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

Privacy Policy Manual

Table of Contents

Privacy Risk Assessment (PRA)

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

11/28/2021

C. Purpose

The purpose of this policy is to provide guidance on the process of an initial then ongoing assessment of the Organization's privacy risk analysis which will create items for remediation. The stated purpose for this regular privacy risk analysis is to reduce the risk of privacy events, incidents or breaches to an acceptable level, while assisting with the Organization's overarching HIPAA security and privacy rule compliance program.

D. Policy Statement

This policy is intended to provide the basis for assessment of privacy risks within the Organization and to provide a list of items that need to be addressed through remediation of the identified privacy risks, in a reasonable and appropriate manner. Note: In this Organization, the term 'Privacy Risk Assessment' may also be interchanged with 'Privacy Risk Analysis' or 'Privacy Gap Assessment'. Assessment of privacy risks and compliance with HIPAA Privacy and Security Rules is a continual process, with repeated assessments as computer networks and systems change or workflow processes are updated. The entire Privacy Risk Assessment should be reviewed and re-assessed yearly to ensure maximum compliance.

The results of our Organization's Privacy 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.

Our Privacy Risk Assessment is intended to meet the requirements contained within HIPAA, from both privacy and security perspectives; and, for evaluating items to be remediated and managed. Performing a Privacy Risk Assessment is more of a general requirement than the more regulated Security Risk Analysis which is called for within the HIPAA Security Rule as well as the Meaningful Use program. Privacy Risk Assessments are emphasized as crucial to successful compliance programs; therefore, this Organization considers our Privacy Risk Assessment to be as important as Security Risk Assessments.

All privacy risk assessment activities shall be documented and kept, as with all other 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 Privacy Risk Assessment of the potential

risks and vulnerabilities to the confidentiality, integrity, and availability of the PHI we create and maintain. Whenever changes to technology or procedures occur, there may be changes to privacy and 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 Privacy and Security Risk Assessment tools (PRA & 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
- List additional references: none

Documentation for Security and Privacy Compliance

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

11/28/2021

C. Purpose

The purpose of this policy is to provide guidance on development, management and maintenance of documentation related to HIPAA requests, complaints, investigations and ongoing compliance activities.

D. Policy Statement

This policy is intended to govern the creation, use, and maintenance of documentation (documents) related to HIPAA compliance. Workforce members must document in writing (or in electronic format) all HIPAA-related activities that require documentation. Any action, activity or assessment that must be documented shall be stored or maintained in accordance with this and other policies and procedures implemented by the Organization. Such documentation must be used, applied and reported according to the law and other Organizational policies.

This Organization retains all HIPAA-related documentation for a minimum of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later. All workforce members need to have appropriate access to security and privacy policies and procedures, which should be organized in a logical, indexed fashion for ease of retrieval. Policies and procedures addressing documentation of Security and Privacy compliance must be regularly updated and maintained for accuracy. Changes introduced by technology (especially those impacting investigation, logging and tracking or documenting and reporting on security or privacy events/incidents, requests, complaints, etc.) should be reflected and addressed in the Organization's compliance program documents.

Technology is increasingly required to manage complex security and privacy compliance programs. As new technologies are introduced, the Organization's policies and procedures should be updated any time there is a material change to the processes or safeguards that the technology introduces.

Documentation to be strongly considered for retention throughout the entire HIPAA-defined retention period includes, but is not limited to the following list:

- Security Risk Assessment (Analysis), also known as (SRA)
- Privacy Risk Assessment (PRA)
- Privacy and Security Risk Management Plan and all program-related documentation

- Sanction and mitigation activities
- Business Associate Agreements (or if a BA, Sub-contractor Agreements) , Confidentiality Agreements and other privacy or security compliance agreements or contracts
- Wrongful disclosure violation / breach detection, investigation, determination and notification forms
- Configuration, update and patch management
- Results of disaster recovery test plans, results, emergency testing and business continuity documentation
- List of software used to manage and control internet access and use
- Penetration testing and vulnerability scans
- Security issues logs
- List of workstations, their use and employees who can access them
- Audit log copies
- Business Associates and other agreement documentation surrounding the protections of privacy and security in congruence with this Organization's policies
- Business Associate ongoing compliance monitoring
- Documentation surrounding Patient Rights requests (Individual Access to PHI, Amendment, Restrictions, Accounting of Disclosures forms), any Confidential Communications, etc.
- Proactive, concurrent and retrospective access; other privacy audits and reviews
- Privacy and security education and training
- Other general security and privacy documentation

Appropriate workforce members who need access to this information must be provided such access.

E. Related Polices:

- 19as - HIPAA Privacy and Security Compliance Program Master Policy
- 123s - Record Retention
- List additional related polices: none

F. References

- Stericycle Online Privacy and Security Risk Assessment tools (PRA & SRA)
- 45 CFR §164.302 - §164.318, §164.312(b)(2)(i), §164.316, §164.530(j)(1)(ii), §164.530(j)(1)(iii)
- SRA Line Items: B1, B4, b7, B11, B12, B49, B61, B62, B63, B93, C17, D18, D19, E11, F4, F5, F6, F7.
- 2013 HIPAA Omnibus Privacy Final Rules
- List additional references: none

Appropriate Access to PHI by Workforce Members

A. Coverage

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

B. Create / Revision Date

11/28/2021

C. Purpose

To define the policy related to timely and appropriate access to patient information along with PHI confidentiality. Each user is ultimately responsible for adhering to this policy. Users must only access/view the minimum set of PHI that they have a legitimate "need to know," regardless of the extent of access provided.

D. Policy

Appropriate access to clinical information is defined as providing a user timely access to patient-specific information, which is necessary to perform his/her professional responsibilities. Access will be granted for an individual to provide and/or support quality patient care processes, as defined by an individual's professional responsibilities to the patient and the facility. All department management, Administration, and members of the Organization's Executive Committee are responsible for ensuring that this policy is applied to all individuals using PHI.

This policy embraces the following principles related to the collection, processing, maintenance, and storage of patient information.

1. Workforce members will access, use, collect, dispose, process, view, maintain, and store patients' clinical and financial information in an honest, ethical, and confidential manner.
2. The access, use, collection, processing, viewing, maintenance, and storage of patient information will be done in such a manner that, at a Minimum, it meets all applicable Federal and State Laws, Rules, Regulations, and Accreditation Standards.
3. Each department within this Organization must provide support to effectively maintain patient information in a confidential manner.
4. Access to patient information will be limited to individuals with a legitimate "need to know" in order to effectively perform their specific job duties and responsibilities. Minimum Necessary use of PHI principals is also applied. User roles and related permissions are defined and managed within all computer systems that contain PHI (ePHI).
5. Workforce member access to PHI will be granted after execution of appropriate confidentiality statement by the workforce member.
6. Job descriptions will address what PHI is accessible by which job roles.
7. Access to PHI will be according to specific written policies and procedures.
8. All workforce members must conform to security polices, i.e., not sharing access credentials, to help protect PHI.

E. Protocol for Breach of PHI Confidentiality (Privacy):

Breach of Privacy will be handled in accordance with administrative policies, including the Privacy Event Breach Determination; Harm Threshold Analysis; Notification; Sanctions, Enforcement and Discipline policies.

F. Related Polices:

- 7s - Confidentiality of PHI
- 21s - Privacy Event Breach Determination, Harm Threshold Analysis and Notification
- 26s - Sanctions, Enforcement and Discipline
- List additional related polices: none

G. References

- JCAHO Standard: Management of Information Standard 2.10 and 2.20
- 45 CFR §164.530
- Stericycle Online Security Risk Assessment (SRA)
- SRA Line Items: B26, B39, B44, B62, C2, D3, D5
- List additional references: none

Confidentiality of PHI

A. Coverage

HCBS Provider (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

11/28/2021

C. Purpose

To define the Organization's Confidentiality Policy and the use of confidential communications.

D. Policy

All Organization workforce members who have access to or disclose sensitive or confidential patient information (also referred to as *protected health information (PHI)* or *electronic protected health information (ePHI)* by Health and Human Services and in HIPAA law) have a responsibility to maintain at all times the confidentiality of this information.

Examples of sensitive or confidential information include, but are not limited to the following types of information:

1. Patient demographics or financial information
2. Medical Records, diagnostic or clinical records in general
3. Employee
4. Payroll
5. Billing
6. Contract
7. Medical Staff

Access to, or disclosure of PHI/ePHI must be controlled and monitored by the Organization at all times.

Organization in General

The policy of the Organization is to maintain patient confidentiality when using Protected Health Information (PHI/ePHI) in any form, including, but not limited to the following:

1. Verbal communications
2. Hard copy records (charts)
3. Electronic records
4. Printouts pertaining to the patient

5. Notes maintained by staff or physicians providing care to the patient
6. White boards
7. Patient sign-in sheets
8. Message logs
9. Inquiries or information from payers
10. Faxed patient information
11. Diagnostic testing/results
12. Printed patient information
13. Electronic copies of patient information
14. Data Exchanged copies of patient information
15. E-mails, letters or other individual (patient) communications / disclosures of PHI

The Organization applies HIPAA-based security measures (i.e. password protection and encryption) to prevent unauthorized users from accessing patient and other information in computerized data systems.

In addition, the Organization does the following to protect patient confidentiality:

1. Restricts the amount of information released in response to calls about current patients.
2. Responds to and follows all proper individual (patient) requests for confidential communications; Confidential communications can be facilitated through a number of differ manners. This Organization's workforce will work with the individual (patient) to create a confidential atmosphere for communications of their PHI according to their guidelines as to the method, format and receiving parties of these communications.
3. Incorporates into its Policies and Procedures, existing laws and additional protections for highly sensitive information, such as HIV diagnosis and treatment records.
4. Provides training on privacy and security policies and practices to all workforce members.
5. Applies appropriate sanctions when violations of this policy occur.
6. Identifies information that is classified as confidential by using sign-on screen notices, splash screens, signage, or other methods of identification to flag user that information is confidential.
7. Insert other specific procedures/practices used to protect patient confidentiality: secondary verification with password protection, encryption for email that contains PHI

Departmental Responsibilities

Each organizational unit within the Organization is responsible for enforcement of policies, standards, and practices set forth by the Organization to maintain patient confidentiality.

Management responsibilities shall include, but are not limited to the following:

1. Secure storage of patient information.
2. Procedures for release of patient information to third party payers, providers, etc.)
3. Procedures for disposal of hard copy records and electronic records.
4. Secure transmission and storage of electronic records.
5. Protection of confidential information from access, use, or dissemination by unauthorized persons.
6. Use of confidential communications as agreed to by the Organization from an individual (patient) request.
7. Monitoring that access to PHI is secured, controlled, documented and closely managed and in accordance with written policies and procedures.
8. Auditing for inappropriate access and use of PHI by individuals and workforce members.

Individual Responsibilities

All Organization workforce members and vendors are responsible for adhering to this and related information security policies and standards and for safeguarding all confidential patient information. These responsibilities shall include, but are not limited to, the following:

1. Avoid access, retrieval, or use of any information on a current or former patient unless authorized for legitimate job related duties (i.e. assisting in care/treatment, providing a consultation, or approved educational research or business purposes) within the Organizational unit.
2. Limit the access, use, and disclosure of protected health information to the minimum amount necessary to accomplish the intended purpose.
3. Interact with individuals (patients) to determine the best methods and formats for confidentially communicating with them, especially upon, but not necessarily as a result of their specific request.
4. Dictate patient notes and discuss patient care only in private areas (i.e. not in hallways, elevators, cafeteria lines).
5. Protect personal User ID and password used to access the Organization's data *Systems* from disclosure to others.
6. Take special care to protect information (e.g. in hard copy charts, printouts or on computer screens) from being viewed by unauthorized persons.
7. Use secure methods for authorized storage, transmission, disclosure and disposal of confidential PHI.

Employees are responsible for reporting to the HIPAA Privacy Officer or HIPAA Security Officer any known or suspected internal /external violation of Organization privacy policies or any wrongful use or disclosure of PHI.

Privacy Officer Contact Information:
Cathy Stein, CEO
610-453-5005
cathy@hcbsprovider.com

Security Officer Contact Information:
Cathy Stein, CEO
610-453-5005
cathy@hcbsprovider.com

E. Definitions

Breach of PHI:
Section 13400 HITECH
(1)(A) Breach – (is the) unauthorized acquisition, access, use, or disclosure of' PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
(B) Exceptions – Breach does not include
- (i) any unintentional acquisition, access or use of PHI by an employee or individual acting under the authority of a covered entity or business associate if
  - (I) such acquisition was made under good faith and within the course and normal scope of employment or professional relationship…with CE or BA
  - (II) such information is not further acquired, accessed or used
- (ii) any inadvertent disclosure for an individual who is otherwise authorized to access PHI at a facility operated by a CE or BA
- (iii) any such information received as a result of such disclosure is not further acquired,

accessed, etc.

Electronic Health Record: An EHR (electronic health record) is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Personal Health Record: A PHR (personal health record) is managed, shared, and controlled by or primarily for the individual

F. Related Forms

- Gs – Request for Patient's Rights
- Vs - Confidentiality and Security Agreement
- List additional related forms: none

G. Related Polices:

- 21s - HIPAA Violation and Breach
- 26s - Sanctions, Enforcement and Discipline
- 6s - Appropriate Access of PHI by Workforce
- 11s - Disclosure of PHI
- List additional related polices: none

H. References

- SRA Line Items: B14, B25
- List additional references: none

HIPAA Designated Record Set

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

11/28/2021

C. Purpose

HIPAA regulations state that patients have a right to access portions of their medical record, which is called the "Designated Record Set."The purpose of this policy is to define what is included in the HIPAA-compliant Designated Record Set that is subject to access by individuals (patients) for purposes of obtaining copies of or amending their PHI.

D. Policy

Designated Record Set definition for the Organization is defined with a multi-layered strategy to facilitate management of the processes surrounding patient inspection, copying, restriction and amendment of the records that fit the definition.

Generally speaking, both the patient's medical record (whether paper or electronic health record) and billing records are used to provide access for inspection, copying, requests for restrictions and amendment.

The Organization will engage all individuals making proper HIPAA requests (i.e. requests for access, amendment, disclosure accounting, restriction, or confidential communications) to fully understand and communicate the plans to fulfill these requests in a manner that satisfies the individual and keeps the administrative burden manageable for the Organization.

E. Policy Discussion

On December 28, 2000, the Federal Government published the Standards for Privacy of Individually Identifiable Health Information, more commonly referred to as the HIPAA Privacy Rule. The Privacy Rule was amended on August 14, 2002. The Rule establishes the rights of individuals to inspect, obtain a copy of, and request amendments to information about them in a Designated Record Set.

Section 164.524 of the Privacy Rule states that individuals generally have a right to inspect and obtain a copy of PHI about them in a Designated Record Set. In addition, section 164.526 of the Rule states that individuals generally have a right to have a Covered Entity (CE) amend PHI about them in a Designated Record Set, according to strict guidelines and with CE approval.

Privacy Rule Definition of a Designated Record Set

The Privacy Rule (section 164.501) provides the following definitions for Designated Record Set and PHI in order to clarify the access and amendment standards summarized in the previous paragraphs.

Designated Record Set is defined as a group of records maintained by or for a CE that is:

1. The medical and billing records about individuals maintained by or for a covered healthcare provider. These records are the primary source of Designated Record Set records for the Organization accessible by patients for copying, inspection and amendment and include medical records and Business Office documents and reports. These records are generally more accessible, understandable by patients and include complete summaries and reflections of the complete documentation for patient care and billing. The HIM and Business Office departments are both capable of facilitating patient inspection, copying, and amendment should the site deem these activities appropriate. Other Organization source systems may not be designed to easily facilitate these tasks, and again, are redundant to the information kept within the primary medical records and Business Office records.
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan if a part of the Organization.
3. Information used in whole or in part by or for the CE to make decisions about individuals. The record, data, document and report sets may occur in a multitude of other Organization 'Source Systems' and would be subject to patient inspection, copying and amendment only upon determination from HIM, Compliance, Clinical Management and Information Systems that such inspection, copying, and amendment is necessary to archive the patient's goals, is deemed appropriate given the restrictions to these activities that HIPAA defines (see below for a further explanation of these exceptions) and is technically possible.
4. According to the preamble of the Privacy Rule, records held by a Business Associate (BA) that meet the definition of Designated Record Set are part of the CE's Designated Record Set. However, the individual's rights to access, amend, and receive an accounting of disclosures does not attach to the BA's records if the BA's information is the same as the information maintained by the CE.
5. Uses or disclosures that are required by Law; and
6. To meet the requirements of HIPAA, such as for the content of standard transactions.

Record Sets Not Included in the Designated Record Set

The preamble of the Privacy Rule emphasizes that individuals have a right to access and request amendments only to PHI in a Designated Record Set. Therefore, information obtained during a phone conversation, for example, is subject to access only to the extent that it is recorded in the Designated Record Set. The Rule does not require a CE to provide access to all individually identifiable health information, because the benefits of access to information not used to make decisions about individuals is limited and is outweighed by the burdens of locating, retrieving, and providing access to such information.

The preamble also underscores the fact that CEs often incorporate the same PHI in a variety of different data systems, not all of which will be used to make decisions about individuals. The preamble provides an example in which information systems used for quality control or peer review analysis may not be used to make decisions about individuals. In this example, the preamble says the information systems would not fall within the definition of Designated Record Set. Furthermore, the

preamble states that it does not require entities to grant an individual access to PHI maintained in these types of information systems.

The Privacy Rule and discussions in the preamble also make it clear that individuals do NOT have a right of access to:

1. Psychotherapy notes
2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
3. PHI held by clinical laboratories if the Clinical Laboratory Improvements Amendments of 1988 (CLIA) prohibit such access
4. PHI held by certain research laboratories that are exempt from the CLIA regulations (164.524)

The Rule defines, however, rare circumstances in which access to information contained within the Designated Record Set can be denied. For example, access can be denied when, in the exercise of professional judgment, it is likely to endanger the life or physical safety of the individual or another person.

