodologies: Off Site Back Up Procedures

Reporting and testing utilities are used to validate the accuracy, completeness, and integrity of data backups. These validations generate daily reports and logs which are kept according to determined timeframes, see Data Retention policy. Any detected errors will be acted upon immediately. Responsible personnel will contact technical support as needed to resolve problems and ensure the validity of backup data on a continual basis. To ensure data integrity, availability, and confidentiality of electronic protected health information, designated personnel are responsible for operating the backup procedures on a pre-determined/regular schedule; testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster. Successful restore functions shall be logged in the appropriate log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Any personnel who detect or suspect a data backup problem should immediately report the same to appropriate responsible party.

Continuity of patient care requires uninterrupted access to patient information, however in a dangerous emergency, evacuating personnel has priority over preserving information assets. To ensure uninterrupted access, this Organization backs-up its data every Daily.

Emergency Operations

Areas to address in the event of an emergency:

- Call 911 and sound appropriate alarms if necessary
- Evacuate if necessary
- If appropriate, engage manual fire extinguishers or fire suppression systems
- Take manufacturer recommended precautions if automated systems engage
- If safe, close all doors as you leave
- Notify other departments and staff of situation and emergency protocols
- Initiate orderly shut-down of computers and networks, if possible
- If a fire or flood is imminent or just starting, disconnect power if possible
- If a fire or flood occurs, try to prevent further damage from water by covering areas with plastic and ensure adequate ventilation and drainage
- Move records/equipment/storage media away from area being flooded; Organize and label health information logically and clearly for continued access
- Invoke business continuity procedures and downtime processes as appropriate
- List other, appropriate specific emergency operations items: none

Downtime Operations

- List procedures and operations to be used in the event of computerized record downtime: manual entry of data once operations are back up a running
- List procedures to be used if the normal paper record operations are compromised by a business continuity interruption: halting procedures until normal operation can be resumed

Disaster Recovery Operations

The Organization's business continuity program calls for the implementation of the following disaster recovery steps, as appropriate (after the emergency has passed).

All workforce members should:

- Prevent personnel from entering the area until officials have determined that the area is safe to reenter
- Assess the extent of the damage and whether additional equipment and/or supplies are needed
- Determine how long it will be before service can be restored, and notify departments
- Replace hardware, software, infrastructure, i.e. wiring as necessary to restore service
- Notify insurance carriers
- Restore and test backup files
- Remove water-damaged paper records by the wettest first; Freeze wet items to stabilize documents; Wrap wet records to prevent them from sticking together
- Get and use advice from appropriate paper restoration vendors
- Set up IT operations at an alternate site(s) if necessary
- Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed
- Determine how and where paper and electronic records will be used until normal operations are resumed
- Keep administration, medical staff, HIM, IT personnel, and others informed of the status of the downtime or emergency mode operations
- List other, appropriate specific emergency operations items: none

Preventive Measures

This Organization has established and implemented needed policies and procedures for preventing and responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that could cause damage to *Systems* that contain electronic protected health information.

V. Related Plans and Procedures

- Preventive measures for fire, theft, vandalism, system failure, natural disasters, others as needed and addressed within this Organization's Contingency Plan: off site daily back up that is secured
- Emergency operations procedures: address emergency and continue with normal operations
- Disaster recovery procedures: back up from offsite company
- Business continuity procedures: operated or halt business procedures as to not compromise PHI
- Data backup procedures: daily offsite back up
- Data Criticality Analysis and Management Tools illustrating the relative Weights of Importance of each set of data and their supporting applications: review during quality management procedures

W. Related Polices:

- 6s - Appropriate Access to PHI by Workforce

- 2s - Documentation for Security and Privacy Compliance
- Record and Data Retention (for General Records)
- List Any Additional Related Policies: none

X. References

- Stericycle Security Risk Assessment (SRA)
- SRA Item Number: B2, B3, B5, B6, B58, B80, B81, B82, B83, B84, B85, B86, B87, B88, B89, B90, B91, B92, B93, B94, C3
- 44 C.F. R. §164.302 - §164.318, § 164.308(a)(7), § 164.308(a)(8), § 164.310(a)(1-2)
- NIST 800-111 -- Guide to Storage Encryption Technologies for End User Devices
- DEPARTMENT OF HEALTH ANDHUMAN SERVICES 45 CFR Parts 160 and 164 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act.
- List Any Additional References: none

Emergency Access

A. Coverage

Home Community Based Services, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on gaining emergency access to critical EHR (electronic health record) *Systems* and other computers/systems which contain necessary electronic protected health information and/or operational data needed during an emergency situation.