Additional, Specific Information NOT Included in the Organization's Designated Record Set

1. Health information generated, collected, or maintained for purposes that do not include decision making about the patient or which is exempt from disclosure to the patient:
    a. Data collected and maintained for research.
    b. Data collected and maintained for peer review purposes.
    c. Data collected and maintained for performance improvement purposes.
    d. Data collected and maintained for quality control purposes.
    e. Data collected and maintained for compliance purposes.
    f. Data collected and maintained by the psychiatric Patient's Rights Officer.
    g. Appointment and surgery schedules.
    h. Birth and death registers.
    i. Surgery registers.
    j. Diagnostic or operative indexes.
2. PHI held by clinical laboratories in the Clinical Laboratory Improvements Amendments (CLIA) of 1988, 42 U.S.C. §263 a, prohibit such access. PHI held by certain research laboratories that are exempt from CLIA regulations (164.524).
3. Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding. This includes notes taken by the Organization's employees during a meeting with the Organization's attorney about a pending lawsuit.
4. Employer records
    a. All employee health records.
5. Source Data – interpreted or summarized in the individual's medical record
    a. Pathology slides
    b. Diagnostic films
    c. Electrocardiogram tracings from which interpretations are derived
    d. Photographs
    e. Fetal Monitor Strips
    f. Google Documents data, documents and reports

F. Definitions

Designated Record Set
Designated Record Set is defined as a group of records maintained by or for a CE that is;

1. The medical and billing records about individuals maintained by or for a covered healthcare provider. These records are the primary source of Designated Record Set records for the Organization accessible by patients for copying, inspection and amendment and include medical records and Business Office Records, documents, and reports.
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan.
3. Information used in whole, or in part by, or for the covered entity to make decisions about individuals.

Protected Health Information (PHI) or electronic ePHI

Any information whether oral, written, electronic (ePHI) or recorded in any form that is created or received by the Organization as a healthcare provider and relates to an individual's past, present or future physical or mental condition; healthcare treatment and payment for services. PHI also includes data that identifies the individual (i.e. Name, SSN, MRN, account number, address, telephone number, DOB, e-mail address, names of relatives, employer, etc).

G. Related Polices:

- 2s – Documentation for Privacy and Security Compliance
- 10s – Individual Access to PHI
- 11s – Disclosure of PHI

- 13s – Request for Amendment of PHI
- 14s – Request to Restrict use and Disclosure of PHI
- 15s – Accounting of Disclosures
- List additional related polices: none

H. References

- HIPAA §164.501
- Practice Brief AHIMA: Defining the Designated Record Set
- AHIMA Article in HIM Body of Knowledge: Defining the Designated Record Set and the Legal Health Record
- GAO Report HIT 2008 Report to Chairman
- AHIMA Article HIM Body of Knowledge Preparing for Designated Record Sets – What Shadow Records Can Tell You
- Guidance for Identifying Designated Record Sets under HIPAA V2, Prepared by NCHIA Designated Record Sets Work Group, Approved for Public Distribution February 3, 2003, endorsed by the NCHIMA
- Section 164.524 of the HIPAA Privacy Rule

- Section 164.526 of the HIPAA Privacy
- Section 164.501 of the HIPAA Privacy Rule
- PRA Line Item: E.1, E.2
- List additional references: none

Minimum Necessary, Limited Data Set and De-identification of Data

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 supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

11/28/2021

C. Purpose

When using or disclosing PHI or when requesting PHI from another Covered Entity (CE), the Organization will make reasonable efforts to limit PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request.

D. Policy

As a general rule, the Organization may not use, disclose, or request the entire medical record of a patient unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

Uses or disclosures that impermissibly involve more than the minimum necessary information may qualify as Privacy Breaches under Interim and Final HIPAA Privacy Rules. In contrast, a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper Minimum Necessary procedures would not be a violation of the Privacy Rule.

One manner in which Minimum Necessary criteria can be met is by disclosing 'limited data sets' that exclude the direct identifiers listed below as well as dates of birth and zip codes, for a total of **18 identifiers**. The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members. Under the HIPAA Privacy Rule "identifiers" that must be removed include the following:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be

aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted; and the CE does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Note: Birthdates and Zip codes no longer qualify as exceptions to the requirement to perform Breach Determination as of September 23, 2013, upon implementation of the Omnibus Final Privacy Rules.

Limited Data Sets

Limited Data Set (LDS) is created by removing the identifiers listed above for the purpose for which the LDS was created. A LDS can be utilized to disclose records without PHI for research, public health, or healthcare operations. The Organization's workforce may not use or disclose a LDS until a Data Use Agreement with the recipient of the LDS has been obtained. All uses of a LDS will comply with the Minimum Use. In accordance with the Organization's Accounting of Disclosures policy the LDS does not need to be recorded in the Accounting of Disclosure log or with any Accounting of Disclosures request.

Minimum Necessary Applicability

The Organization's workforce shall use, disclose or request the minimum necessary amount of PHI in all situations except the following:

1. Disclosures to or requests by a health care provider for treatment;
2. Uses or disclosures made to the individual;
3. Uses or disclosures made pursuant to a valid, written patient authorization;
4. Disclosures to the Secretary of the U.S. Department of Health and Human Services or related entities such as the Office for Civil Rights (OCR), charged with HIPAA privacy and Security enforcement;
5. Uses or disclosures that are required by Law; and
6. To meet the requirements of HIPAA, such as for the content of standard transactions.

The following protocols are facilitated by the Organization's Privacy and Security Officer(s) relative to

the Minimum Necessary rule:

1. The Organization shall identify persons (or classes of persons) within the Organization who need access to PHI to carry out their duties.
2. For each person (or classes of persons), the Organization shall identify the category (or categories) of PHI to which access is needed and any conditions appropriate to such access.
3. Once persons within the Organization who need access to PHI and categories of information are identified, the Organization must make reasonable efforts to limit access only to such identified persons and such uses or disclosures only in such identified categories. With respect to *System* access, patient privacy will be supported through authorization, access, and audit controls and will be implemented for all systems that contain patient identifiable information. Within the permitted access, a staff member may only access information needed to perform his/her job duties.
4. For disclosures that are of a non-routine nature, the Organization's Privacy Officer:
    i. will develop criteria and train the applicable staff to limit the PHI disclosed to the amount reasonably necessary to accomplish the purpose of the disclosure or request; and
    ii. have the applicable staff at the Organization review requests for disclosure on an individual basis in accordance with such criteria.
5. Standard Policies and Procedures can cover 'routine and recurring' uses, disclosures and requests without need for any review. A process must exist for reviewing the non-routine events on an individual basis.
6. The Organization's staff may rely on a requested disclosure as the Minimum Necessary for the stated purpose (if reliance is reasonable under the circumstances) in the following situations:
    a) When making disclosures to authorized public officials if the requesting official represents that the information is the minimum necessary.
    b) When the information is requested by another CE.
    c) When the information is requested by a professional who is a member of the Organization's workforce, or is a Business Associate (BA) of the Organization for the purpose of providing professional services to the Organization, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).
    d) When the information is requested for research purposes and the person requesting the information has provided documentation that requests specific information.

De-identification of PHI

The Organization may disclose de-identified PHI as set forth in this policy. De-identified PHI is health information that does not identify an individual, and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Health information shall be considered de-identified if either of the de-identification procedures set forth below is followed. In addition, the Organization may use PHI to create de-identified health information or disclose PHI to a BA to create de-identified health information. The Organization may determine that health information is de-identified health information if the following conditions exist:

- Statistical Methods

  A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (a) determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (b) documents the methods and results of the analysis to justify such determination; or

- Safe Harbor

1. All eighteen (18) of the following identifiers of the individual or relatives, employers or household members of the individual are removed:
   a. Names;
   b. Geographic subdivisions smaller than a state (e.g. street address, city, county, precinct, zip code, etc.);
   c. All elements of dates, except year, directly related to an individual date, admission date, discharge date, date of death; and for all ages over 89, all elements of date including year indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older. Note, however, that for research or other studies relating to young children or infants, the Organization may express age of an individual in months, days or hours;
   d. Telephone numbers;
   e. Fax numbers;
   f. Electronic-mail addresses;
   g. Social security numbers;
   h. Medical record numbers;
   i. Health plan beneficiary numbers;
   j. Account numbers;
   k. Certificate/license numbers;
   l. Vehicle identifiers and serial numbers, including license plate numbers;
   m. Device identifiers and serial numbers;
   n. Web universal resource locators (URLs);
   o. Internet protocol (IP) address numbers;
   p. Biometric identifiers including finger and voice prints;
   q. Full face photographic images and any comparable images; and
   r. Any other unique identifying number, characteristic, or code; except the Organization may assign a code or other means of record identification to allow the Organization to re-identify information that was identified if:
      i. The code or other means of record identification is not created from information about the individual and cannot be translated to identify the individual; and
      ii. The Organization does not use or disclose the code or other means of record identification for any other purpose and does not disclose the method by which to re-identify the individual.

   HHS has removed the exception for limited data sets that do not contain any dates of birth and zip codes. In the Omnibus Final Rule, following the impermissible use or disclosure of any limited data set, a Covered Entity or Business Associate must perform a risk assessment that evaluates the 4 'low probability of compromise' factors to determine if breach notification is not required.

2. The Organization does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual patient who is a subject of the information.

In addition, a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified may be disclosed except as otherwise permitted under the Organization's policies for disclosure of PHI.

De-identified information that has been re-identified may not be disclosed or used except as

otherwise permitted under the Organization's policies for use and disclosure of PHI.

E. Related Polices:

- 6s - Appropriate Access to PHI by Workforce
- 102s – Workforce Security Clearance
- 115s – Access Controls
- List additional related polices: none

F. References

- Title 45, Code of Federal Regulations, Parts 160 and 164, August 14, 2002
- HHS Interim Final Rule Breach Notification for Unsecured Protected Health
- Omnibus Privacy Final Rule Modifications, January 2013.
- Information Title 45 CFR Parts 160 and 164
- §164.502(d) and 164.514(a)-(b)
- SRA Line Items: B39, B44
- PRA Line Item: C.8, C.9, K.6
- OCR (Office for Civil Rights); Guidance Regarding Methods of De-identification of Protected Health Information in Accordance With HIPAA Privacy Rule, September 04, 2012
- List additional references: none

Individual Access to Protected Health Information (PHI)

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

11/28/2021

C. Purpose

Specifics on how individuals (patients or their authorized representatives) may request access and copies of their Protected Health Information (PHI) contained within designated record sets.

D. Policy

Individuals (patients or their authorized representatives) who wish to access PHI may do so only in accordance with applicable State and Federal Laws. Requests for access and copying must be in writing and signed by the patient or legal representative unless during a period of active care. This Policy and Procedure establishes the process for handling patient requests, circumstances where the Organization may deny access, the patient's right to appeal a denial, the time frame within which requests will be processed, and fees for making requested copies available.

Generally speaking, a patient's medical record (whether paper, electronic document management, electronic health record (EHR) or defined hybrid systems and billing records contained within the designated record set) is used to provide inspection, copying and amendment of information. Because these records are compilations and summaries of information from other Source Systems and are in fact copies of other existing data and document types, they will be primarily offered for individual access, restriction and amendment.

Patient Access to PHI during an Episode of Care

Pertinent information may be provided to patients and their personal representatives to share with other providers for treatment purposes. Patients may review their medical records (without addition or correction) during the period of active care. Corrections or additions must be handled in accordance with the administrative policies for 'Patient Request for Amendment of Protected Health Information'. The patient's attending physician should be notified if the patient has questions about the documentation or feels that information may be in error. These disclosures do not require authorization or written request. Access to Behavioral Health records should be handled in accordance with this Individual Access to PHI policy and with the guidance of the physician(s).

Patient Access to PHI after Patient Has Concluded the Episode of Care

1. Information available to the patient

Upon appropriate written request, access will be permitted to the individual patient's PHI, primarily medical records and billing records unless the information falls into one of the categories which may be denied as discussed below. Peer review, quality assurance, and information created and maintained for business purposes of the Organization and not used to make decisions about an individual patient in the process of healthcare delivery are *not* considered part of the designated record set and are not subject to review or copying by the patient or legal representative.

In addition, patients may *not* have the right to access and obtain copies of:

a. Psychotherapy Notes
b. Information compiled for use in civil, criminal, or administrative actions
c. Information subject to prohibition by the Clinical Laboratory Improvement Act (CLIA); or
d. Information that is not part of the designated record set

2. Request must be in writing

Individual patients or legal representative must request access to their own protected health information in writing. The request must be signed and dated by the patient or legal representative. Electronic forms and signatures may be used in place of paper forms and handwritten signatures.

3. Time frame for response to patient request

Access to inspect medical and billing records will be provided within five (5) working days of receipt of the written request. Copies will be provided within fifteen (15) working days of receipt of the written request.

4. Manner of access

The Organization will arrange with the individual a convenient time and location in the facility to inspect or obtain copies of the PHI. Individuals reviewing records must provide identification upon request.

Inspection will be attended by an Organization workforce member. The patient or legal representative will be referred to the patient's physician for discussion of clinical questions. Copies of the records may be mailed in lieu of inspection at the facility upon patient request.

5. Fees

No fee will be charged for retrieving a patient's records and allowing the patient or his legal representative to review them.

Reasonable cost-based fees (also per State mandated fee schedules) may be charged by the Organization for providing copies of PHI, other than those requests delineated as no charge within appropriate published fee schedules or policy.

The fees will include the costs of copying paper records or printing for electronic records (including supplies and labor) and postage (if the individual has requested that the records be mailed). A current fee schedule will be provided upon request. Storage media may not be charged for.

6. Denial of patient access

   A request for access or copies may be denied in the following situations:

   a. The request is for records that are not available for inspection;
   b. The Organization is acting under the direction of a correctional institution to deny access to an inmate;
   c. The PHI has been created or obtained during an active research project and the patient agreed that access would not be permitted while the research project was active;
   d. The PHI contains information obtained from someone other than a healthcare provider under a promise of confidentiality and the requested access would reveal the source of the information;
   e. The requested information has been compiled in anticipation of a civil, criminal, or administrative proceeding;
   f. The request is for behavioral health records, which may contain reference to another person, and the CEO has determined that the information may endanger the life or safety of the patient or the other person referenced; or
   g. The request is from the patient's legal representative for behavioral health records which makes reference to another person, and the CEO has determined that access to the information is likely to endanger the life or safety of such other person.
   h. If access or copies are denied, a written explanation of
   i. the basis for denial will be provided to the patient or legal representative within five (5) working days of receipt of the request. This explanation will include information regarding whether or not an appeal to the Organization may be made, the process for placing and handling such an appeal, and how to register a complaint with the Secretary of the Department of Health and Human Services.

7. Appeal of denial

   If access is denied, it must first be determined whether the denial may be appealed.

   a. Unreviewable grounds for denial –
      No appeal process exists under State or Federal Law in the following circumstances:
      i. the PHI is exempted from the right of access;
      ii. the Organization is acting under the direction of a correctional institution to deny access to an inmate, and the information could jeopardize the health, safety, security, custody, or rehabilitation of the inmate, any officer, employee, or other inmates;
      iii. a patient's right to protected health information created or obtained in the course of research may be temporarily suspended while the research is in progress, provided the patient has agreed to the denial of access when agreeing to participate. The right of access will be reinstated upon completion of the research; or
      iv. the PHI contains information obtained from someone other than a healthcare provider under a promise of confidentiality and the requested access would reveal the source of the information.
   b. Reviewable grounds for denial –
      The individual may appeal a denial under the following circumstances:
      i. The CEO has determined that the access is likely to endanger the life or safety of the individual;
      ii. The records contain reference to anther individual and the CEO has

determined that the access is likely to endanger the life or safety of such other person; or

iii. The request is made by the individual's legal representative and the CEO has determined that the access is likely to endanger the life or safety of the individual or another person.

8. Appeal for review of a denial of access

If access is denied based on reviewable grounds, an appeal must be made in writing and signed and dated by the patient or legal representative who made the original request.

If an appeal is made, the review must be performed within a reasonable period of time by a licensed healthcare professional designated by the Organization who did not participate in the original decision to deny access.

The reviewer will determine whether or not to deny access based on the items listed above under 'Reviewable grounds for denial.' The reviewer will promptly report his decision to the CEO

9. Retention of documentation

All documentation related to an individual's, or legal representative's, request for access, and any documentation related to a denial process, will be filed with the medical record and retained in accordance with the policy for retention of medical records for a minimum of at least six (6) years.

Procedures for Patient Access to PHI

All requests for access to PHI by an individual patient or legal representative will be assessed in accordance with this policy. Appropriate response will follow promptly.

1. Written request

All requests for access of copies of protected health information must be in writing (or via permanent electronic form) and must be signed and dated (which can be via electronic methods) by the individual patient or legal representative. Incomplete requests will be considered invalid and will be returned to the requestor immediately.

2. Reply to request

Unless denied, access to inspect medical, behavioral health, and billing records will be permitted within validate these timeframes five (5) working days of receipt of the written request. Copies will be provided within validate these timeframes fifteen (15) working days of receipt of the written request.

Patient requests for access to behavioral health information will be referred to the CEO and the requestor will be so notified immediately upon receipt of the request.

If access or copies are denied under conditions listed above in this policy, the CEO, Risk Manager, or designee, will be so notified. A written explanation of the basis for denial will be provided to the patient or legal representative within five (5) working days of receipt of the request.

3. The process for appeal

Upon receipt of a written appeal for review of the denial CEO, or designee, will be notified.

Administrative arrangements will be made promptly to secure the services of a licensed healthcare professional not previously involved in the denial process.

The requestor will be notified promptly of the determination of the reviewer. If access is to be permitted, arrangements will be made to permit inspection within five (5) days of the determination. If copies are to be provided, the copies will be provided within fifteen (15) days of the determination.

4. Retention of documentation

All documentation relating to the request, or any denial or appeal will be filed with the medical record and retained in accordance with the policy on retention of medical records.

5. Timeliness provision changed.

    a. The Final Omnibus Privacy Rule modifies the timeliness requirements for right to access and to obtain a copy of PHI to 30 days from the date of the request.
        i. OCR has removed the provision that permits 60 days for timely action when protected health information for access is not maintained or accessible to the covered entity on-site.
        ii. OCR has retained the provision that permits a covered entity a one-time extension of 30 days to respond to the individual's request;
            1. With written notice to the individual of the reasons for delay and the expected date by which the entity will complete action on the request.
        iii. Covered entities that spend significant time before reaching agreement on the electronic format for a response are using part of the 30 days permitted.

Copies of Electronic Records

1. The Privacy Rule requires that if an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the CE must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or
    a. If not, in a readable electronic form and format as agreed to by the covered entity and the individual.
    b. In such cases, to the extent possible, we expect covered entities to provide the individual with a machine-readable copy of the individual's PHI.
        i. HHS/OCR considers machine-readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer.
        ii. For example, this would include providing the individual with an electronic copy of the PHI in the format of MS Word or Excel, text, HTML, or text- based PDF, among other formats.
        iii. If an individual requests a form of electronic copy that the covered entity is unable to produce, the covered entity must offer other electronic formats that are available. If the individual declines to accept any of the electronic formats that are readily producible by the covered entity, the covered entity must

provide a hard copy as an option to fulfill the access request.

c. If the designated record set includes electronic links to images or other data, the images or other data that is linked to the designated record set must also be included in the electronic copy provided to the individual.
d. How and to what extent a BA is to support or fulfill a CEs obligation to provide individuals with electronic access to their records will be governed by the Business Associate Agreement between the CE and the BA.

2. PDF is recognized as a acceptable electronic format, although OCR remains technically neutral.

3. Hard copy is to be provided if the individual denies all formats of electronic offered by the CE.

4. CEs are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email.

E. Related Polices:

- 19as – HIPAA Privacy and Security Compliance Program Master Policy
- List additional related polices: none

F. References

- Omnibus Final Privacy Rule Modifications – January 2013
- Title 45, Code of Federal Regulations, Parts 160 and 164, August 14, 2002
- 45 CFR 164.524
    - §164.524(a)(1)
    - §164.524(a)(2)
    - §164.524(a)(4)
- JCAHO Standard: Management of Information Standard 2.10 and 2.20
- PRA Line Item: C.19, C.21, C.22, C.23
- List additional references: none

Disclosure of Protected Health Information

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

11/28/2021

C. Purpose

This Policy defines appropriate administrative guidelines to ensure the confidentiality of protected health information (PHI) and to ensure that PHI is released as appropriate, in accordance with Organization policy, legal and regulatory agency requirements (most notably, state and federal HIPAA regulations).

D. Policy

The medical record is a confidential and privileged document. The medical record is the property of the Organization and is maintained for the benefit of the patient, the medical staff, and the Organization. It is the responsibility of the Organization to safeguard the information in the record against loss, defacement, or use by unauthorized persons. Original medical records shall not be removed from the premises except on a court order, subpoena from a court of law, or statute, and only when accompanied by the Organization's designated *Custodian of Medical Records*. Any release of PHI to persons not otherwise entitled to receive this information requires the patient's written authorization.

General Rules

All requests for PHI received by the Organization will be forwarded to appropriate staff members for processing. No PHI will be released by anyone other than HIM/Medical Records personnel or individuals authorized to do so for emergency medical care purposes.

Authorization

1. The following shall constitute a valid authorization, those cases in which a valid authorization is required before PHI may be released.

a. The authorization must:
    i. Be in writing (an electronic form with electronic signature is acceptable)
    ii. Identify person(s) authorized to make the use/disclosure
    iii. Identify person(s) to whom the disclosure may be made
    iv. Describe the information to be disclosed in a specific/meaningful fashion
    v. Contain expiration date
    vi. Describe individual's right to revoke in writing
    vii. Describe exceptions to right to revoke
    viii. Describe how to revoke
    ix. State that information used/disclosed may be subject to re-disclosure by recipient
    x. Contain the signature of the individual and date
    xi. Describe the individual's authority to act, if signed by patient representative.
    xii. Right to a copy of the form
    xiii. Conditioning Statement
    xiv. Purpose for releasing records
    xv. Be in plain language
    xvi. Include any State requirements
b. The authorization must be dated subsequent to the last visit requested. The authorization must be utilized within a 90-day period from the date of the authorization unless stipulated otherwise.
c. The authorization must not have been revoked or restricted subsequent to the date of the signed authorization. An authorization may be revoked or restricted verbally by the patient with proper notation of this being made in a prominent place on the form in the medical record. At the time of the verbal revocation or restriction, the patient should be requested to submit/send a written statement of his or her wishes.
d. Photocopies of the original authorization are acceptable, in lieu of the original.
e. The authorization must be signed by one of the following personal representatives:
    i. Patient, this includes an emancipated minor which is anyone under 18 years of age, who
        1. is married or
        2. is financially independent and not living with parents or has been declared legally emancipated by an action in a court of law
    ii. Parent, guardian, or other person acting in loco parentis when patient is a minor (in case of divorce, the parent with legal custody must sign the release)
    iii. Exceptions:
        1. Minor consented to the health care treatment.
        2. Minor lawfully obtained healthcare services without the parent/guardian consent.
        3. Parent/guardian agrees to confidentiality between the facility and the minor.
        4. Healthcare surrogate or Durable Power of Attorney designated by the patient (documentation will be required to prove as such).
        5. Guardian, when the patient is legally declared mentally incompetent.
        6. Executor or administrator of the estate if the patient is deceased. (Documentation will be required to prove as such).
        7. Next of kin of deceased, if there is not an executor of the estate.
            i. Next of Kin - A patient's next of kin is determined in the following order of priority:
            ii. Married Patient - If the patient is married, authorization is obtained from:
                1. The spouse;
                2. Or if no spouse is living;

3. Any child of such marriage;
4. Or in the event of a minor child of such marriage.
5. The guardian of such child, if any;
6. Or in the absence of such guardian,
7. The court having jurisdiction of the person of such a minor;
8. Or in the event neither spouse nor child survives.
9. A person who would be allowed to give permission in the case of an unmarried patient.

iii. Unmarried Patient - If the patient is unmarried, authorization should be obtained from one of the following, in order of priority as follows;
1. Parents
2. Guardian
3. Next of Kin

iv. Next of Kin means the nearest relative to the patient either by blood relationship or by Marriage. Priorities of rights are as follows:
1. Legal spouse
2. Children
3. Parents
4. Brothers and sisters
5. Grandparents
6. Uncles and aunts

iv. The facility may refuse to treat an individual as a personal representative of an individual in the following incidences:
1. Individual may be subject to domestic violence, abuse, or neglect.
2. Treating as personal representative would endanger the patient.
3. Not in the patient's best interest to treat as personal representative.

f. The identity and authority of the individual requesting and/or receiving PHI must be verified in one of the following methods:
i. Obtaining documentation, statement, or representation forms (i.e., driver's license, Durable Healthcare Power of Attorney, etc.). A copy of the documentation form should be made and filed with the authorization in the medical record.
ii. Agency identification badge, government letterhead, and written or oral statement of legal authority for public officials.
iii. Exercising professional judgment regarding the involvement of individual in care of the patient.

Disclosure of PHI Authorization Required

1. Patients/Families - Medical records may be released to a patient or his/her legal representative when a written authorization to disclose health information is submitted by the patient or someone authorized to act on his/her behalf.

2. Non-Staff Physician - A physician not on the staff of the Organization who requests copies of records must provide a signed authorization from the patient.

3. Other Hospitals and Health Care Institutions/Emergency Release - Information may be released to other hospitals and health care institutions upon receipt of a signed authorization

by the patient, unless in emergent, treatment situations.

Exception

Emergency phone calls for diagnostic and therapeutic information on patients are honored if the caller identifies himself as a physician or an allied health practitioner caring for the patient. Emergency phone calls constitutes that harm could be brought to the patient without this information. When the necessary information is obtained, the caller is asked for his phone number so the call can be returned. This allows time to verify the name of the institution or practitioner making the request before the information is given. The information released, and to whom, must be documented on an authorization form and placed in the patient's medical record. Documentation should include whether information was verbally released or faxed. List all the areas where these releases are documented.

Copies of the medical record may be sent with a patient being transferred to another hospital or nursing home.

1. Other Attorneys - If an attorney wishes to obtain a copy of the patient's medical record, he must present a valid authorization. A request to review the medical record onsite will be referred to the CEO.
2. Note: The Organization's Risk Manager will be notified of attorney requests if viewed to possibly result in litigation against the Organization, this is called 'Litigation Response'.
3. Insurance Companies - All insurance companies requesting copies of medical records must do so in writing. If the requesting insurance company is listed as Primary, Secondary or Tertiary carrier, and the patient has signed the Patient Consent Admissionand/or Medical Treatment form, the records will be released.
4. Financial Auditors - Financial Auditors not employed by the Organization wanting to review a patient's record for financial audit purposes (substantiation of specific Organization charges), must present a valid authorization signed by the patient. The medical record need not be complete at the time of review.
5. Law Enforcement Officials (State, County Police, FBI, CIA, etc.) - The fact that a request comes from a governmental agency does not constitute a waiver. Confidential information should be released upon presentation of a valid authorization signed by the patient, guardian, or a valid Law Enforcement subpoena for medical records.
6. Federal, State, and Local Government and Voluntary Welfare Agencies (Schools, Welfare Department's, VA, IRS, Rehabilitation, etc.) - Confidential information should not be released without a valid authorization.
7. Blue Cross, Blue Shield, Medicare - Medical information can be released without an authorization if listed as the patient's insurance carrier and the Patient Consent of Admission and/or Medical Treatment form has been signed by the patient. No charge will be made for furnishing such information.
8. News Media - All requests for information from the News Media will be treated as normal requests for information, none will be released without patient authorization.
9. Parties in Cases Involving Adoption - Attorneys, physicians or agencies may receive PHI regarding the infant upon receipt of a signed authorization given by the natural mother.

Authorization not required

1. Staff Physician - Members of our Medical Staff may view and/or obtain copies of medical records of patients they have treated during the requested visit. Members of the Medical Staff may have unrestricted use of the medical records of Organization to fulfill the function of the Organization and Medical Staff Committees and Medical Staff departments established under the by-laws.
2. Organization Attorney - The attorney representing the Organization may review medical records or obtain copies without the patient's authorization.
3. Public Health Authorities - Information may be furnished to public health authorities without a signed authorization from the patient for the following purposes: preventing or controlling disease, injury, or disability; reporting injuries from domestic/wild animals, recording births or deaths; public health surveillance; and reporting abuse, neglect, or domestic violence. The Public Health investigator must provide personal identification. If the request is via telephone, information will be furnished by return phone call with proper identification of the recipient of the information being made at that time. Information released should be entered into the disclosure tracking system.
4. Medical Examiner - Any information requested may be released to the Office of the Medical Examiner without a signed authorization. No information may be released to a Medical Examiner or investigator without verification by the Medical Examiner's Office that he does represent the Office of the Medical Examiner. Information released should be entered into disclosure tracking system.
5. Administration – Administrators of our practice may have access to medical records when needed to carry out the administrative duties.
6. Organization Personnel- Access to medical records is permitted by employees of this practice for Treatment, Payment, or Operations in the normal course of their duties. Exception: Organization employees requesting access to their own or a family member's record will be addressed the same as any patient request for PHI. An authorization must be provided before any information is released.
7. Worker's Compensation Cases - The worker's compensation insurance carrier is entitled to a narrative summary (face sheet, discharge summary and operative report) of the patient's worker's compensation hospital visit.
8. Home Health Agencies – PHI should not be released without a valid authorization unless it is documented in the medical record that the patient has been discharged to the requesting agency.
9. Employer - Employer may receive PHI if the Organization provided healthcare at the request of the employer, or if the Organization is providing medical surveillance for a work related injury.
10. Food and Drug Administration (FDA) - Information may be released to the FDA without a signed authorization from the patient for the following purposes: reporting adverse events, product defects or biological product deviations, tracking products, enabling product recalls, repairs, or replacement, and conducting post marketing surveillance. Information released should be entered into the disclosure tracking system.
11. Health Oversight Activities - Information may be released to health oversight entities for review of compliance with regulatory standards, federal requirements, and state statues. Examples would be HIPAA, JCAHO, AHCA, or FMQAI. Information released should be entered into the disclosure tracking system.
12. Funeral Director - Information may be released to the funeral director without a signed authorization from the next of kin for the purpose of completing the death certificate.
13. Specialized Government Functions - These functions include military and veteran activities, National Security and Intelligence, Protective Services, Department of State (medical suitability), correctional institutions, and government programs providing public benefits.

14. Immunization records provided to schools with verbal authorization from parents or loco parentis, provided our Organization documents in writing this verbal authorization.

Subpoena / Production of Documents

1. The subpoena must be legal and complete. The following must be included:
    a. Name of the medical records being subpoenaed
    b. Date, time and place to appear for deposition
    c. Court number or the location of the court in which suit is pending
    d. Docket number
    e. The style of the suit (Plaintiff vs. Defendant)
    f. The source of the authority issuing the subpoena (attorney, clerk of court, judge)
    g. Party summoning the witness
    h. Date and signature of person authorized to issue the subpoena.
    i. Must be issued in the Pennsylvania.

    If the subpoena requests medical records of a third party who is not a party to the lawsuit, a statement from the attorney acknowledging that this third party has been notified of the request if required.
2. The Production of Documents is a request by an attorney accompanied by a certificate of service. Optional; Pennsylvania.
3. A Court Order is a document issued by a judge for the mandatory release of medical records. The Court Order will stipulate where the records are to be sent.

AIDS / HIV / Alcohol / Drug Abuse / Mental Health Records

An all-inclusive written authorization indicating the release of AIDS/HIV, Alcohol/Drug abuse, or mental health information, signed and dated by the patient or legal guardians within the last 90 days, and after the last date of service, must be presented to obtain medical records of this sensitive nature.

Optional; Pennsylvania. The following language is valid only in Florida, but it shown as a specimen. Patient Authorization is not required to be included with a subpoena under Florida law, however notice to the patient is, therefore if possible a patient authorization should be included with all subpoenas. Upon "the issuance of a subpoena from a court of competent jurisdiction" in a civil or criminal action, "and proper notice to the patient or the patient's legal representative" is made by the person seeking the records.

Faxing of Medical Records

Medical records will be faxed only to healthcare providers for continuing medical care. In cases where an authorization is required, it must be obtained prior to the records being faxed. If the

patient is unable to sign an authorization, the physician or allied health practitioner requesting the records will need to document the reason why, and sign their names on the authorization. AIDS/HIV, Alcohol/Drug Abuse, and Mental Health Records should not be faxed. Faxing of records should be minimized as this is a form of unsecured PHI disclosure which can result in the patient and OCR (Office for Civil Rights) needing to be notified in the case of a Privacy Breach.

Selected, Detailed Statutory Requirements

Uses and Disclosures for Disaster Relief Processes

§164.510(b)(4) A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraph (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

The above uses and disclosures apply if:

(2) Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

(3) Limited uses and disclosures when the individual is not present. If the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's.

Public Health Activities and Purposes

§164.512(b)(1) - A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is

acting in collaboration with a public health authority;
(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated products or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:
(a) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
(b) To track FDA-regulated products;
(c) To enable product recalls, repairs, or replacement, or look back (including locating and notifying individuals who have received products that have been, withdrawn, or are the subject of look back); or
(d) To conduct post marketing surveillance;
(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or
(v) An employer, about an individual who is a member of the workforce of the employer, if:
(a) The covered entity is a covered health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer:
(1) To conduct an evaluation relating to medical surveillance of the workplace; or
(2) To evaluate whether the individual has a work-related illness or injury;
(b) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
(c) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and
(d) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:
(1) By giving a copy of the notice to the individual at the time the health care is provided; or
(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

Child Abuse and Neglect

§164.512(c)(1) - Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:
(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
(ii) If the individual agrees to the disclosures; or

(iii) To the extent the disclosure is expressly authorized by status or regulation and:
(a) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
(b) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

§164.512(c)(2) - A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:
(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

Law Enforcement Requests

§164.512(f) - A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.
(1) Pursuant to process and as otherwise required by law. A covered entity may disclose protected health information.
(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or
(ii) In compliance with and as limited by the relevant requirements of:
(a) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
(b) A grand jury subpoena; or
(c) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demands, or similar process authorized under law, provided that:
(1) The information sought is relevant and material to a legitimate law enforcement inquiry;
(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) De-identified information could not reasonably be used.

§164.512(f)(2) - Limited information for identification and location purposes: Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:
(i) The covered entity may disclose only the following information:
(a) Name and address;
(b) Date and place of birth;
(c) Social security number;
(d) ABO blood type and factor; (e)Type of injury;
(f) Date and time of treatment;
(g) Date and time of death, if applicable; and

(h) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purpose of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of blood fluids or tissue.

§164.512(f)(3) - Victims of a crime - Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to a paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosures; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance provided that:

(a) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(b) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(c) The disclosure is in the best interest of the individual as determined by the covered entity, in the exercise of professional judgment.

§164.512(f)(4) - A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicious that such death may have resulted from criminal conduct.

§164.512(f)(5) - Crime on premises - A covered entity may disclose to law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

§164.512(f)(6) - Reporting crime in emergencies (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to law enforcement official if such disclosure appears necessary to alert law enforcement to:

(a) The commission and nature of a crime;

(b) The location of such crime or of the victim(s) of such crime; and

(g) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

Decedents Over 50 Years

1. PHI ceases to be PHI, with no application of privacy and security rules, 50 years after death of the individual to whom the PHI relates.
2. The final rule amended §164.510(b) to permit covered entities to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the CE (or BA).