D. Policy Statement

Access controls are necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. Emergency access procedures for obtaining access to the Organization's EHR and other critical *Systems* have been created to maintain security protections for electronic Protected Health Information (ePHI/PHI). The Security Officer has ultimate authority over the creation, maintenance, testing, updating and documentation of these procedures. These procedures have been developed to ensure that authorized workforce members can access necessary health information in emergency situations.

All emergency access will be logged with the user information and reason for the emergency access. Audit controls will be reviewed by appropriate compliance governance on a routine basis. Emergency access procedures are closely related to those for disaster planning and emergency response.

E. Related Procedure

- Insert appropriate emergency access procedures: direct communication with administration team and independent contractors once emergency is identified
- Insert appropriate emergency access review procedures: will be reviewed during quality management review:

F. Related Polices:

- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- 116s - Emergency Plan Testing and Update
- 109s - Business Continuity, Data Criticality, Back-up, Disaster Recovery List additional related policy

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: B39, B42, B43, B85, C2, C3, D8
- 45 CFR §164.302 - §164.318, § 164.104, §164.306, §164.312(a)(1), §164.312(a)(2)(ii)
- List Additional References: none

Hardware, Digital Media and Mobile Device Management

A. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information contained on computers and digital/mobile devices. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on the management of this Organization's hardware, digital media and mobile devices to prevent wrongful access, use or disclosure of electronic PHI (ePHI) or otherwise sensitive information/data contained on these devices. This policy also addresses the use of personal devices used to access PHI or sensitive organizational data.

D. Policy

Management of computer hardware, digital media and digital mobile devices (including but not limited to cell phones, smart phones, tablets and flash drives) present unique challenges and risks to the security and privacy of confidential health information. These risks can be minimized by establishing appropriate controls and implementing the necessary measures for optimal protections. This Organization's policies and procedures are to be clearly communicated and enforced for all workforce members to establish expectations and convey accountability.

Definitions and guidelines on personal and Organization-issued mobile devices and their use as relates to the capture, storage, access, use and disclosure of this Organization's electronic data and PHI have been developed and implemented.

This Organization shall track all details (to the extent reasonably possible) about the location of hardware, digital media and mobile devices that contain PHI or other sensitive information throughout their entire life-cycle (from procurement through final disposition). A catalog (Inventory Lists) of IT hardware, software, network diagrams and interfaces are all part of the management plan for IT devices. The tracking of these devices is a task that must be updated constantly with documentation kept for the required timeframe. Specific procedures for such tracking have been developed and implemented. The Organization also maintains an incident response plan to guide the management of loss, theft or any potential or real compromise of the security of our hardware, mobile devices and data. Responsibility for maintaining this plan, documenting and managing the processes surrounding it lies with the Security Officer or their designee.

Hardware and more portable and re-useable digital recording and storage media containing

individually identifiable health information, including PHI (Protected Health Information) or other sensitive information must be properly erased, encrypted, or completely destroyed at the end of its lifecycle. Re-use of media is not allowed unless appropriate erasure and device updating is applied. This organization will dispose of all media PHI in compliance with the requirements of the HIPAA Security Rule and other applicable regulations.

Encryption and decryption of data in digital devices (including, but not limited to those that are portable or re-useable) shall be undertaken in compliance with the Organization's strategic IT plan. Data encryption should be managed according to HIPAA Security and NIST compliance regulations to prevent wrongful access, use and disclosure of PHI and other types of sensitive information. HIPAA Privacy Rule breach safe harbor will be established by the use of compliant encryption and decryption for as many of the data sets within this organization as possible. It is anticipated that the amount of encryption will increase over time as the different states of data (i.e., in motion, at rest and in use) are addressed.

All hardware, digital media and mobile devices will have their data erased in compliance with HIPAA regulations prior to transfer of ownership (sale, donation or trade) or disposal of the devices, including, but not limited to: copiers, medical devices, computers, phones, flash drives, etc. Media will be erased before re-use by another user.

All devices will be supported by designated support staff, be up-to-date with the latest approved version and all security / bug type patches (among others). Dedicated employees will be assigned to specific devices and tracked as users of those devices to facilitate reporting as needed.