Immunization Records to Schools

1. Our Organization may disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student.
2. Written authorization will no longer be required to permit this disclosure; our Organization will still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting in loco parentis for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor.
3. If our Organization does provide this information without a written authorization, we must document the agreement obtained under this provision ourselves in writing and this documentation must be kept for the minimum 6 years.

E. Related Polices:

- 6s - Appropriate Access to PHI by Workforce
- 7s - Confidentiality of PHI
- Insert State Specific Policy Requirements: Pennsylvania
- List additional related polices: none

F. Related Forms

- Bs - Security or Privacy Report
- Cs - Investigation and Corrective Actions
- Ns - Breach Determination and Reporting
- AAs - ROI, Breach and Patient Rights Log

G. References

- **Omnibus Privacy Final Rule Modifications**
- 45 CFR 45 CFR 164.502 - 164.514
- 45 CFR 45 CFR 164.502 - 164.514
- § 164.510(b)
- §164.510(b)(2)
- §164.510(b)(4)
- §164.510(b)(4)
- §164.512(c)(1)
- §164.512(c)(2)
- §164.512(d)(1)
- §164.512(f)
- §164.512(f)(2)
- §164.512(f)(3)
- §164.512(f)(4)
- §164.512(f)(5)
- §164.512(f)(6)
- §164.512(k)(1)
- §164.512(l)

- §164.514
- §164.524
- SRA Item Numbers: C.285
- PRA Line Items: C.185, C.15, C.16, C.17, C.195, C.196, C.197, C.45
- List additional references: none

Fax Transmissions

A. Coverage

Home Community Based Services Provider, Inc (hereafter referred to as the 'Organization') workforce members (i.e. employees, contractors and volunteers) who utilize Fax technology for the disclosure of Protected Health Information (PHI).

B. Create / Revision Date

11/28/2021

C. Purpose

Ensure that fax technology is utilized as minimally as possible, and with proper procedures, to maintain PHI Privacy during fax disclosures.

D. Policy

As the facsimile (fax) transmission of information has become common in the health care industry, the Organization has adopted this policy for the control of health information transmittal, which is deemed 'unsecure' by HIPAA Privacy and Security Rules, which means that misdirected faxes are subject to Privacy Breach Notification, which is highly undesirable.

1. Facsimile transmission (fax) of medical records should be limited to use by health care providers for treatment purposes only or upon written request of the patient to receive their PHI via this method. Fax is an inherently 'unsecured' method of communicating patient information (defined as Protected Health Information or 'PHI') and therefore per HIPAA Privacy Rules should be restricted to the minimum possible.
2. Options to fax, such as *secure* e-mails (with encryption according to HIPAA Security Rules) should be utilized, if available, in lieu of faxes.
3. The facsimile transmission of patient information should be sent or received to a device that is manned by authorized health care personnel or designated by the patient in the written request. The device should also be located in a secured area where unauthorized access is avoided.
4. Procedures shall be followed to ensure correct transmission and receipt of faxes by intended recipient are confirmed.
5. A fax cover sheet should always be utilized when faxing patient information outside the Organization that has the following items completed: date, fax telephone number, name of recipient, name of sender, and any appropriate comments regarding the information. The cover sheet should also contain a disclaimer statement and contact information in case the fax is received in error, including the immediate destruction of any information received by wrong recipients due to fax errors.
6. Whenever possible, auto-faxing should be utilized for reduction of human errors in dialing the fax telephone numbers. However, auto fax numbers must be tested and audited regularly to ensure their validity.
7. Records of a privileged nature, as protected by Federal Law and state statutes, (specifically psychiatric, drug/alcohol abuse, AIDS, and AIDS related conditions, and HIV tests and

information), should receive special consideration. Records of this nature should not be faxed except in an extreme emergency.

8. On a regular basis all fax machines with auto-faxing capabilities should be audited for correct numbers and processing of faxes with test results being retained as part of ongoing HIPAA Privacy compliance records.

E. Related Forms

- Fax Cover Sheet

F. Related Polices

- 11s – Disclosure of PHI
- List additional related polices: none

G. References

- PRA Line Item: C.35, L.3, L.4
- List additional references: none

Request for Amendment of PHI

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 supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

11/28/2021

C. Purpose

To communicate the policy of the Organization to recognize the right of an individual to request an amendment or correction to Protected Health Information ("PHI") or a record about a patient in the Organization's 'Designated Record Set', typically the medical records and Business Office records.

D. Policy

HIPAA allows for individuals to request amendment to their PHI, if they are authorized and under certain circumstances according to the Organization's Notice of Privacy Practices (NPP). Generally speaking, the patient's 'Medical Record' (regardless of whether in paper, electronic document management, electronic health record (EHR) or defined hybrid systems) and the 'Business Office Records' (managed within the Financial Systems application) are used to provide for amendment and/or correction requests from individuals. Because these records are compilations and summaries of information from other Source Systems, and are in fact copies of other existing data and document types, they will be primarily offered for individual access and amendment.

An individual must make a request for an amendment in writing. All requests must be submitted on the *'Request for Amendment of Protected Health Information'* form and provide a reason to support the requested amendment. All requests shall be directed to the appropriate staff.

Action on the Request for Amendment

The Organization shall act on the individual's request no later than sixty (60) days after receipt of the request. The Organization may extend the time for action by no more than thirty (30) days. If the thirty (30) day extension is required, the Organization must provide the individual with a written statement, within the sixty (60) day period, denoting the reasons for the delay and the date by which the Organization will complete its action on the request. The Organization may have only one such thirty (30) day extension.

The Organization may accept or deny the amendment. Determinations of whether to accept or deny the request for the amendment will be made by the Organization's Privacy Officer following a review

of the relevant record and Designated Record Set, consultation with the treating physician and/or author of the entry requested to be amended, evaluation of the individual's request, and to the extent appropriate, other health professionals familiar with the patient's course of treatment.

Acceptance of the Amendment

If the Organization accepts the Amendment the Organization will make the appropriate amendment to the PHI or record that is the subject of the request for amendment by identifying the records in the Designated Record Set that are affected by the Amendment and appending or otherwise providing a link to the location of the Amendment.

The amendment to the PHI may be in the form of an addendum, which would be placed in the record, or an actual change to the documentation in the record. The addendum should be completed by the individual making the original entry and should be located in the same proximity as the original entry. The addendum should be clear, concise, and reflect the problem with the original record entry. Electronic record systems should appropriately document the reason for the Amendment, the party that has created the Amendment and index the information so that it can be readily accessed by authorized users.

For correction of a paper record entry (which is to be utilized only in clear circumstances as opposed to amendments which are favored), a single line should be drawn through the incorrect information, corrected entry documented, dated, and initialed by the individual making the correction. Corrections for electronic records should be accompanied by audit log entries that document the changes (prior to and after the correction) and the ability to see data or document versions (prior to and after the correction versions) after the correction(s) is made.

The Organization will timely inform the individual in writing that the Amendment has been accepted and obtain the individual's identification of and agreement to have the Organization notify the relevant persons with which the Amendment needs to be shared.

The Organization will make reasonable efforts to inform and provide the Amendment within a reasonable time to (a) persons identified by the individual as having received PHI about the individual and requiring the Amendment; and (b) persons, including Business Associates of the Organization, that the Organization knows has PHI that is the subject of the Amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

Denial of the Amendment

If the Organization denies the amendment in whole or in part, the Organization will provide the individual who requested the amendment with a written denial within sixty (60) days after receipt of the Request for Amendment. The denial will use plain language and contain:

1. One of the following reasons for the denial if the PHI:
    a. Was not created by the Organization, unless the individual provided a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
    b. Is not part of the Designated Record Set;

   c. Would not be available for inspection (i.e. psychotherapy notes, information compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding, and certain PHI maintained by the Organization that are subject to portions of CLIA relating to laboratory certification and operations or that are exempt from CLIA) or
   d. Is accurate and complete.
2. A statement of the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
3. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the Organization provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
4. A description of how the individual may complain to the Organization pursuant to the complaint procedures established as part of HIPAA or to the Secretary of the U.S. Department of Health and Human Services. The description must include the name, or title and telephone number of the Organization's Privacy Officer.

For partial denials, the denial notice will explain what portion of the amendment will be granted and what portion will be denied. The notice will also explain how the patient may contact the Organization if he or she wishes the Organization to make the partial amendment. The partial amendment may not be made without the patient's permission. If permission is granted, then the record will be amended / corrected in the manner as outlined in the 'Acceptance of the Amendment' section of this policy. The Organization will permit the individual to submit to the Organization a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

The Organization will prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the Organization will provide a copy to the individual who submitted the statement of disagreement.

The Organization will, as appropriate, identify the record of PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individuals request for an amendment, the Organization's denial of the request, the individual's statement of disagreement, if any, and the Organization's rebuttal, if any, to the designated record set.

Future Disclosures

1. If a statement of disagreement has been submitted by the individual, the Organization will include the material appended, or at the election of the Organization, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.
2. If the individual has not submitted a written statement of disagreement, the Organization must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.
3. When a subsequent disclosure as described above is made using a standard transaction and the standard transaction or code set does not permit the additional material to be included with the disclosure, the Organization may separately transmit the material required to the recipient of the standard transaction.

If the Organization is informed by another Covered Entity of an amendment to an individual's PHI, the Organization will amend the PHI in appropriate designated record sets as provided in this policy.

The Organization will retain all documentation associated with requests for amendments (and the associated determinations) for the longer of:

1. Six (6) years from the date of its creation; or
2. The last effective date of the relevant documents. All such documentation shall be maintained by the Organization's Privacy Officer and in the individual's medical record. All documentation must identify the titles of the persons or offices receiving and processing requests.

E. Definitions

Amendment
A formal statement of revision of or change to protected health information added to a Designated Record Set, near but not replacing the original documentation. Amendments can be created for both paper and electronic records.

Correction

A revision to the original designated record set documentation, for either paper or electronic records.

Designated Record Set

Designated Record Set is defined as a group of records maintained by or for a Covered Entity that is;

1. The medical and billing records about individuals maintained by or for a covered healthcare provider. These records are the primary source of Designated Record Set records for the Organization accessible by patients for copying, inspection and amendment and include medical records, Business Office records, documents, and reports.
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan.
3. Information used in whole or in part by or for the Covered Entity to make decisions about individuals

Protected Health Information (PHI)

Any information whether oral, written, electronic or recorded in any form that is created or received by the Organization as a healthcare provider and relates to an individual's past, present or future physical or mental condition; healthcare treatment and payment for services. PHI also includes data that identify the individual (i.e. Name, SSN, MRN, account number, address, telephone number, DOB, e-mail address, names of relatives, employer, etc).

TPO

According to HIPAA the acronym 'TPO' refers to PHI collected, stored and utilized for Treatment, Payment, and Operations.

F. Related Procedures

- List of Designated Record Set systems: Google Documents
- List how to perform amendments and corrections in electronic systems: Request sent to CEO, administration team to review request, if appropriate changes will be made with documentation
- List how to link forward amendments and corrections for future related disclosures: Request sent to CEO, administration team to review request, if appropriate changes will be made with documentation

G. Related Forms

- Gs - Request for Patient's Rights
- Hs - Denial of Amendment or Restrictions Form
- AAs - ROI, Breach and Patient Rights Log
- List additional related forms: none

H. Related Polices

- 9s - Designated Record Set
- 19as - HIPAA Privacy and Security Compliance Program Master Policy
- List additional related polices: none

I. References

- Stericycle Online Privacy Risk Assessment (PRA)
- Title 45, Code of Federal Regulations, Parts 160 and 164
- §164.524(e)
- §164.526
- PRA Line Item: C.24
- List additional references: none

Restrictions on Certain Disclosures of Health Information

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 supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

11/28/2021

C. Purpose

To define the process by which an individual can restrict the subsequent disclosure of certain PHI (Protected Health Information) for payment and operations.

D. Policy

Section 164.522(a) of the Privacy Rule requires Covered Entities to permit individuals to request that a Covered Entity restrict uses or disclosures of their protected health information for treatment, payment, and health care operations purposes, as well as for disclosures to family members and certain others permitted under § 164.510(b).

In the case that an individual requests that a Covered Entity restrict the disclosure of the protected health information of the individual, the Covered Entity must comply with the requested restriction if—

1. Except as otherwise required by Law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); *and*
2. The protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

Individuals requesting restrictions to the disclosure of their PHI must submit a written request form. Written requests should only be accepted after an individual pays the entire balance of the billing for the service or item for which restriction for payment or operations is requested. The Covered Entity should discuss the process with the individual requesting the restriction so that they clearly understand the requirement of having the item or service paid for out of pocket and at $0 balance before this restriction request must be honored.

HIPAA does not require the Organization to agree to a restriction requested by an individual except in limited cases where the item or service has been paid out of pocket and in full; any acceptance by Organization to agree to a restriction will only consider the addition of restrictions on disclosure in very limited circumstances as determined on a case-by-case basis.

Exceptions to Restrictions

If in the event Organization has agreed to restrict the use or disclosure of PHI, Provider shall not use or disclose the restricted PHI in violation of such restriction except that:

1. To facilitate treatment; and
2. Organization may use or disclose restricted PHI, if such use or disclosure is permitted or required under Organization policies relative to research and patient registries.

Terminating a Restriction

If Organization has agreed to restrict the use or disclosure of PHI, Organization may terminate its agreement to restrict its use or disclosure of such PHI if:

1. The individual agrees to or requests the termination in writing;
2. Organization informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI about the individual created or received after Organization has so informed the individual;
3. Organization discovers the agreement for restriction of use or disclosure for payment or operations for item or service paid out of pocket by an individual was not actually completely paid to a zero balance for that item or service.

Organization shall document any restriction in the patient's medical record and such restriction will also be documented in the appropriate tracking system. Organization shall maintain such documentation for six (6) years from the date when the restriction was last in effect.

Agreement to Restriction Exception for Emergency Treatment

A Covered Entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual. (iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

Downstream Notice of Restrictions

This Organization is only required to maintain restrictions to the uses or disclosures of PHI under regulatory requirements or as agreed upon with the individual to whom the PHI applies. This Organization does not have a responsibility to notify other providers of care on legitimate uses of the PHI about the restrictions, that being solely the individual's responsibility. This Organization will engage in open dialogue with individuals to ensure that they are aware that previously restricted PHI may be disclosed to the health plan unless they request an additional restriction and pay out of

pocket for the follow-up care.

Exception for Medicare and Medicaid

There is an exception to the right of restriction such as mandatory claim submission provisions under Medicare and similar requirements under Medicaid.

E. Related Forms

- Gs -- Request for Patient's Rights
- Hs – Denial of Amendment or Restrictions
- AAs – Release of Information, Breach and Patient Rights Log
- List additional related forms: none

F. Related Polices

- 10 -- Individual Access to PHI
- 11s -- Disclosure of PHI
- 19as – HIPAA Privacy and Security Compliance Program Master Policy
- List additional related polices: none

G. References

- ARRA / HITECH Act February 17, 2009 SEC. 13405
- Omnibus Privacy Final Rule, January 2013
- §164.522(a)(2)
- §164.522(a)(3)
- §164.522(a)(1)(i)
- Stericycle Online Privacy Risk Assessment (PRA)
- PRA Line Item: C.25
- List additional references: none

Accounting of Disclosures (HIPAA)

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

11/28/2021

C. Purpose

To define the policy for creating a HIPAA Accounting of Disclosures for patients who make a request.

D. Policy

The Organization will provide an accounting of how an individual's PHI (Protected Health Information) has been disclosed outside of the facility for the past six (6) years (accounting time period to commence on April 14, 2003, or after). The requestor will receive response within a specified time period, and will be notified in writing if there is a delay. All documentation related to the accounting will be retained by HIM.

The accounting must provide the patient with the following information for each disclosure: the date, the name of the person or organization that received the information, his or her address (if known), a brief description of the PHI disclosed, and a brief statement explaining the purpose of the disclosure.

Disclosures excluded from an Accounting of Disclosures (AOD)

1. Disclosures made for treatment, payment, and healthcare operations;
2. Disclosures made to the patient;
3. Disclosures authorized by the patient
4. Disclosures made for the Organization patient directory;
5. Disclosures made to persons involved in the patient's care;
6. Disclosures made for National Security or Intelligence purposes;
7. Disclosures to correctional institutions or law enforcement officials for patients who were imprisoned or in police custody;
8. Disclosures made prior to April 14, 2003;
9. Disclosures that do not identify individual patients;
10. Disclosures that are part of a Limited Data Set;
11. Disclosures that are incidental to another permitted use or disclosure.

Disclosures that must be included in an AOD

All disclosures of PHI that are not for Treatment, Payment or (delivery of healthcare) Operations and;

HIM based Disclosures - These disclosures, typically managed by the HIM department, must be tracked:

1. Subpoenas
2. Law enforcement requests
3. Court orders
4. State required reporting from medical records
5. Birth certificates
6. Insurance company reviews
7. Other external reviewers that are not TPO (RAC is TPO)
8. State Department of Health for medical record requests
9. Joint Commission
10. NB Screening Program

Non-HIM based Disclosures - These must be tracked whether the disclosure was verbally, electronically or in paper:

1. Suspected domestic and child violence and abuse reporting
2. Incident reporting to outside entities
3. Government discharge reporting
4. Other planning databases and reporting
5. Disclosures by Business Associates that are not for TPO
6. Underage pregnancy reporting
7. Communicable disease reporting
8. Research disclosures, research disclosures under IRB or Privacy Board waiver
9. Disclosures made for research unless authorized by the patient or his legal representative.
10. Disclosures made to government agencies
11. Disclosures to law enforcement
12. Public Health Agencies
13. Health oversight agencies
14. State neonatal reporting
15. Birth defects registry
16. Cancer registry
17. Trauma registry
18. Death registry
19. Poison control
20. County medical examiner
21. Disclosures to funeral homes
22. Reporting to the FDA, CDC, DEA, EPA, OSHA, FEMA, NTSB, DOJ, etc.
23. Disclosures made by BAs for non-TPO purposes
24. Organ procurement

INCLUSIONS

Disclosures of PHI for any of the following activities, purposes, and reporting requirements, including any documentation relating to such disclosures, are subject to HIPAA's accounting of disclosures

requirement. These disclosures must be tracked and available for inclusion in an accounting of disclosures within the medical record.

Disclosures to Public Health Authorities

- For public health surveillance activities (tracking infectious diseases)
- For public health investigations
- For public health interventions (e.g., actions taken to limit health authorities; for example, with China, to track and limit the spread of SARS)
- Birth records reporting
- Death records reporting
- Elder abuse/neglect reporting
- Teen suicide reporting
- Patient safety reporting (such as to a state department of health)
- To prevent serious harm (needle stick reporting)
- Communicable disease reporting

Disclosures to Food & Drug Administration

- Reporting of adverse events, product defects, or biological product deviations
- To track products
- To enable product recalls, repairs, or replacements
- To conduct post-marketing surveillance
- To manufacturers of defective products

Disclosures to Employers

- To employer requesting health care be provided to an employee when made without the employee's authorization for medical surveillance purposes, in relation to a work related injury or illness, and needed for the employer to comply with OSHA, the Mine Safety and Health Administration (MSHA), or similar state law

Disclosures to Health Oversight Agencies

- Required reporting to government benefit programs (such as Medicare, Medicaid)
- Compliance activities (such as compliance with government benefit programs)
- Required by civil rights laws
- Reporting to trauma registry
- Reporting to tumor registry
- Vital statistics reporting
- Alzheimer's and other dementia reporting
- Disclosures in judicial and administrative proceedings

- In response to a court order
- In response to a subpoena

Disclosures to Law Enforcement

- As required by law
- In response to court order, court ordered warrant, subpoena, or summons
- In response to an administrative request
- For purposes of locating a suspect, fugitive, material witness, or missing person
- During emergency treatment, crime is elsewhere
- About crime victims
- About crimes on the health care organization's premises
- About suspicious deaths (suspected homicide or suicide)
- To avert a serious threat to health or safety (of an individual or the public)

Disclosures Regarding Deceased Persons

- To coroner or medical examiner
- To funeral directors
- For organ, eye, or tissue donation/procurement purposes

Disclosures for Research Purposes

- When an institutional review board waiver is used in place of a patient authorization to release PHI
- In reviews preparatory to research
- In research on decedent's information

Disclosures for Specialized Government Functions

- For military and veterans activities
- To protective services
- To department of state related to medical suitability (for example, an individual's PHI may be disclosed to determine if she is available to serve overseas)
- By government programs providing public benefits
- About foreign military personnel to appropriate foreign military authority

Disclosures for Worker's Compensation Purposes

- To comply with existing laws (see state law)

- To state health data commission (unless operations)
- To U.S. embassies
- To contractors and business associates (if not for treatment, payment, or healthcare operations)
- To vendors (if not for treatment, payment, or healthcare operations)

EXCEPTIONS

The following are the exceptions to the accounting requirement. You may include these types of disclosures of PHI in an accounting of disclosures, but you are not required to do so:

- To carry out treatment, payment, and health care operations
- To individuals, of PHI about them
- Incident to a permissible use or disclosure of PHI
- In response to a HIPAA-compliant patient authorization
- For the facility's directory or to persons involved in the individual's care or other notification purposes
- To correctional institutions or law enforcement officials
- Occurring before the HIPAA compliance date for the covered organization (April 14, 2003, for most organizations or April 14, 2004, for small health plans)
- As part of a limited data set

Timeframe for AOD

The Organization will reply in writing to a request for Accounting of Disclosures within 60 days by either providing the requested information or a letter explaining the reasons for delay that specifies the date by which the information will be provided (no longer than an additional 30 days). No further delays are allowed under federal law.

ARRA AOD Laws

The 2009 ARRA law (and subsequent regulations) substantially changes HIPAA's AOD requirements, however depending upon whether Covered Entities (CEs) had an Electronic Health Record (EHR) in place prior to January 1, 2009; these regulations do not take effect until either January 1, 2011 or 2014.

AOD Table Example

Date of Disclosure	Person or Organization Receiving PHI	Address Where Disclosed (if known)	Brief Description of PHI Disclosed	Brief Reason for Disclosure

E. Related Polices

- 2s -- Documentation for Security and Privacy Compliance
- List additional related polices: none

F. Related Forms

- Gs – Request for Patient's Rights Form
- AAs – Release of Information, Breach and Patient Rights Log
- List additional related forms: none

G. References

- CFR Title 45 Sub-Title A HHS Part 164 Privacy & Security §164.528
- CFR §164.506, §164.502, §164.508, §164.512, §164.514
- Analysis of Health Care Confidentiality, Privacy and Security Provisions of ARRA 2009 March 2009 – AHIMA
- Developing a Plan of Action – How to Conduct an Accounting of Disclosures – AHIMA article – Susan Stuard – 07/02/03
- Calculating Costs for Accounting of Disclosures Journal of AHIMA 74, no.5 (May 2003): 65-66 – Rose Dunn
- Uncovering the Impact of HIPAA's Accounting of Disclosures on Healthcare Providers AHIMA - Fred Schade and Matthew Cottrell
- Stericycle Online Privacy Risk Assessment (PRA)
- PRA Line Item: C.26, K.13
- List additional references: none

H. Reference Text

Calculating Costs for Accounting of Disclosures – AHIMA – Rose Dunn

The Privacy Rule allows a CE to charge a cost-based fee for providing an Accounting of Disclosure (AOD). The balance struck by HHS with regard to cost was to grant the individual a right to an accounting once a year without charge. The covered entity may impose reasonable, cost-based fees for any subsequent requests during the one-year period.

HHS clarifies that the CE may recoup its reasonable retrieval and report preparation costs as well as any mailing costs incurred in responding to subsequent requests. The Privacy Rule requires that

individuals be notified in advance of these fees and provided an opportunity to withdraw or amend a request for a subsequent accounting to avoid incurring excessive fees.

Setting Fees

The Privacy Rule allows a CE to charge a fee for providing copies of medical records and providing an AOD. However, calculating the cost for an AOD as permitted in 164.528 (c)(2) differs from calculating the cost for copying and related supplies provided for in 164.524 (c)(4). For example, in 164.528(c)(2):

1. The CE cannot charge for first request for an AOD during any 12-month period but can charge for copies of medical records each time a request is received
2. The fee charged for the AOD covers the entire process including preparation, while the fee charged for copies of medical records is limited to labor and supplies directly related to copying rather than the total release of information process

Accounting for Disclosure Cost Analysis Worksheet Labor Components

1. Review and verify the request for the Accounting of Disclosure including confirming whether the request is “initial” or “repeat” within the same year. Discuss the purpose and content limitations of the accounting, availability, whether the patient wishes to have the report mailed or picked up, the accounting fee, and, if applicable, postage required and state sales tax
2. Log request
3. Find the patient in the Master Patient Index
4. Determine where accounting information is maintained:
   - Are disclosures maintained in the patient record?
   - Are disclosures maintained in a database?
   - Must calls be made to various departments to capture disclosures?
   - All of the above?
5. Determine the locations of the records
6. Determine disclosure locations to research
7. Pull records
8. Research databases for disclosures
9. Poll other disclosure locations
10. Prepare inventory of disclosures in a format established by the organization; copy requests if appropriate
11. If this is a repeat request, prepare an invoice. If applicable, capture mailing costs
12. Contact the patient regarding the accounting’s availability and, if applicable, the fee required
13. Annotate log to indicate that request has been prepared. File a copy in the designated location
14. Annotate log with release date of accounting to patient and, if applicable, fee received
15. If applicable, deposit fees received
16. Conduct time studies or prepare estimates of time to perform the above.

Non-labor Expenses

1. Space (including utilities) to house staff and equipment to perform the Accounting of Disclosure
2. Furnishings
3. Benefits and payroll taxes of staff performing this function
4. Administrative overhead overseeing this function
5. Other applicable overhead
6. Consulting and professional guidance (for example, legal, accounting, consulting)
7. Liability insurance
8. Copy machine maintenance and supplies (if copies are prepared)
9. Consumable supplies used: paper, staples, envelopes, etc.
10. Printer maintenance and supplies
11. Software license and annual maintenance
12. PC maintenance
13. MPI system maintenance
14. Depreciation expense on items owned by the entity for this function
15. Telephone
16. Education
17. Reference manuals

List additional references: none

Audit Controls, Access and Privacy 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

11/28/2021

C. Purpose

To define the policy for on-going audit controls, as well as privacy and security auditing measures to identify suspicious activity and/or breaches of information and monitoring functions as a deterrent to workforce members from seeking inappropriate access to PHI/ePHI.

D. Policy

An ongoing audit, monitoring and evaluation process is critical in detecting noncompliance and improving the quality of work, and ultimately helps ensure the success of the Organization's privacy program. Audit controls will be utilized in various ways to ensure compliance with regulations and this Organization's policies and procedures. In furtherance of its obligations as a Covered Entity (CE) or Business Associate (BA) that manages protected health information, this Organization will perform internal audits and ongoing monitoring to measure compliance and provide feedback in areas that are found to need continued work. This ongoing audit, monitoring and evaluation process will include the following:

1. Regular audits of compliance with the Organization's privacy policies and procedures, to be conducted or directed by the Privacy and Security Officer(s) and appropriate oversight committees.
2. Special audits focusing on access to electronic records that contain PHI;
3. Audits of BAs and their Privacy Practices, Polices and Procedures.
4. Perform regular activity reviews, including various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports. The goal of Information Technology activity review is to prevent, detect, contain, and correct security and / or privacy violations and threats to individually identifiable health information, whether in electronic or any other forms. All information system activity review audits and monitors are routinely performed and documented.

The audits, monitoring and reviews will focus on the Organization's compliance with specific rules and areas that have been the focus of particular attention on the part of the Federal Office for Civil Rights (OCR), which enforces HIPAA, include the name of state agencies if applicable. The Privacy and Security Officer(s) shall supervise all auditing and monitoring under privacy and security compliance programs. The Organization recognizes that privacy and security are intertwined and

co-dependent, resulting in an interdepartmental, enterprise-wide approach to both privacy and security compliance programs, policies and procedures. Additionally, the Privacy and Security Officer(s) shall maintain all reports, documents and written materials created by the ongoing monitoring, including reports of suspected noncompliance.

Techniques

Audit techniques may include, but are not limited to:

1. Personnel interviews.
2. General questionnaires submitted to Employees and Contractors;
3. Reviews of OCR Privacy and / or Security complaints;
4. Other Electronic Health Record (EHR) system audit log monitoring for unauthorized PHI access, use or disclosure.
5. Request and review all BA records to ensure privacy and security compliance per Business Associate Agreement (BAA)
6. List additional audit techniques as implemented

Operational Privacy and Security Monitor and Audit Topics

The topics of operational privacy and security monitoring audits can vary according to perceived needs, complaints or routine proactive vigilance. Below are a list of topics that can be audited for Privacy. Each audit requires its own design and configuration according to the Organization's policies and procedures. Newer HIPAA topics such as Breach Determination and Notification should be factored into current audit plans.

1. Individual (Patient) Rights
    a. *Notice of Privacy Practices* form completion at Pre-registration or Registration and follow-up on changes or restrictions documented
        i. NPP posted
    b. Patient access to their own (or otherwise authorized) PHI
        i. Properly completed authorization(s)
        ii. Proper ID and supporting documentation presented
        iii. Electronic record access for individuals (patients)
        iv. Electronic record mandated copies for individuals (patients)
    c. Patient Amendment to PHI
        i. Properly executed form
        ii. Physician notification process followed
        iii. Denial / Rebuttal process
        iv. Confirm requested elements amended as requested (if allowed)
    d. Restrictions on PHI use being followed (patients can request and must be granted certain restrictions, there are fewer options not to provide restrictions by the CE)
        i. Flags set for notification within Registration and other electronic systems to notify workforce members of restrictions
        ii. Securing disclosures of PHI in response to restrictions processes being followed
    e. Accounting of Disclosures
        i. TPO (Treatment, Payment and Operations) disclosures must be tracked

starting in either 2011 or 2014 dependent upon implementation of an EHR prior to January 1, 2009.

2. Privacy Event and Determination Investigations
    a. Completion of appropriate forms and logs for Privacy Events
    b. Proper Privacy Event and Privacy Violation (Breach Determination) procedures followed
    c. Proper individual (patient), Organization and OCR notifications
3. Workforce Member Privacy Training
    a. Training on Privacy procedures being followed, at new hire (volunteer or other) orientation
    b. Routine, periodic Privacy training being accomplished on schedule and with correct materials
4. Workforce Member PHI Use, Access and Disclosure
    a. Login attempts and Logins, with locations if possible
    b. Is access level to PHI in electronic systems appropriate? (examples below):
        i. Users who accessed a defined patient
        ii. Access by device
        iii. All patients accessed by a defined user
        iv. Access to defined user / patient
        v. All access for a period of time
        vi. Access by application
        vii. Same last name match user / patient
        viii. Same street match user / patient
        ix. Patients and CE employee match
        x. User / patient location match
        xi. Discharged patients
        xii. Patient Provider match
        xiii. Excessive session duration match
        xiv. VIP / Confidential match
        xv. Total time per device / application
    c. Was access to systems (de-provisioning) with PHI removed within 1 day?
    d. Were devices containing PHI returned to the Organization within 1 day of termination?
        i. Are appropriate records kept for these activities?
    e. Are print permissions appropriate?
        i. Print copies by user
        ii. Print times by user
        iii. User printing by devices
        iv. Actual documents printed
    f. Audit log reviews of PHI access, use and disclosure
    g. Release of Information logs and appropriate disclosure of PHI by workforce members
    h. Secure messaging / email disclosure audits
    i. Electronic copies for disclosure audits, who, what, when, and to which requesting parties
    j. Fax logs and misdirected fax detection
    k. Auto fax number integrity
5. Fields that are helpful to capture for privacy and security auditing (both manual and automated). This is by no means an all encompassing list, rather suggestions for minimum audit capabilities.
    a. Account number
    b. EMPI number
    c. Medical Record number
    d. Confidential patient flag

e. Discharge Date
f. Employee Department
g. Employee Match
h. Facility
i. Guarantor Name
j. Location Match
k. Menu, Pt. Address
l. Pt. Address (additional)
m. Patient Location
n. Patient Name
o. Patient Zip Code
p. Procedure
q. Provider Match
r. Session Start Date and Time
s. Session Stop Date and Time
t. Print by user and device

Documentation of Privacy Compliance Efforts

The Organization documents its efforts to comply with applicable statutes, regulations, guidelines and Federal and State healthcare privacy and security program requirements. For example, when the Organization, in its efforts to comply with a particular statute, regulation, guideline, or program requirement, requests advice from a government agency, including OCR, the Organization shall document and maintain a record of the request and any written or oral response. Additionally, the Organization shall maintain a log of all inquiries between its workforce members and any third parties, as well as any records relevant to issues where the Organization relies upon the reasonableness of any responses it receives from a State or Federal Healthcare privacy or security program or agency. This procedure is extremely important for the Organization in order for it to rely upon such responses and to guide it in future decisions, actions or appeals.

Privacy and Security Officer Function

The Privacy and / or Security Officer(s), or their designee, shall record the information necessary to conduct an appropriate investigation of all privacy and security complaints.

Reprisal/Retaliation Prohibited

Any threat of reprisal against a person who acts pursuant to his or her responsibilities in relation to privacy and security laws, rules, and regulations is not only against the Organization's policy, it may in some instances be a violation of the law. Reprisal, if proven, shall be subject to appropriate disciplinary action.

False Reports/Discipline

It is the policy of the Organization that no workforce member will be punished solely on the basis that they reported what was reasonably believed to be an act of wrongdoing or a violation of privacy or security. However, a workforce member will be subject to disciplinary action if the Organization reasonably concludes that the workforce member knowingly made a false allegation, or knowingly distorted, exaggerated, or minimized an incident to either injure someone else or to protect the workforce member or others. Any attempt to harm or slander another person through false accusations, malicious rumors, or other irresponsible actions is a violation of the Organization's policy.

Anonymity

The Organization, at the request of a reporting workforce member, shall provide anonymity to the workforce member who reports the privacy or security event or suspected Violation as is possible under the circumstances in the judgment of the Privacy or Security Officer, consistent with the Organization's obligation to investigate concerns and take necessary corrective action.

Admissions of Wrongdoing

An admission of personal wrongdoing will not guarantee that a workforce member will be protected from disciplinary action. The weight to be given to the admission in determining whether a workforce member will be disciplined will depend on all the facts known to the Organization at the time. An admission of wrongdoing will be taken into account if the Organization was not previously aware of the reporting workforce member's conduct, or its discovery was not imminent, and if the admission was complete and truthful.

E. Related procedures

- Insert appropriate procedures and descriptions of technologies used for auditing and monitoring: reports to be reviewed during quality management assesment

F. Related Policies

- 6s - Appropriate Access to PHI by Workforce
- Mitigation for Improper Use or Disclosure of PHI
- 26s - Sanctions, Enforcement and Discipline
- 106s - Login Monitoring
- List additional related policies: none

G. References

- Title 45, Code of Federal Regulations, Parts 160 and 164, August 14, 2002.
- 45 CFR 164.524, §164.312(b)
- 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule
- Stericycle Online Security Risk Assessment (SRA)

- SRA Line Item Numbers: B14, B15, B16, B22, B33, B42, B43, B65, B96, C2, D5, D17,D18, D19, D20
- List additional references: none

Use and Disclosure of PHI for Marketing, Fundraising and Sale

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 supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

11/28/2021

C. Purpose

To communicate policy of the Organization in accordance with the final HIPAA Omnibus Privacy Rule regarding use and disclosure of PHI for marketing, fundraising and the sale of Protected Health Information.

D. Policy

This Organization abides by all HIPAA and State privacy regulations regarding the use of individual (patient) PHI for marketing, fundraising or sale. In general, individual authorization is required before any of these uses of his/her PHI.