Responsibility for the procedures facilitating proper hardware, digital media and mobile device tracking and management resides with the Security Officer. Hardware, digital media and mobile device encryption, erasing and other disposal-related activities will be documented in compliance with the Organization's Documentation for Security and Privacy Compliance policy and procedures.

Workforce members and other users of PHI and sensitive information shall be given appropriate security awareness training, including, but not limited to specifics on the use of mobile devices. Confidentiality and "Rules of Use" agreements will be signed and maintained for all users as policy dictates.

All documentation related to these policies will be maintained for the required 6-year HIPAA document retention timeframe.

E. Policy Discussion

The following items are detailed within this policy in order to facilitate Strategic IT planning and development of appropriate security- and privacy-related procedures. These items are drawn from and implemented according to the Organization's Strategic IT Plan, security risk assessments or similar works. This Organization will, as deemed reasonable and acceptable, implement the following or similar technologies and processes.

1. This Organization routinely reviews policy decisions as the technology marketplace changes
2. This Organization has a documented set of rules governing the acceptable use of mobile devices, including the 'Conditions of Use' by all workforce members as well as, Business Associates, contractors, temporary employees, students or anyone that may come in contact with PHI or sensitive Organization information. Personal device use is covered within these documented rules as well
3. All users are required to sign a copy of a confidentiality statement including guidelines for personal / mobile devices prior to being allowed to use a device; This Agreement holds the

employee accountable for the device and its data and protection of said data.
4. Use of the assigned mobile device is restricted solely to the designated employee
5. This Organization identifies and defines usage guidelines for PHI and sensitive information on Organization-issued hardware and devices
6. We employ appropriate technologies and techniques for the destruction of PHI and sensitive information at appropriate points in the lifecycle of the hardware or device
7. Organizational definitions, roles and responsibilities for accessing and managing corporate resources such as email, calendars, distribution and contact lists are documented
8. All workforce members, Business Associates, Contractors, et al., shall be educated and familiar with this Organization's policies and procedures regarding the use and management of all devices that contain PHI or sensitive information; information on how to respond to the loss or theft of computer hardware, mobile devices or their information is covered in training
9. This Organization maintains a current list of Organization-owned mobile device users with the assigned equipment's serial number, and software applications
10. This Organization's PHI and sensitive information should not be stored on mobile personal devices. Information is more secure when stored on the Organization's network where PHI is routinely backed up and subject to business continuity processes; If network storage is not possible, information should be encrypted to protect it from unauthorized access should the device be lost or stolen
11. This Organization routinely checks for and applies operating system, firmware updates, software application patches and updates
12. Antivirus, Malware, Firewalls, Filters and other similar technical safeguards are kept up to date and routinely maintained
13. Password protection guidelines should be followed according to the Unique User ID policy and procedure
14. We incorporate appropriate encryption for each device in use, as reasonable and according to this Organization's strategic IT plan
15. In addition to routine tracking and management of all hardware, mobile devices and the data they contain, this Organization performs audits to ensure policies, procedures, tracking and management of hardware, devices and mobile devices are continually monitored and updated
16. Hardware encryption solutions for mobile devices such as laptop computers is preferred and will be implemented as deemed reasonable within the strategic IT plan. This Organization will determine if mobile devices proposed for use can support encryption and, in cases where encryption is not available, evaluate the risks of using the device. The Organization will ensure encryption products have a central key management infrastructure to enable the recovery of lost or forgotten encryption keys. This Organization evaluates hardware and mobile devices in reference to the availability of encryption to prevent wrongful access, use and disclosures and to place the data within the breach safe harbor. We will opt for devices that provide hardware-based encryption which does not require administrative rights on the host computer in order to operate, if reasonable and appropriate, on a case by case basis.
17. Physical security and technology will be utilized by this Organization to prevent or recover from theft, loss, damage to PHI or sensitive information contained within hardware or mobile devices
18. This Organization will centralize the oversight, documentation and tracking of media destruction and reallocation where reasonable and appropriate
19. Workstation access is restricted to organizationally-approved devices only; This includes personal devices
20. This Organization will routinely audit for appropriate access and use of all hardware and devices
21. To the extent reasonable and appropriate, this organization will restrict the use of CD/DVD burners / writers; encryptable CD/DVD media is encouraged in areas that have a legitimate need