Marketing

It is the policy of the Organization and the Organization's entities not to use or disclose PHI about an individual for marketing purposes without first obtaining the individual's written authorization except as noted within this policy.

The Omnibus Final Rule significantly modifies the approach to marketing by requiring authorization for all treatment and health care operations communications where the Covered Entity receives financial remuneration for making the communications from a third party whose product or service is being marketed. For example, a device manufacturer cannot pay for marketing of that device to patients without their authorization.

Under the Omnibus Final Rule, for marketing communications that involve financial remuneration, the Covered Entity must obtain a valid authorization from the individual before using or disclosing protected health information for such purposes, and such authorization must disclose the fact that the Covered Entity is receiving financial remuneration from a third party.

There continues to be a stand-alone exception for prescription refill reminders and certain drugs and biologics.

Fundraising

A Covered Entity may use, or disclose to a Business Associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without patient authorization.

- Demographic information relating to an individual.
  - The Omnibus Final Rule addresses the scope of demographic information relating to an individual includes names, addresses, other contact information, age, gender, insurance status and dates of birth.
- Dates of health care provided to an individual.
- Omnibus Final Rule added to the categories of PHI that may be disclosed
  - Department of Service information (e.g., cardiology, pediatrics)
  - Treating physician information
  - Outcome information (e.g., sub-optimal results and death of patient)

The Covered Entity may NOT use or disclose protected health information for fundraising purposes as otherwise permitted unless a statement required by §164.520(b)(1)(iii)(B) is included in the Covered Entity's *Notice of Privacy Practices*;

1. The Covered Entity must include in any fundraising materials it sends to an individual under this provision a description of how the individual may opt out of receiving any further fundraising communications.
2. The Covered Entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

There also may be state laws, rules or regulations to consider in reference to the definition and execution of marketing programs.

The Omnibus Final Rule does not modify the types of communications that are currently considered to be for fundraising purposes.

- A communication to an individual that is made by a Covered Entity, an institutionally related foundation, or a Business Associate on behalf of the Covered Entity for the purpose of raising funds for the Covered Entity is a fundraising communication.
- Permissible fundraising activities include appeals for money, sponsorship of events, etc.
- They do not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc.).

Sale of PHI

The Final Rule defines “sale of protected health information” as a disclosure of PHI by a Covered Entity (CE) or Business Associate (BA), if applicable, where the CE or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

A sale of PHI occurs when the CE or BA primarily is being compensated to supply data it maintains in its role as a CE or BA. Such disclosures require the individual’s authorization unless they otherwise fall within an exception.

The Final Rule permits the same types of costs under this exception as the research exception; as well as costs that are in compliance with a fee schedule provided by State law or otherwise expressly permitted by other applicable law. Thus, costs may include the direct and indirect costs to prepare and transmit the data, including labor, materials, and supplies, (but not profit margin).

Exceptions / Exclusions:

- General exception permitting a CE to receive remuneration in the form of a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for any disclosure otherwise permitted by the Privacy Rule.
- Grants, sponsors and research use of PHI may be excepted, complex rules.
- HIEs where members pay fees, which supports the service of the HIE, not the sale of 'data'.
- Disclosures for public health purpose (definition of 'cost based' in the rule is quite complex; remuneration for public health activities is not required to be cost-based)
- Disclosures for research purposes are excepted from the remuneration prohibition to the extent that the only remuneration received by the CE or BA is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes.
- There is an exception for remuneration paid by a CE to a BA for activities performed on behalf of a CE.
- The prohibition on sale of PHI without patient authorization applies to the receipt of nonfinancial as well as financial benefits.

E. References

- Omnibus Privacy Final Rule – published January 2013.
- §164.508:
- §164.514(f)
- §164.520(b)(1)(iii)(B)
- Stericycle Online Privacy Risk Assessment (PRA)
- PRA Line Item: C33
- List additional references: none

HIPAA Privacy and Security Compliance Program Master Policy

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 supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

11/28/2021

C. Purpose

This policy establishes a Privacy and Security Compliance Program, including a reporting and accountability structure, in order to facilitate compliance with federal and state privacy laws and security regulations.

D. Policy

The Security Officer shall be accountable for the Organization's electronic Personal Health Information compliance, ensuring data and hardware, mobile device, network, software, back-ups and device security. The Privacy Officer is responsible for providing direction and oversight of the processes that impact confidentiality and related safeguards of patient data, as well as, rights afforded under HIPAA. This person (or persons) will develop, implement, monitor and maintain the Organization's program of compliance concerning the privacy of and access to patient health information as designated by HIPAA.

In smaller organizations the Privacy and Security Officer can be the same person. These Officers will be established at the direction of the CEO/Board of Directors or their designee.

The HIPAA Privacy and Security Officers duties include:

- Manage all HIPAA-related compliance activities.
- Develop, implement and maintain appropriate privacy- and security-related policies and procedures.
- Conduct various risk assessments, as needed or required.
- Manage HIPAA violation and breach notification investigations, determinations, and responses, including breach notifications.
- Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.
- Ensure consistent application of sanctions for failure to comply with privacy policies for all individuals in the Organization's workforce, in cooperation with Human Resources, the information Security Officer, Administration, and Legal.
- Administer patient requests related to Patient Rights as designated by HIPAA Privacy regulations.
- Administer the process for receiving, documenting, tracking, investigating, and taking action

on all privacy complaints in conjunction with HR, other Compliance Officers and legal counsel.

- Cooperate with HHS and its Office for Civil Rights, other legal entities, and Organization officers in any compliance reviews or investigations.
- Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- Conduct periodic privacy audits and take remedial action as necessary.
- Remediate and mitigate discovered privacy and security violations according to Organizational policy.
- Provide for uniform enforcement of sanctions brought on by privacy or security violations.
- Oversee employee training in the areas of information privacy and security.
- Deter retaliation against individuals (patients) who seek to enforce their own privacy rights or those of others.
- Remain current and advise on new technologies to protect data privacy.
- Remain current in reference to laws, rules and regulations regarding security and privacy, updating the Organization's policies and procedures as necessary.
- Anticipate patient or consumer concerns about our use of their confidential information, and develop policies and procedures to respond to those concerns.
- Ensure Business Associates, (or if a BA) Sub-contractors have necessary privacy and security compliance programs. Ensure Business Associate Agreements (or Sub-contractors agreements if a BA) are in place, monitored and enforced.
- Ensure Group Health Plans and Memorandums of Understanding (MOUs) with government entities are compliant with HIPAA and afford the highest levels of protections.

The Organization will fully document all HIPAA compliance-related activities and efforts, in accordance with appropriate policies. All HIPAA compliance related investigation documentation will be retained for at least the timeframe required by regulation from the date of creation or last revision, whichever is later and in accordance with the Organization's Document Retention policy.

The Security Compliance Program is governed by a structure that fosters Organization wide workforce participation to support ongoing compliance with regulatory requirements.

1. Security and Privacy Compliance Program governance and staffing shall be defined and appointed by the CEO/Board of Directors or their designee
    a. Organizational stakeholders involved in Privacy and Security Compliance Program governance shall represent be represented by management staff including, but not limited to:
        i. Administration
        ii. Security Officer
        iii. Privacy Officer
        iv. Senior Corporate Compliance Officer
        v. Health Information Management
        vi. Risk Management
        vii. Medical Staff Services
        viii. Information Systems
        ix. Nursing
        x. Human Resources
        xi. List others as applicable
2. Organizational governance of the Privacy and Security Compliance Program shall undertake, but not be limited to:

a. Meeting on a regular basis and as needed for urgent events.
b. Having established procedures for recording of meeting minutes.
c. Providing guidelines for implementation of security (and related privacy) compliance policies and procedures in accordance with federal and state laws, regulations, and accreditation standards.
d. Communication and propagation of privacy and security compliance policies and procedures.
e. Establishing procedures, guidelines, tools, reports, to monitor compliance with Privacy and Security Compliance Program policies and procedures.
f. Reviewing violation issues/trends concerning security and related privacy compliance within the Organization with recommendation and follow-up of corrective action with appropriate personnel. Documentation and appropriate reporting on all findings.
g. Ensuring that Privacy and Security incidents are managed by a dedicated team with dedicated tools and processes.
h. Ensuring that security or privacy event (incident) analysis with corrective actions, mitigation or remediation is adopted into on-going policies, procedures and training.
i. Conducting investigations in relation to breach determination, probability of compromise analysis and breach notification as needed.
j. Reporting privacy and security violations or breaches to the Organization's Senior Corporate Compliance Officer, OCR and individuals, as appropriate.
k. Assisting in OCR Investigations, as appropriate.
l. Determining user group access levels necessary to carry out job responsibilities, including determination of access to confidential patients.
m. Determining content of materials and tracking of privacy and security awareness training.

3. The Organization's Privacy and Security Compliance Program will be compliant with all mandatory Federal and State privacy and related security regulations, including but not limited to HIPAA. The Organization recognizes its status as a Covered Entity or Business Associate if appropriate under the definitions contained in the HIPAA regulations and that they must comply with HIPAA privacy and security regulations concerning state law preemptions of HIPAA regulations. HIPAA generally preempts state laws regarding privacy. However, state laws that provide stronger protections for confidential health data, or that provide for better access to data than HIPAA, will preempt HIPAA regulations. In general *both* HIPAA law and state law shall be complied with whenever possible. If there is a conflict between the two, a preemption analysis and determination, possibly involving legal counsel, must be made to assess which laws (HIPAA, state laws, or both) must be followed.

4. The Privacy Officer is responsible for analysis of HIPAA preemption issues, if necessary in consultation with Security Officer and Legal Counsel to make preemption determinations. The Privacy Officer will then create, modify, or amend organization policies and procedures to accurately reflect preemption determinations The Privacy Officer performs ongoing research to monitor legislative changes in the state(s) where the Organization operates that may impact HIPAA preemption issues.

5. Failure of workforce members to comply with all Organizational privacy and security policies and procedures will be dealt with according to defined mitigation, remediation, corrective action and sanction policy and procedures.

6. HIPAA regulations and best practices call for the creation and implementation of specific policies and procedures addressing HIPAA privacy and security compliance and they must be followed by all workforce members. Privacy and security policies and procedures shall be updated and amended by the respective Privacy and Security Compliance Officers and staff, as needed or as required by law. All policies and procedures shall be made accessible to appropriate members of the workforce. The

Organization's Security Compliance Program will be compliant with all mandatory Federal and State privacy and related security regulations, including but not limited to HIPAA. The Security Compliance Program follows numerous guidelines, including HIPAA Security and HITECH, Omnibus Privacy Final Rule but also may include PCI and other standards for Security Compliance.

7. Privacy and Security Risk Assessments will be undertaken on a routine basis in order to prioritize risks, determine mitigation priorities and reduce risks to an acceptable level. These prioritized risks will become a part of a global risk management plan. Within a Security Risk Assessment the Security Rule has two types of implementation specifications, 'Required' and 'Addressable'. The required specifications must be implemented. The addressable implementation specifications are not required but must be 'addressed'. Not being required does not mean optional. The Organization has one of three courses of actions with addressable items, one of which must be taken. The organization will decide to implement a specification, implement an alternate equivalent, or not implement it at all. 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. These assessments will need to include whether technologies for security are adequate and include vulnerability scans, penetration, data network tests.

8. Covered Entities will assess and monitor Business Associate Compliance Programs and/or BA- Sub-contractor if appropriate. CEs and BAs will agree upon breach discovery timeframes, breach determination processes and which party is to provide notifications. Note: Under HIPAA Omnibus Final Rules CEs, BAs and Sub-contractors are all directly liable for their HIPAA compliance.

9. HIPAA rules are flexible in relation to the actual implementation of required rules; larger organizations will need to utilize more sophisticated methodologies. Although it must be recognized that all rules are required to be met at all times, what is considered 'reasonable and appropriate' may vary by organization type, size and nature of the PHI they manage.

10. Any healthcare clearinghouses owned or affiliated with this Organization will have separate staff, physical space, ePHI and compliance plans.

11. Security standards to be maintained per HIPAA Security Rules (§164.306) in reference to the Organization's Security Compliance Program:

(a) General Requirements - Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
(4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of Approach

(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:
  (i) The size, complexity, and capabilities of the covered entity.
  (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
  (iii) The costs of security measures.
  (iv) The probability and criticality of potential risks to electronic protected health information.

E. Related Procedures

- List specific Security Compliance standards followed by this organization: HCBS Provider, Inc will be compliant with federal, state and local HIPAA compliance rules
- List security incident management procedures: HCBS Provider, Inc will follow the state of Pennsylvania's HIPAA compliance violation rules

F. Related Forms

- AAs – ROI, Breach and Patient Rights Log
- Bs -- Security or Privacy Event/Incident Reporting Form
- Cs – Security or Privacy Event Investigation Form
- Ds -- Security or Privacy Event Corrective Action Form
- Gs – Request for Patient Rights Form
- Ns – Breach Determination and Reporting Form
- List additional related forms as applicable: none

G. Related Policies

- 2s – Documentation for Security and Privacy Compliance
- 27s – Investigations by HHS, OCR or Other Regulators
- 21s- HIPAA Violation and Breach Determination
- 26s – Sanctions, Enforcement and Discipline
- 34s – Workforce Training Policy HIPAA
- 108s – Security Incident Reporting
- 125s – Security Officer Job Description
- 126s – Combined Privacy and Security Job Description for Physician Practice
- List additional related policies as applicable: none

H. References

- Stericycle Online Security Risk Assessment (SRA) tool
- SRA Line Item Numbers: B18,B19,b21, B22, B36, B37, B38, B46, B47, B71, B72, B74, B75, B76, B96, B97, B98, B99, B101, D29, E7, E8, E9, E14, E15, E16, F2, F7
- 45 CFR 164.302 - 164.318
- 45 CFR Parts 160 and 164 (HIPAA) §164.530§ 164.104, § 164.306, § 160.201 to § 160.205
- HITECH Act § 13401,
- HIPAA laws fostering Policies and Procedures § 160.310, § 164.306, § 164.312, § 164.316 and § 164.530(i)

- 45 CFR Parts 160 and 164 (HIPAA) §164.530
- §164.306 - Security standards: General rules
- NIST Incident Handling SP800-61 Rev 1
- 2013 Omnibus HIPAA Privacy Final Rules
- List additional references as applicable: none

Breach Determination and Reporting (Federal HIPAA)

A. Coverage

HCBS Provider, Inc (hereafter referred to as the 'Organization') workforce members that access, use or disclose confidential patient information.

B. Create / Revision Date

11/28/2021

C. Purpose

To provide foundational elements for the determination and response to privacy violations, breaches (wrongful acquisition, access or disclosure of PHI), the resultant breach risk analysis and breach notification responsibilities, policies and procedures that may be required from both HIPAA and State perspectives. HIPAA is considered to be reverse pre-emption (a set of 'floor') rules. If the State in which a Privacy Event occurs has more stringent Laws, Rules, or Regulations, these will prevail; these policies are created to address HIPAA Privacy / Security and will apply both Federal and State requirements.

D. Policy

The HITECH portion of ARRA (American Reinvestment and Recovery Act, February 17, 2009) markedly expands HIPAA Privacy and Security. HITECH when combined with The "HIPAA Breach Notification for Unsecured PHI, Interim Final Rule" issued by HHS (Health and Human Services) on September 23, 2009 and the "Omnibus Privacy Final Rule Modifications" issued in January 2013 creates the detailed Federal Rules governing requirements for determining privacy violations resulting in breaches of PHI and the processes for notifying individuals (patients) and governmental entities that an individual's PHI was breached.

The Organization fully complies with the Federal and Pennsylvania Laws, Rules, and Regulations concerning PHI Privacy such as HIPAA (Health Insurance Portability and Accountability Act): http://www.hhs.gov/ocr/privacy

This Organization treats each potential Breach of PHI separately, applying procedures which follow the HHS (Health and Human Services) and OCR (Office for Civil Rights) guidelines. Within the Organization the occurrence of 'Privacy Events' that may have HIPAA or State privacy implications will trigger procedures defined by this policy to determine whether or not a potential HIPAA violation and a resultant Breach of PHI has occurred and the steps that will result. Each of these Privacy Events will be addressed separately according to its own individual characteristics, but always according to this defined policy.

The means of discovery of a Privacy Event, be it through internal processes or reported via external party, does not change the application of these policies. This Organization encourages workforce members and individuals (patients) to report issues and privacy concerns to this Organization's Privacy Officer; and if thereafter more reporting is desired to the HHS (Health and Human Services) Office for Civil Rights (OCR) without fear of retaliation. The OCR website link for complaints is:

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

If a Privacy Event occurs within a Business Associate (BA), the BA should without unreasonable delay, typically 1 business day, notify the Covered Entity (CE). Recommend above language, but the CE and BA must agree on who provides notification to OCR and individuals.

The Organization will provide Breach Notification for the individuals who were treated and whose PHI was created within their Organization, even if the Breach occurred while in the control of the BA. The Business Associate Agreements (BAA) between the Organization and their BAs will address the details of Privacy Event Discovery, Determination, and Notification.

This Organization's procedure for determining and addressing HIPAA violations, Breach of PHI, Harm Threshold Analysis, and Notification are generally outlined by the following steps:

1. Investigation and documentation by CE (or BA) of a Privacy Event (incident).
2. Final determination of whether a (HIPAA) privacy violation has occurred.
3. Determine if a breach of *unsecured* PHI has probably occurred;
4. Determine based on the data of the violation / potential breach whether to apply Omnibus Final Rule standards.
5. If unsecured PHI has been breached, perform the Omnibus Low Probability Analysis.
   a. If the breach meets the criteria established by the CE that identifies this violation is technically a breach of unsecured PHI either notify OCR either immediately (if over 500 individuals per event) or annually (if under 500 individuals per event).
   b. Notify individual(s) of the breach of their PHI.
6. Feedback, mitigation, sanctions and corrective actions developed and recorded.