22. The Security Officer or their designee has evaluated the use of USB mass storage devices (i.e. flash or jump drives) and determined the most reasonable and appropriate ways to secure these devices
23. Local repair facilities are preferred for hardware and mobile devices to avoid potential theft or loss during shipment to or from the factory when devices are sent for repair or replacement. Local facilities should be bound by Business Associate Agreements as reasonably appropriate. If hardware or mobile device repair is needed off-site consider, if possible, removing the hard drive prior to sending the device outside the Organization. If the hardware or device is being returned as part of an equipment exchange or trade-in, be sure all data is completely erased and destroyed in accordance with HIPAA and NIST standards. Dispose of the hard drive using an acceptable destruction method such as a NIST-approved secure overwrite method, magnetic degaussing, or physical destruction of the hard drive. Return devices through a delivery service that will properly record the signature of the receiving party and will not leave the parcel unattended.
24. Security awareness training should include: avoidance of using mobile devices where events or human error can occur result in their loss or theft; mobile devices should never be left in a visible location inside a vehicle; if a device is stolen during travel, report to local police and complete an investigation report immediately; any lost or stolen device must immediately be reported to this Organization's Security Officer or their designee

Mobile Device Security Tips from HHS

In their December 2012 guidance titled "Your Mobile Device and Health Information Privacy and Security," HHS provides the following tips which our Organization recognizes and follows:

- Install and enable encryption to protect health information stored or sent by mobile devices
- Use a password or other authentication
- Install and activate wiping and/or remote disabling to erase the data on your mobile device if stolen
- Disable and do not install or use file sharing applications
- Install and enable a firewall to block unauthorized access
- Install and enable security software to protect against malicious applications, viruses, spyware and malware based attacks
- Keep your security software up to date
- Research mobile apps before downloading
- Maintain physical control of your mobile device—Know where it is at all times to limit the risk of unauthorized use
- Use adequate security to send or receive health information over public Wi-Fi networks
- Delete all stored health information on your mobile device before discarding it
- Provide mobile device privacy and security awareness training

F. Related Procedure

- List specific procedures for hardware tracking: all hardware is owned by independent contractors and administration team
- List specific procedures for mobile, re-useable or portable device tracking: all mobile devices are owned by independent contractors and administration team
- List specific procedures for hardware, network, software application and portable or re-useable

device Virtru is used to encrypt emails, all mobile device communication is secondary verification password protection:

- List specific procedures for media destruction: company owed device hard drives will be destroyed by a certified PHI destruction company and certificate will be presented upon destruction. All independent contractor devices will be asked for a sign off that documents the destruction of PHI after no longer in use
- List specific procedures for media re-use: IT director will make sure any media re-use is compliant

- List specific security awareness education and training for hardware, mobile devices, data, including personal use: will be included in the company's once year required training
- List specific procedures for Device and Data Ownership, including mobile / personal device Conditions of Use and written authorization for Mobile / Personal Device Use: documentation of sign off for use of personal devices, mobile and PC
- List the USB Mass Storage procedure: all devices will require password access
- List additional related procedures: none:

G. Related Polices

- 2s - Documentation for Security and Privacy Compliance
- 6s - Appropriate Access to PHI by Workforce
- 105s - Malware Protection
- 108s - Security Incident Management
- 114s - Authentication and Unique ID
- Strategic IT Plan
- Conditions of Use Agreement for Mobile / Personal Devices
  List additional related policy or related documents on strategic IT plan or Conditions of Use Agreement for Mobile / Personal Devices: none

H. References

- Stericycle Online Security Risk Assessment (SRA)
  - SRA Item Numbers: B2, B3, B5, B6, B8, B58, B61, C17, C25, C26, C27, C28, C29, C31, C32, D30
- 45 CFR §164.302 - §164.318; § 164.310(d)(1-2), § 164.312(a)(1-2)
- AHIMA April 2012 Practice Brief 'Mobile Device Security (Updated)
- HHS Guidance: *Your Mobile Device and Health Information Privacy and Security:*

http://www.healthit.gov/providers-professionals/your-mobile-device-and-health- information-privacy-and-security

Automatic Log-off

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose, or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on the use of automatic log-off features within this Organization's IT systems.

D. Policy Statement

Usage of automatic log-off for any computer system containing PHI or other sensitive information is a crucial part of this Organization's security program. All computer systems in use within this Organization must utilize automatic log-off procedures that terminate an electronic session after a predetermined time of inactivity.

Settings and automatic timings shall be as uniform as possible across the organization and its various IT *Systems*. Workstation log-off or automatic workstation lockout, especially in patient /public facing areas, should occur within list maximum duration of inactivity prior to session termination.

Responsibility for the development and implementation of automatic log-off policies and procedures reside with the Security Officer. All automatic log-off procedures shall be documented in accordance with the Documentation for Security and Privacy Compliance policy.

E. Related Procedure

List specific log-off procedures, timings and settings, requests for exceptions to the timing requirement: automatic log off after 1 minute of not being used

F. Related Polices:

- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- List additional related policies: none

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: C16, D9, D11
- 45 CFR §164.302 - §164.318§ 164.306 and § 164.312(a)(1-2)
- List additional references: none

Workstation Security and Use

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on the security and use of the computer workstations within this Organization.

D. Policy Statement

This Organization's policy and procedure combined with workforce training about security and the use of computer workstations is a crucial element in our IT security program. Adherence to workstation security procedures is vital in maintaining the confidentiality of all PHI (Protected Health Information) and sensitive information within this Organization.

Responsibility for the development and implementation of the Workstation Security and Use policy and procedures resides with the Security Officer. All documentation for Security and Privacy compliance is maintained in accordance with HIPAA and other related regulations. Workstation Security includes physical safeguards and practices to restrict access to authorized users only. Procedures implementing physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) have been documented.

Security reminders along with HIPAA Security Awareness training (for new hires and at routine points in workforce members' tenure) will continually reinforce concepts and practices for workstation security. The Confidentiality and Security Agreement signed by workforce members makes every individual responsible for maintaining the security of workstation(s) and the privacy of data accessible through them.

Workstation use is logged and tracked via a number of different monitors. Inappropriate use of any kind (i.e., visiting unauthorized sites, personal web surfing and similar is not allowed). Inappropriate use of Organizational computer workstations will be managed through the use of sanctions as outlined within the Sanctions, Enforcement and Discipline Policy.

This Organization shall track all details about and the location of workstations that contain PHI or other sensitive information throughout their entire life-cycle from procurement through final disposition. The party responsible for this tracking is the Security Officer or their designee.

Workstation hardware and software encryption, erasing and other disposal related activities will be documented in compliance with the Organization's Documentation for Security and Privacy Compliance policy and procedures.

1. This Organization routinely reviews workstation policy decisions as the technology marketplace changes
2. This Organization has a documented set of rules governing the acceptable use of workstations, including the Conditions of Use by all workforce members, Business Associates, contractors, temporary employees, students or anyone that may come in contact with PHI or sensitive Organization information
3. All users are required to sign a copy of a confidentiality statement including guidelines for workstation use
4. Use of an assigned mobile device or workstation is restricted solely to the designated employee
5. This Organization identifies and defines both PHI and sensitive information on Organization workstations
6. We employ appropriate technologies and techniques for the destruction of end-of-lifecycle workstations that contain PHI and sensitive data
7. All workforce members, Business Associates, Contractors, et al., shall be educated and familiar with this Organization's policies and procedures regarding the use of all devices that contain PHI or sensitive information
8. This Organization routinely checks workstations and applies operating system, firmware updates, software application patches and updates
9. Antivirus, Malware, Firewalls, Filters and other similar technical safeguards are kept up to date and routinely maintained
10. Password protection guidelines should be followed according to the Unique User ID policy and procedure
11. All workstation will have data erased in compliance with HIPAA regulations prior to transfer of ownership (sale, donation or trade) or disposal
12. We incorporate appropriate hardware or software encryption for each workstation in use, as reasonable and according to this organization's strategic IT plan
13. Physical security and technology will be utilized by this Organization to prevent or recover from theft, loss, damage to PHI or sensitive information contained within hardware or workstations.
14. This Organization will routinely audit for appropriate access and compliant use of a significant number of workstations
15. To the extent reasonable and appropriate, this organization will restrict the use of CD/DVD burners / writers; Encryptable CD/DVD media is encouraged in areas having a legitimate need

E. Related Procedures

- List workstation security procedures: password protection
- List workstation access and use procedures: password protection

F. Related Polices:

- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- 111s - Hardware & Device Management
- Vs - Confidentiality and Security Agreement
- List additional related polices: none

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: C6, C7, C8, C9, C15, C16, C18, C21, C23
- 45 CFR §164.302 - §164.318§ 164.310(b), § 164.310(c)
- List additional references: none

Access Controls

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on access controls and role-based protections to maintain the security of this organization's PHI and sensitive information.

Access control and validation procedures are designed to control and validate individual access to this organization's PHI (Protected Health Information). Access controls are addressed with many techniques from physical security (i.e., locks and workstation placement) to software based solutions for user identification. These controls are often based upon an individual's role or function and may include visitor control, when and where visitors are allowed.