Steps to follow for determination of the scope of a Privacy Event

After investigation, Privacy Events may or may not be determined to be privacy violations (this determination typically is drawn from HIPAA Rules, but also possibly from State-based requirements). The scope of the determination of the results of a Privacy Event investigation results in the procedures that will need to be undertaken in the form of notification and corrective actions.

1. Privacy Event Investigation

Investigation and documentation by CE (or BA) of a Privacy Event will occur after 'discovery' of a Privacy Event and reporting to appropriate CE staff member. Privacy Events must be reported as soon as discovered with the clock running from the time of discovery until notification. The time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete Enter State time frames, if less than the HHS mandated 60 day time period>. Be careful to differentiate between 'working' and 'calendar days' § 164.404(b) requires covered entities to notify individuals of a breach without unreasonable delay but in no case later than 60 calendar days from the discovery of the breach, except in certain circumstances where law enforcement has requested a delay.

Privacy Events will be recorded in the *Security or Privacy Event Investigation* Form and will follow the guidelines set below.

2. Privacy Violation and Breach of Unsecured PHI Determination

Final Determination of whether a privacy violation has occurred will encompass both HIPAA Privacy and any applicable State requirements. HIPAA Privacy is very specific and according to language in the Interim Final Rule, a privacy violation may have occurred if there is an 'unauthorized acquisition, access, use, or disclosure of PHI'. Therefore, one of the first steps in determining whether notification is necessary under this subpart is to determine whether a use or disclosure of PHI violates the HIPAA Privacy Rule. Note that uses or disclosures that impermissibly involve more than the minimum necessary information, may qualify as violations and breaches. Privacy violations of administrative requirements, such as a lack of reasonable safeguards or a lack of training, do not themselves qualify as potential breaches under this subpart (although such violations certainly may lead to impermissible uses or disclosures that qualify as breaches). Therefore; the test to determine if a privacy violation has occurred is to make the determination on whether an 'unauthorized acquisition, access, use, or disclosure of PHI' has occurred, remembering that disclosure of more than the Minimum Necessary (See Minimum Necessary and Limited Data Set Policy) PHI may be designated as a privacy violation. There are also exceptions listed in HIPAA that help determine whether a privacy violation is technically a breach of unsecured PHI. These 3 exceptions include:

(1) Unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a CE or BA;
(2) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates;
(3) Unauthorized disclosures in which an unauthorized person to whom protected health information is disclosed would not reasonably have been able to retain the information.

Once it has been determined that a privacy violation has occurred, the CE must make the determination (by use performance of a low probability of compromise analysis) of whether a breach of unsecured PHI has occurred in order to determine reporting requirements.

Be sure to record the determination of whether a breach of unsecured PHI occurred in an Investigation and Corrective Action for Security / Privacy Compliance Form, including if the Privacy Event was not deemed a breach because it fell into one of the above listed exceptions.

This Organization treats a breach of unsecured PHI as having occurred at the time of the impermissible use or disclosure, but also recognizes that the CE or BA may require a reasonable amount of time to confirm whether the Privacy Event or violation qualifies as a breach of unsecured PHI. A breach is considered discovered, and thereby assumed to be a breach unless proven otherwise to have a low probability of PHI compromise, when the incident becomes known, not when the CE or BA concludes the above analysis whether the facts constitute a Breach. Section 164.404(a)(2) states that a breach shall be treated as discovered by a CE as of the first day the breach is known to the CE, or by exercising reasonable diligence would have been known to the CE. Thus, a CE is not liable for failing to provide notification in cases in which it is not aware of a breach unless the CE would have been aware of the breach had it exercised reasonable diligence. The Interim Final Rule further provides that a CE is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the CE. This again illustrates the need for all workforce members to promptly report any suspected Privacy Events, violations or breaches of unsecured PHI.

The Covered Entity and / or Business Associate may be liable for breach determination or reporting as enumerated within the Business Associate Agreement. A Business Associate's Sub-contractors must also report Privacy Events, potential breaches, as soon as possible, per the terms of their agreements with the Business Associate

3. Omnibus Final Privacy Rule - Breach Determination Standard

Effective September 23, 2013 the 'Omnibus' Final HIPAA Privacy Rule mandates a different calculation of whether a HIPAA Violation (assumed to be a 'breach') is determined to be a reportable breach as the result of an impermissible access, use or disclosure of unsecured PHI. If occurring after September 23, 2013, all potential HIPAA violations for wrongful access, use or disclosure of PHI are now designated as 'breaches' and are subject to this new determination standard.

The definition of breach was amended in the final rule to clarify that an impermissible use or disclosure of protected health information is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

The final rule acknowledges, by including a specific definition of breach and identifying exceptions to this definition, as well as by providing that an unauthorized acquisition, access, use, or disclosure of PHI must compromise the security or privacy of such information to be a breach, that there are several situations in which unauthorized acquisition, access, use, or disclosure of protected health information is so inconsequential that it does not warrant notification.

- For example, if a CE misdirects a fax containing protected health information to the wrong physician practice, and upon receipt, the receiving physician calls the CE to say he has received the fax in error and has destroyed it, the CE may be able to demonstrate after performing a risk analysis that there is a low risk that the protected health information has been compromised.

Instead of assessing the risk of harm to the individual, CE and BAs must assess the probability that the protected health information has been compromised based on a risk analysis that considers at least the following 4 factors. HHS/OCR emphasizes that the entity must evaluate all the factors, including those discussed below, before making a determination about the probability of risk that the protected health information has been compromised.

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

- **The first factor** requires CEs and BAs to evaluate the nature and the extent of the PHI involved, including the types of identifiers and the likelihood of re-identification of the information. To analyze this factor, entities should consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature.

    - For example, with respect to financial information, this includes credit card

numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud.

- With respect to clinical information, this may involve considering not only the nature of the services or other information but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results).
- Considering the type of PHI involved in the impermissible use or disclosure will help entities determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests.
- Additionally, in situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, entities should determine whether there is a likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other available information.

    - For example, if a CE impermissibly disclosed a list of patient names, addresses, and hospital identification numbers, the PHI is obviously identifiable, and a risk analysis likely would determine that there is more than a low probability that the information has been compromised, dependent on an analysis of the other factors discussed below.
    - Alternatively, if the CE disclosed a list of patient discharge dates and diagnoses, the entity would need to consider whether any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served by the CE, or whether the unauthorized recipient of the information may have the ability to combine the information with other available information to re-identify the affected individuals (considering this factor in combination with the second factor discussed below).

- **The 2nd factor** requires CEs and BAs to consider the unauthorized person who impermissibly used the protected health information or to whom the impermissible disclosure was made. Entities should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information; there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity. OCR also emphasizes that this factor should be considered in combination with the factor discussed above regarding the risk of re-identification. If the information impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the protected health information has the ability to re- identify the information.

- **The 3rd factor** requires CEs and BAs to investigate an impermissible use or disclosure to determine if the protected health information was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed.

    - For example, as discussed in the interim final rule, if a laptop computer was stolen and later recovered and a forensic analysis shows that the protected health information on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed.
    - In contrast, however, if a CE mailed information to the wrong individual who

opened the envelope and called the entity to say that she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.

- **The final factor** included in the final rule requires CEs and BAs to consider the extent to which the risk to the PHI has been mitigated. CEs and BAs should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. HHS/OCR notes that this factor, when considered in combination with the factor regarding the unauthorized recipient of the information discussed above, may lead to different results in terms of the risk to the PHI.

    - For example, a Covered Entity may be able to obtain and rely on the assurances of an employee, affiliated entity, BA, or another CE that the entity or person destroyed information it received in error, while such assurances from certain third parties may not be sufficient.

A CEs or BAs analysis of the probability that protected health information has been compromised following an impermissible use or disclosure must address each factor discussed above. Other factors may also be considered where necessary.

HHS/OCR expects these risk analysis to be thorough, completed in good faith, and for the conclusions reached to be reasonable. If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that the protected health information has been compromised, breach notification is required.

HHS/OCR has removed the exception for limited data sets that do not contain any dates of birth and zip codes. In the final rule, following the impermissible use or disclosure of any limited data set, a Covered Entity or Business Associate must perform a risk analysis that evaluates the factors discussed above to determine if breach notification is not required.

Encryption according to published guidance is still considered a safe harbor; breach notification is not required.

CEs and BAs have the burden of proof to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach and to maintain documentation; (e.g., of the risk analysis demonstrating that there was a low probability that the PHI had been compromised; or of the analysis that the impermissible use or disclosure falls within one of the other exceptions to breach) as necessary to meet this burden of proof. Thus, Covered Entities and Business Associates have adequate incentive to conduct reasonable and diligent risk analyses.

Regarding the exceptions to the definition of breach in the interim final rule, the Department adopts these exceptions without modification in this final rule. The substance of these exceptions has not changed.

4. Notification to Individuals and OCR

The Interim final rule provides the requirements for the notifications CEs are to provide to individuals affected by a breach of unsecured PHI, this did not change under Omnibus.

The CE shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired, used, or disclosed as a result of such breach.

A CE shall send the required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the CE. Thus, provisions for timeliness should be read together with the above provisions for when a breach is treated as discovered. This Organization expects to make the individual notifications as soon as reasonably possible. The CE may take a reasonable time to investigate the circumstances surrounding the breach.

Individuals and the Secretary of HHS (via the Office for Civil Rights; OCR) are notified if the CE (or in rare cases the BA) determines there is a reasonable potential of harm to the Individual from the breach. This means that not all privacy violations are reported to Individuals or OCR.

Individual Notification can be delayed for Law Enforcement reasons, see the Interim Final Rule for details. (Section 13402(g) of the HITECH Act)

The Notification to Individuals is to include, to the extent possible, the following elements. The OCR notification is via a website that also requires most of this information.

a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
b. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved). Just send a 'general description' of the PHI involved in the breach, not the actual details of the PHI. 'Diagnosis' is listed as an example of a type of PHI to make clear that, where appropriate, the CE may need to indicate in the notification to the individual whether and what types of treatment information were involved in a breach.
c. Any steps individuals should take to protect themselves from potential harm resulting from the breach.
d. A brief description of what the CE involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches. This part of the notification should describe the steps the CE is taking to mitigate potential harm to the individual resulting from the breach and that such harm is not limited to economic loss.
e. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, web-site, or postal address.
f. It is important for individuals to be able to understand the information being provided to them in the Breach Notifications and the Interim Final Rule includes a requirement that such Notifications be written in plain language. To satisfy this requirement, the CE should write the Notice at an appropriate reading level, using clear language and syntax, and not include any extraneous material that might diminish the message it is trying to convey.
g. OCR is notified in the case of either less than 500 individuals per event annually or for greater than 500 individuals immediately (within 60 calendar days under all circumstances) via the following link and the instructions therein.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

h. Breaches involving more than 500 individuals require website posting and other

specialized notifications and should be referred immediately to legal counsel for guidance.

i. Breaches involving more than 10 patients with unknown contact information also require special notifications (e.g. website posting) and must be managed with care according to applicable Statutes and Rules.

5. Methods of for Notification of Individuals

HIPAA provides for both actual written notice to the individual, as well as substitute notice to the individual if contact information is insufficient or out-of-date. A CE must provide Breach notice to the individual in the following manner(s):

a. In written form by first-class mail at the last known address of the individual.
b. Interim Final Rule also provides that written notice may be in the form of electronic mail, provided the individual agrees to receive electronic notice and such agreement has not been withdrawn.
c. Note in cases where the individual affected by a Breach is a minor or otherwise lacks legal capacity due to a physical or mental condition, notice to the parent or other person who is the personal representative of the individual will satisfy the requirements of § 164.404(d)(1).
d. The statute also requires that, if the individual is deceased, notice must be sent to the last known address of the next of kin. The Interim Final Rule provides that such notice be sent to either the individual's next of kin or personal representative; as such term is used for purposes of the Privacy Rule, recognizing that in some cases, a CE may have contact information for a personal representative of a deceased individual rather than the next of kin.

E. Definitions

Breach of PHI

The Omnibus Privacy Final Rule added language to the definition of breach to clarify that an impermissible use or disclosure of protected health information is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

Breach Notification

The Organization defines Breach Notification as does ARRA / HITECH, see section See Section 13402. In a CE that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured health information (as defined in subsection (h)(1)) shall, in case of Breach of such information that is discovered by the CE, notify each individual who unsecured PHI has been or is reasonably believed by the CE to have been accessed, acquired or disclosed as the result of such Breach.

Enforcement of HIPAA Privacy and Security

The enforcement of HIPAA Privacy and Security is managed by the Office for Civil Rights (OCR), a

department of Health and Human Services (HHS): http://www.hhs.gov/ocr/

Probability of Compromise

The standard for Breach analysis mandated by the Omnibus Privacy Final Rule - This standard contains 4 factors that must be analyzed (at a minimum) to determine whether a Privacy Event / HIPAA Violation is a reportable Breach under Federal regulations.

PHR (Personal Health Record)

A **PHR** (personal health record) is managed, shared, and controlled by or primarily for the individual.

Privacy Event

Privacy Events are discovered incidents and occurrences related to the acquisition, access use and disclosure of an individual's PHI that upon further investigation may or may not be deemed HIPAA Privacy violations or Breaches of unsecured PHI.

Protected Health Information (PHI)

Protected Health Information (PHI) as defined in Section 160.103 of Title 45, Code of Federal Regulations - Any information whether oral, written, electronic or recorded in any form that is created or received by CE as a healthcare provider and relates to an individual's past, present or future physical or mental condition; healthcare treatment and payment for services. PHI also includes data that identify the individual (e.g. Name, SSN, MRN, account number, address, telephone number, DOB, e-mail address, names of relatives, employer, etc).

Secured PHI

PHI that is secured through the use of a technology or methodology specified by the HHS Secretary in guidance issued under paragraph (2) - Secured PHI applies to data in all of its various states, per the Federal Register Data in use, motion at rest and disposed as outlined in the 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 of 2009;

Unsecured PHI

Unsecured Protected Health Information (PHI)(A)The term 'unsecured protected health information' means PHI that is not secured through the use of a technology or methodology specified by the (HHS) Secretary in guidance issued under paragraph (2).

E. State Law Breach Requirements

Pennsylvania Law Breach Requirements and how they operate in relation to HIPAA. Tailor the procedure below to include any applicable State laws and regulations.
Covered entities: "An entity* that maintains, stores, or manages computerized data that includes personal information." (§2303(a)) * "Entity" means a "[s]tate agency, a political subdivision of [Pennsylvania] or an individual or a business doing business in [Pennsylvania]." (§2302) Service provider requirement: Yes. "A vendor that maintains, stores, or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores, or manages the data." (§2303(c))

F. Procedure

- Upon discovery of a security or privacy event, use 'Cs – Investigation and Corrective Action' form to document your findings.
- If the investigation points to a possible HIPAA Violation or Breach continue the investigation, documenting the required Breach Determination Assessment; there are two to choose from;
    a. If the event occurred between September 23, 2009 and September 23, 2013 utilize the '*S1s - Privacy Interim Final Rule Breach Analysis*' form.
    b. If the event occurred after September 23, 2013 utilize '*Ss - Omnibus Privacy Final Rule Breach Analysis*' form.
- If upon analysis, the determination is made that the event was a reportable breach complete Ns – Reporting Form to organize your data for breach reporting.
- Be sure to report on time to the patient and the Federal government.
- If applicable, Timing: "Except as provided in [(§2304) authorization delay pursuant to the needs of law enforcement] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay." (§2303(a)) Delay: "The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise theinvestigation or national or homeland security."

(§2304).
- Be sure to keep all documentation for six years.

G. Related Policies

- 25s - Mitigation of Improper Use or Disclosure
- 26s - Sanctions, Enforcement and Discipline
- 8s - Minimum Necessary and Limited Data Set and De-Identification
- 9s - HIPAA Designated Record Set
- 6s - Appropriate Access of PHI

H. Related Forms

- Bs - Security or Privacy Report Form
- Cs - Breach Investigation and Reporting Form
- N - Privacy Event Investigation Form for CE
- Na - Privacy Event Investigation Form for BA
- Ss - Omnibus Final Rule Breach Analysis Form (Manual)
- S1s - Interim Final Rule Breach Analysis Form (Manual)
- 29 - Business Associate Agreement
- V - Confidentiality Agreement

I. References

- Title 45, Code of Federal Regulations, Parts 160 and 164, August 14, 2002.
- ARRA / HITECH Act February 17, 2009 –Section 13400
- HHS Omnibus HIPAA Privacy Final Rule Modifications, January 17, 2013
- HHS Interim Final Rule Breach Notification for Unsecured Protected Health Information Effective September 23, 2009
  DEPARTMENT OF HEALTH AND HUMAN SERVICES
  45 CFR Parts 160 and
  164 RIN: 0991-AB56
  Breach Notification for Unsecured Protected Health Information
  §164.400
- Office for Civil Rights website: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- Federal Register/Vol. 74, No. 79/Monday, April 27, 2009/ Rules and Regulations 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 Special Publication 800-66 Revision 1; An Introductory Resource Guide for Implementing the HIPAA Security Rule
- OMB Memorandum M-07-16 which requires breach notification policies for personally identifiable information that take into account the likely risk of harm caused by a Breach in determining whether Breach Notification is required.

Handling Privacy Complaints, Internal and External

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 supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

11/28/2021

C. Purpose

To support the Organization as we continually improve the quality of services provided and to define a process for handling complaints and grievances related to the use or disclosure of Protected Health Information (PHI).

D. Policy

1. HIPAA privacy and security laws and rules grant individuals (patients) specific 'rights' relating to their PHI, many of which overlap with patient rights mandated by state law. In addition to privacy rights related to their PHI, individuals (patients) are granted the right to: access their PHI/medical record information; request restrictions on the use or disclosure of their PHI; request that communications related to their PHI be confidential; request an amendment to their PHI; and receive an Accounting of Disclosures of their PHI. HIPAA also mandates that a Covered Entity (CE) implement a process for individuals to submit a complaint about the CE's privacy-related policies and procedures and its compliance with those policies and procedures.