Individuals involved in the Organization's software testing and version are also subject to appropriate access controls. These individuals may be members of this Organization's workforce, a Business Associate or Contractor. These controls ensure the processes of software testing and version upgrades will be maintained with maximum integrity.

Responsibility for developing, testing, analyzing, periodically updating and monitoring information access control and validation procedures resides with this Organization's Security Officer or their designee. Development and implementation of specific information access control and validation procedures shall be conducted in accordance with guidance and information provided by the HIPAA Security Rule, the National Institute of Standards and Technology (NIST), and other standards applicable to security compliance within this Organization. Access controls are to be evaluated for strengths and weaknesses as a part of any security reviews.

Workforce members are to be regularly trained on authentication (i.e. logon) methodologies and requirements.

All access controls, including visitor controls, are fully logged, tracked and documented in accordance with the Documentation for Security and Privacy Compliance policy and any other appropriate, related best practices.

D. Related Procedures

- List access to information controls procedures: Two person control over log in assignment and password control. Monthly reports to be reviewed.

- List visitor access controls: no access given to visitors or under special circumstances they will be assigned a specific log in ID
- List procedures for access control monitoring, logging and reporting: Monthly log in reports to be reviewed
- Workforce access to authentication (i.e. Log-on methods and requirements): secondary verification procedure upon log in or receipt of email

E. Related Polices and Documents:

- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- 34s – Training Workforce HIPAA
- Vs - Confidentiality and Security Agreement
- Organization's Security Plan (with visitor access controls)
- List additional related polices: none

F. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: C2, D2, D3, D4, D5, D6, D24, D25
- 45 CFR §164.302 - §164.318, §164.310(a)(1-2)
- List additional references: none

User Authentication and Unique User ID

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on user authentication and the Organization's procedures to verify that a person or entity seeking to access PHI is the one claimed.

D. Policy Statement

Unique user IDs for secure logon to all computers and digital devices is required by this Organization in compliance with HIPAA Security rules and to maintain the privacy of PHI and other sensitive information. These unique IDs serve to authenticate a user's identity and to deny imposter access. Each user must always be individually identified (authenticated) by their logon credentials in order to accurately account for and track acceptable and wrongful access, use and disclosure of PHI or sensitive information.

Responsibility for the development and implementation of the User Authentication and Unique User ID policy resides with the Security Officer or their designee.

All workforce members and any other party acceptably accessing the Organization's PHI through the use of computers or digital devices shall be given appropriate security awareness training on proper person or entity authentication practices and the sanctions for misuse of logon credentials.

Nothing in this policy shall limit the use of additional security measures (including multi-factor techniques, biometrics, tokens, proximity detection, etc.) to further enhance logon and access security protections this Organization provides to PHI and sensitive information. A unique user ID (username and password) is the most common, but not necessarily the most secure method of assuring authentication. However, it is a key IT security component and is a part of this Organization's comprehensive user identity management program(s). Each logon will trigger audit logging and similar events that record successful and unsuccessful attempts to access data. Failed logon attempts will be tracked for inappropriate access.

Determinations will be made by the Security Officer and IT staff as to which logs and metadata on logons and attempts will be kept and for what period of time. A robust set of documentation will be retained as a part of the Organizational Documentation for Privacy and Security Compliance policy.

Conditions of use for logon credentials and secure password management are addressed in the

Confidentiality and Security Agreement. All workforce members, Business Associates, Contractors or other parties that have lawful access to PHI and other sensitive information using this Organization's computers and digital devices must sign a Confidentiality and Security Agreement prior to being issued passwords and logon credentials. Sanctions will be applied for violations to this Agreement.

E. Related Procedures

- List authentication and password management procedures: To be assigned and updated by Heather Bass Phil

F. Related Polices:

- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- Vs - Confidentiality and Security Agreement
- List additional related polices: none

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: B42, B43, B66, B67, B68, D4, D5
- 45 CFR §164.302 - §164.318§ 164.306, and § 164.312(a)(1), § 164.312(d)
- List additional references: none

Emergency Plan Testing and Updates

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance in reference to the testing and updates of emergency and contingency operations plans.

D. Policy Statement

This Organization will periodically test, and revise as necessary, all emergency preparedness plans, including emergency and contingency plans. These emergency and contingency operations plans are related to and may be implemented with the business continuity plan. Such emergency and contingency plans are the responsibility of the designated Security Officer, Privacy Officer and other designated staff who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements. All emergency and contingency plans shall be reviewed, and revised if necessary, at least annually (specify different time period if applicable). Testing of the emergency plan is a continual and evolutionary process where issues are identified and mitigated with updates on an on-going basis.

Copies of all emergency and contingency plans shall remain on file and be available to all personnel.

All emergency and contingency plans shall be rehearsed, with all team members participating in such rehearsals, at least twice annually (specify different time period if applicable). These rehearsals shall be planned with business continuity procedures as well. Business continuity, data backup, restoration and emergency IT operations are all key components of the contingency and emergency operations plans.

Protections for PHI and sensitive information will remain in effect during the execution of any emergency or contingency plan. During contingency and emergency operations, workforce members will work to protect the organization's assets, both physical and informational.

Business continuity, emergency and contingency plans, and all the revisions thereof shall be documented in accordance with our Documentation of Privacy and Security Compliance among other policies.

E. Related Procedures

- List specific IT security related procedures for updates to business continuity, contingency and emergency plans: monthly review by quality management team
- List documentation and information access procedures within the execution of business continuity, emergency and / or contingency plans: monthly review by quality management team

F. Related Polices:

- 6s -- Appropriate Access to PHI by Workforce
- 2s -- Documentation for Security and Privacy Compliance
- 115s -- Access Control
- 109s -- Business Continuity, Data Criticality, Back-up, Disaster Recovery
- List additional related polices: none

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: B91, B92, B93
- 45 CFR §164.302 - §164.318. § 164.308(a)(7)
- List additional references: none

Integrity Controls Including Encryption and Decryption

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information contained on computers and digital/mobile devices. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on how this organization prevents PHI or other sensitive information from being altered or destroyed in an unauthorized manner.

D. Policy Statement

The establishment and implementation of effective data integrity controls is a crucial element in this Organization's overall security compliance plan. It is the policy of this Organization to provide data integrity controls and protection procedures in full compliance with all the requirements of HIPAA and other governing regulations.

Responsibility for the development and implementation of these data integrity controls resides with Security / Privacy Officer who ensures that these procedures are maintained, updated as necessary, and implemented fully across this Organization.

Integrity control refers to the safeguards utilized by this Organization to prevent unauthorized documentation, changes, updates, fallacious code or destruction of patient information, PHI or other sensitive business information. The integrity of data can be compromised by both technical and non-technical sources (i.e., identity theft, malicious or accidental incidents, electronic media errors or failures). Integrity control procedures have be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access PHI and other sensitive information.

It is the Policy of this Organization to fully document all data integrity controls-related procedures, activities, and efforts, in accordance with our Documentation of Security and Compliance Policy. Many of the policies guiding this Organization have been created to protect data integrity (Access Controls, User Authentication, etc.).

Encryption and decryption of data is a key element in the maintenance of data integrity. According to NIST and the HIPAA Security Rule, data exists in 4 states: data in motion, data in use, data at rest and data destroyed. Encryption and decryption are important for data when it is being used, moving and at rest. There are a huge number of variations of encryption and decryption, some of which are listed in NISTN 800-111 and Federal Register (see References). In general, wherever this

Organization follows these guidelines and applies appropriate encryption and decryption, our PHI and sensitive information is protected from breach, being deemed in the HIPAA - created Breach Safe Harbor. Whenever and wherever reasonable and appropriate, this Organization's strategic IT objectives include an ever-increasing movement towards Safe Harbor and other applicable encryption and decryption technologies being utilized.

E. Related Procedures

- Insert strategies for protection of data integrity: monthly reports from third party company that provides server security and back up

F. Related Polices:

- 6s -- Appropriate Access to PHI by Workforce
- 2s -- Documentation for Security and Privacy Compliance
- Clinical Documentation
- Registration and Proper Patient identification (Red Flag)
- Health Information (Data) Exchange
- 115s -- Access Controls
- 114s -- Authentication and Unique User ID
- 40s -- Photo, Video and Non-text Management
- 104s -- Physical Security
- 113s - Workstation Security and Use
- List additional related polices: none

G. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Item Numbers: B62, B82, B97, B98, B99, B111, D12, D13, D14, d15, D22, D27, D28, D30, D31, D32, D33
- 45 CFR §164.302 - §164.318, § 164.312(c)(1-2), § 164.312(e)(1-2), §164.312(a)(1-2)
- Federal Register April 27, 2009: DEPARTMENT OF HEALTH AND HUMAN SERVICES 45 CFR Parts 160 and 164 "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act.
- NIST 800-111 Guide to Storage Encryption Technologies for End Users
- List additional references: none

Maintenance Records Related to Security

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members who access, use, disclose or transmit confidential patient information contained on computers and digital/mobile devices. Our workforce includes all clinical providers, clinical support staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

10/21/2024

C. Purpose

The purpose of this policy is to provide guidance on the creation and management of maintenance records related to changes, upgrades or other physical security areas within our Organization.

D. Policy Statement

This Organization maintains facility security maintenance records in compliance with the requirements of HIPAA and other regulations. Facility security maintenance records are created to document repairs and changes to physical infrastructure assets of our Organization as relates to security as detailed in our Facility Security Plan. The responsibility for the creation and updating of facility maintenance records is assigned to insert responsible party. Facility security maintenance records will be maintained in compliance with our Documentation for Security and Privacy Compliance policy.

E. Related Procedures

- List maintenance record related to security management procedures: year maintenance of records by security officer

F. Related Polices:

- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- Facility Security Plan
- List additional related polices: none

G. References

- Stericycle Security Risk Assessment (SRA)
- SRA Item Numbers: B58, B61, C13, F4
- 45 CFR §164.302 - §164.318, § 164.310(a)(1-2)
- List additional references: none

Record Retention Destruction

A. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members who access, use and manage Protected Health Information (PHI), either in the electronic or paper format.

B. Reviewed/Revised

10/21/2024

C. Purpose

This Policy provides detail on procedures regarding patient and other sensitive information retention and destruction, documentation and schedules to be utilized for all records managed by Insert Name of Department, Record Custodian or Other Party, including the Legal Health Record (LHR) that is maintained for evidentiary purposes as one of our business records, in order to insure compliance with all applicable statutes, rules and regulations.

D. Policy

The Organization maintains company and client information in various formats/systems as listed in the attached schedule. At all times; the Organization will keep these retention schedules compliant with applicable standards, including Federal Rules of Civil Procedure, State Law, HIPAA, JCAHO, CMS (Medicare) and other applicable statutes, rules and regulations.

After careful consideration of the needs for information management for our Organization and to maintain compliance, a retention schedule has been determined and outlined.

Destruction of this Organization's stored information is only accomplished in approved manners by certified vendors that utilize appropriate HIPAA certifications, for both electronic and paper copies, as well as PHI as it appears in any form prior to leaving control of the Covered Entity, Business Associate or Sub-contractor; but also in general, for any sensitive company or client information.

When medical records have aged to the point of destruction, they will be destroyed by vendors or software applications that can provide the following types of functionalities:

- If destruction services are contracted, the contract must meet the requirements of HIPAA Privacy and Security Rules.
- Records must be destroyed so there is no possibility of reconstruction of the information.
- Use of secure, multi-pass (or similar) electronic record destruction techniques to ensure all traces of the data are removed and / or destroyed.
- Document the destruction with approved data elements and format including (as applicable, depending on whether electronic or paper data is being destroyed):
    - Date of destruction
    - Method of destruction

- Time that will elapse between acquisition and destruction of data
- Description of the disposed records
- Inclusive dates covered
- A statement that the records were destroyed in the normal course of business
- Signature(s) of the individuals supervising and witnessing the destruction
- Maintain destruction documents permanently. (Such certificates may be required as evidence to show records were destroyed in the regular course of business).
- Shredding or otherwise destroying PHI in paper records (or on other media, such as specimen containers) so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster or other trash receptacle.
- Maintaining PHI for disposal in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- In justifiable cases, based on the size and the type of the covered entity, and the nature of the PHI, depositing PHI in locked dumpsters that are accessible only by authorized persons, such as appropriate refuse workers.
- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

E. Procedures

List procedures utilized for destruction of PHI: destruction by certified third party company that will provide documentation

F. References

- AHIMA Body of Knowledge “Destruction of Patient Health Information (Updated)” 2002
- AHIMA Issues in Electronic Health Records Management “Purge and Destruction” 2004
- HIPAA Security Rule 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii)
- Breach Interim Final Rule
- 45 CFR Parts 160 and 164 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information
  - 45 CFR 164.530(c)
  - 45 CFR 164.310(d)(2)(i)
- HHS HIPAA Security Series 3: Security Standards – Physical Safeguards
- NIST SP 800-88, Guidelines for Media Sanitization