2. Complaints may be related to privacy and/or security issues. This policy is focused more on privacy complaints; however, determinations in the nature of any privacy/security complaint and the resulting, appropriate mitigations and/or sanctions will be applied equally and by the responsible privacy or security compliance parties within this Organization.

3. Privacy complaints (which may be in the form of a grievance) about wrongful access, use or disclosure of PHI, or for any other HIPAA or State regulatory based reason, may come from external sources such as patients themselves, the State or Federal regulators (Office for Civil Rights (OCR), typically), from an internal channel or workforce member.

4. All privacy complaints, regardless of the source, about HIPAA 'rights', access, use or disclosure of PHI shall be investigated and managed in a timely and respectful manner.

5. Complaints concerning PHI, their investigation, disposition or resolution must be documented in writing (or within a computer system) and shall be kept for the appropriate retention period(s) prescribed by regulation.

6. To the extent practicable, any known harmful effect of an access, use or disclosure of PHI in violation of our policies and procedures and the requirements of applicable laws, by any Covered Entity or Business Associate must be mitigated.

7. Our Organization will not retaliate in any way (i.e. intimidation, threatening behavior, coercion, and discrimination) against an individual lodging a complaint, or for testifying, assisting, or participating in any investigation or administrative action. Nor will any individual be asked to waive the rights permitted to him or her under State or Federal Privacy Laws as a condition of treatment, payment, enrollment, or eligibility for benefits.

Responsible Parties

The Privacy Officer is responsible for overseeing the management and documentation requirements related to privacy complaints regarding HIPAA rights, access, use or disclosure of PHI. The Security Officer manages security based complaints and works together with the Privacy Officer to form a unified Privacy and Security Compliance Program.

Procedure

Respond to complaint in writing.

1. Consider confidentiality concerns (i.e., if a relative informed you of the concerns, do you have the authority to discuss the patient health care information with the relative, or do you need a signed consent form?).

2. Notify or consult with the appropriate Organization insurance carrier and/or legal counsel on issues involving liability and litigation potential.

3. Respond in a timely fashion (i.e., the initial response could simply be that the Organization will investigate and inform you of the final decision if enough information is not available to make an immediate determination). A letter with the final resolution or disposition shall be sent to the appropriate party, the individual or the regulatory body.

4. Notify the appropriate individual to address any pertinent employment issues (i.e. investigation, counseling, disciplinary action, or termination) according to applicable policies/procedures and State and Federal Laws.

5. Work to mitigate, to the extent practicable, any harmful effect that is known because of an access, use or disclosure of PHI in violation of organizational policies and procedures or the requirements of applicable laws by the Organization or their Business Associates.

6. Take steps to ensure that the Organization will not retaliate in any way (i.e., intimidation, threatening behavior, coercion, and discrimination) against an individual lodging a complaint or grievance.

7. If the results of the investigation indicate that an employee or Business Associate of the Organization made an unauthorized access, use or disclosure relating to a patient's rights in regards to PHI; failed to maintain the privacy of the patient's PHI; failed to request restrictions

on uses or disclosures of the patient's PHI, or otherwise violated the practice's HIPAA policies and procedures it should be reported to the Privacy Officer. If the investigation was conducted by the Privacy Officer, the Privacy Officer shall report it to the practice's governing body.

8. Follow-up, mitigate and provide sanctions as appropriate.

9. The Privacy Officer shall document all HIPAA-related complaints, their resolution, and any actions resulting therefore. This documentation must be maintained for a minimum period of six (6) years from the date of final resolution, unless modified by State or Federal regulation and defined within another policy.

Tips for Workforce Members Responding to a Privacy Complaint

1. Listen – communication considerations:
   a. Actively listen. Take steps to minimize interruptions by others and interrupting the individual.
   b. Restate your understanding of the nature of the issue.

2. Address the individual's concern if authorized and able to do so, or advise the individual that you would be happy to report the problem or that he or she may report the problem to your immediate Supervisor. Consider the following:
   a. Again, remember confidentiality concerns (i.e., if a relative informed you of the concerns, do you have the authority to discuss the patient health care information with the relative, or do you need a signed consent form?).
   b. An individual has the right to request to file a written complaint with the Privacy Officer.
   c. If the individual expresses a desire to complain to the Department of Health and Human Services or the Office for Civil Rights (OCR), advise the individual that "we also respect your right to file a complaint with the OCR and that the Organization will not retaliate against you." OCR complaints should be filed online at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

3. Document in writing all discussions and maintain notes and any information useful for an investigation. This document should be routed immediately to the Privacy Officer.

E. Definitions

Complaint (or Grievance)

Any concern communicated verbally or in writing by a patient (or a patient's legal representative) questioning any act or failure to act by our Organization relating to a patient's rights to access the patient's protected health information; to maintain the privacy of the patient's protected health information; to request restrictions on uses or disclosures of the patient's protected health information, to request confidential communications regarding the patient's protected health information (PHI); to request an amendment to the patient's protected health information, or to receive an accounting of disclosures of the patient's protected health information.

Protected Health Information (PHI)

Individually identifiable health information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care services provided to an individual. ePHI refers to electronically (computerized) created or stored protected health information.

Responsible Party

The Privacy Officer is responsible for overseeing the management and documentation requirements related to complaints regarding the use or disclosure of PHI. This individual also reviews and responds to complaints concerning PHI as needed.

F. Related Forms

- Bs – Security or Privacy Event/Incident Reporting Form
- Cs – Security or Privacy Event Investigation Form
- Ns – Breach Determination and Reporting Form
- AAs – ROI, Patient Rights and Breach
- List additional related forms: none

G. Related Policies

- 19as – HIPAA Privacy and Security Compliance Program Master Policy
- List additional related policies: none

H. References

- §164.502
- §164.530
- §164.530(g)(1)
- Stericycle Online Privacy Risk Assessment (PRA)
- PRA Items: C.29, C.31
- List additional references: none

Mitigation of Improper Use, or Disclosure of PHI

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

11/28/2021

C. Purpose

To communicate the policy of the Organization to prevent and respond to any improper use or disclosure of an individual's PHI.

D. Policy

The Organization mitigates, to the extent practicable, any harmful effect that is known, occurring as a result of a use or disclosure of PHI by the Organization or any of its Business Associates (BAs) that is in violation of Organization policies related to HIPAA Privacy and Security.

Information regarding any suspected or actual inappropriate access, use or disclosure of PHI by the Organization or any of its BAs that is discovered by any employee of the Organization shall be forwarded promptly to the Organization's Privacy Officer. Suspected or actual inappropriate access, use or disclosure of PHI that has been reported will be termed a 'Privacy Event' and investigated as to whether a Privacy Violation or Breach occurred.

The Organization's Privacy Officer, in response to such reports or other information regarding an unauthorized use or disclosure by the Organization or any of its BAs, including self-disclosures made by BAs pursuant to the terms of each BA's contract or other agreement with the Organization, shall develop and implement a plan as soon as reasonably practicable to mitigate any known or reasonably anticipated harmful effects from such use or disclosure. The actions to mitigate such unauthorized use or disclosure shall be tailored to the circumstances of each case, but may include as appropriate, the following:

1. Identifying the source(s) of the use or disclosure and taking appropriate corrective action
2. Contacting the recipient of the information that was the subject of the unauthorized disclosure and requesting that such recipient either destroy or return the information
3. Instructing such recipient to make no further uses or disclosures of such information
4. Depending on the circumstances, notifying the individual whose PHI was the subject of the unauthorized use or disclosure; and
5. Reviewing, and correcting where appropriate, any policy or procedure of the Organization that directly caused or contributed to the unauthorized use or disclosure.
6. Remember that not all harm to a patient (individual) in the case of a Privacy Violation can be of an economic nature; there are other considerations, such as reputational harm, that will

factor into the mitigation plan.

The Organization's Security or Privacy Officer shall immediately notify, if appropriate, the Organization's Legal Counsel, regarding the Security or Privacy Event, and/or the unauthorized use or disclosure of PHI and shall take further action as so advised. The Organization's Management and Legal Counsel shall determine, in the event that the unauthorized use or disclosure was made by a BA or Contractor, whether such disclosure warrants termination of the BA's contract. In addition, the Organization's Security or Privacy Officer shall notify the individual responsible for compiling accounting of disclosures so that any accounting can include the unauthorized use or disclosure, if appropriate.

E. Related Policies

- 6s - Appropriate Access of PHI
- 7s - Confidentiality of PHI
- 20s - Handling Privacy Complaints Internal and External
- 26s - Sanctions, Enforcement and Discipline Policy
- 34s - Workforce Training Policy – HIPAA
- List additional related policies: none

F. Related Forms

- AAs – Release of Information, Patient Rights and Breach Log
- Bs – HIPAA Security or Privacy Event Reporting
- Cs –Security or Privacy Event Investigation Form
- Ns – Breach Determination and Reporting Form
- List additional related forms: none

G. References

- §164.530
- For CEs: § 164.530(f)
- For BAs: 45 CFR §164.504(e)(2)(ii)(B)
- Security Rule: 45 C.F.R. § 164.314(a)
- Stericycle Online Privacy Risk Assessment (PRA)
- PRA Line Item: C.12
- List additional references: none

Sanctions, Enforcement and Discipline for Security or Privacy Violations

A. Coverage

HCBS 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

11/28/2021

C. Purpose

To define the Policy and Procedures to be followed for Enforcement and Discipline (also known as 'Sanctions') related to HIPAA Security and / or Privacy Violations and Breaches.

D. Policy

Enforcement and Discipline

Sanctions, or disciplinary action for workforce members (Employees) and Contractors who have failed to comply with the Organization's policies and procedures, or federal and state laws, or those who have otherwise engaged in conduct that has the potential of impairing the Organization's status as a reliable, honest and trustworthy entity, is an important part of privacy policy and procedures relating to PHI Privacy and Security. Therefore, all Employees and Contractors are required to acknowledge adherence to these policies and procedures as a material condition of employment or contracting with the Organization. Failure to comply with these policies and procedures will result in discipline up to and including immediate termination.

The Organization has this policy of progressive discipline (sanctioning) for employee wrongdoing, except where immediate termination is identified as the penalty. Disciplinary action may include remedial training, oral warnings, written reprimands, suspension and termination. Contractors can be terminated or sanctioned or otherwise disciplined according to their Business Associate agreement and / or contract terms. Whether the violation is a result of simple negligence, gross negligence, or an intentional act will be considered in determining the appropriate penalty.

If an Employee or Contractor has committed an infraction which would otherwise require discipline or termination, the Employee or Contractor may nevertheless be subject to a lesser punishment at the sole discretion of the Board, CEO or their designee.

Appropriate disciplinary action will depend upon: (i) the nature of the activity; (ii) whether the violator could reasonably be expected to identify the activity as a non-violation; (iii) whether the violator was in a position to take appropriate corrective action; (iv) whether the violator was unduly influenced to participate in the activity; and (v) any past violations or wrongdoings by the violator.

Additionally, the decision to terminate an Employee or Contractor or to impose a lesser sanction will be influenced by: (i) whether the Employee or Contractor promptly reported their own violation;

(ii) whether the report constitutes the Organization's first awareness of the violation and the Employee's or Contractor's involvement; and (iii) whether the Employee or Contractor cooperates fully in investigating and correcting the violation.

To ensure consistency and to monitor the effectiveness of the Security and Privacy Policies and Procedures, every violation or wrongdoing subject to disciplinary action must be reported to the Security or Privacy Officer. Based upon a reported event, the Organization's Security or Privacy Officer, after consultation with Organization's CEO of HCBS Provider, Inc. to administration team, will make a recommendation as to the appropriate disciplinary action to the CEO of HCBS Provider, Inc. to administration team. Any Organization employee subject to disciplinary action under these policies and procedures will have appeal rights consistent with those in his or her employment agreement, or in the Organization's personnel manual, as applicable.

Effective security and privacy compliance programs include procedures to discipline employees who fail to detect wrongdoing as well as those who commit the wrongdoing. Accordingly, the Organization will handle security and privacy violations as set forth in this policy, and any others that are applicable, concerning disciplinary action for security and privacy violations. The imposition of any disciplinary action or penalty under the Organization's security or privacy policies and procedures will not waive the Organization's right to seek monetary damages or to otherwise enforce its legal rights against the disciplined Employee or Contractor.

1. Management's Responsibility for Discipline

   The CEO of HCBS Provider, Inc. shall ensure that the Organization establishes procedures for the discipline of workforce members for violation of the security and / or privacy policies and procedures.

2. Privacy as an Element of Performance Reviews

   Security and privacy policy and procedures require that the promotion of, and adherence to their included elements be a factor in evaluating the performance of the Organization's Employees and Contractors. They will be periodically trained in new privacy policies and procedures. In addition, all managers and supervisors involved in the access, use and disclosure of PHI will:

   (a) Discuss with all of their supervised Employees and Contractors the Organization's policies and legal requirements applicable to their function.
   (b) Inform all of their supervised personnel that strict compliance with these policies and requirements is a condition of employment.
   (c) Disclose to all supervised personnel that the Organization will take disciplinary action up to and including termination for violations of these policies and requirements.
   (d) Managers and supervisors will be disciplined appropriately for failure to adequately instruct their subordinates, or for failing to detect noncompliance with applicable policies and legal requirements, where reasonable diligence on the part of the manager or supervisor would have led to the earlier discovery of any problems or violations and would have provided the Organization with an opportunity to correct them.

3. Record and Reporting of Disciplinary Actions

   The Security and Privacy Officers shall maintain a record of all disciplinary actions involving security or privacy and report at least annually to the Organization's management regarding such actions.

Responding to Detected Offenses and Developing Corrective Action plans

The purpose of this policy is to set forth the procedures to be used by the Organization to respond to reports by Organization workforce members (including employees and contractors) that an individual or individuals affiliated with or employed by the Organization have discovered a Security or Privacy Event (or Incident) that may represent a violation of HIPAA or State Law, Rule or Standards. This policy cannot control procedures utilized by the Organization's affiliate Business Associates (BAs), but should be addressed with each BA as a part of their Business Associate Agreement (BAA).

Purpose of Privacy Event Investigations

The purpose of a Security or Privacy Event Investigation is to:

(a) Identify those situations in which the Laws, Rules and Standards of the HIPAA and the Organization's security and privacy policies may not have been followed;
(b) Identify individuals who may have knowingly or inadvertently caused PHI security/privacy to be managed in a manner which violated Laws, Rules and Regulations of HIPAA and Pe, Rules and Regulations;
(c) Facilitate the correction of any practices not in compliance with security and privacy Laws, Rules and Regulations and
(d) Implement those procedures necessary to ensure future compliance;
(e) Protect the Organization in the event of civil or criminal enforcement actions; and
(f) Preserve and protect the Organization's assets.

Control of Security and Privacy Event Investigations

The respective Security and Privacy Officer(s) are responsible for directing the investigation of the alleged event, problem or incident. Reports of investigations shall be presented to the CEO of HCBS Provider, Inc. to administration team. At the discretion of the CEO of HCBS Provider, Inc. to administration team, if a Security or Privacy Event Investigation reveals intentional, criminal, or reckless conduct, a report may be forwarded to Legal Counsel in which event Legal Counsel shall be responsible for directing the investigation of the alleged problem or incident. In undertaking an investigation, the Security or Privacy Officer or Legal Counsel may solicit the support of internal audit, external counsel and auditors, and internal and external resources with knowledge of the applicable Laws and Regulations and required policies, procedures or standards that relate to the specific problem in question. These individuals shall function under the direction of the Security or Privacy Officer or Legal Counsel and are required to submit relevant evidence, notes, findings and conclusions to the Security or Privacy Officer (as appropriate) or Legal Counsel depending upon who is directing the investigation.

Privacy Event Investigative Process

Upon receipt of a complaint or other information (including audit results) which suggests the possible existence of a pattern of conduct in violation of privacy policies or applicable Laws, Rules or Regulations, a Privacy Event Investigation (under the direction and control of the Privacy Officer or Legal Counsel as necessary), shall be commenced as soon as reasonably possible. Steps to be followed in undertaking the Investigation include, but need not be limited to:

(a) An interview of the complainant and other persons who may have knowledge of the alleged problem or process and a review of the applicable Laws, Rules and Regulations which might be relevant to or provide guidance with respect to the appropriateness or inappropriateness of the activity in question, to determine whether or not a problem actually exists.
(b) The identification and review of the situation to determine the nature of the problem, the scope of the problem, the frequency of the problem, the duration of the problem and the potential financial magnitude of the problem.
(c) Interviews of the person or persons who appeared to play a role in the process which caused the problem. The purpose of the interview is to determine the facts related to the complained of activity, and may include, but is not limited to:
    (i) Personal understanding of the HIPAA and Pennsylvania Laws, Rules and Regulations;
    (ii) The identification of persons with supervisory or managerial responsibility in the process;
    (iii) The adequacy of the training of the individuals performing the functions within the process;
    (iv) The extent to which any person knowingly, or with reckless disregard or intentional indifference, acted contrary to the HIPAA or State Laws, Rules or Regulation;
    (v) The nature and extent of potential civil or criminal liability of individuals or the Organization; and
    (vi) Preparation of a summary report which shall indicate at a minimum:
        - Defines the nature of the problem;
        - Summarizes the Investigation process;
        - Identifies any person whom the investigator believes to have either acted deliberately or with reckless disregard or intentional indifference toward the HIPAA or Pennsylvania Laws, Rules and Regulations.
        - If the review results in conclusions or findings that the conduct referenced in the complaint is permitted under applicable Laws, Rules or Regulations or Policy or that the act did not occur as alleged or that it does not otherwise appear to be a problem, the investigation shall be closed.
        - If the initial Investigation concludes that there has been a HIPAA or Pennsylvania Law, Rule or Regulation violation, or that additional evidence is necessary, the investigation proceeds to the next step.

Corrective Actions

If at the conclusion of an Investigation involving a Security or Privacy issue it appears that there are genuine compliance concerns, the Security or Privacy Officer shall immediately formulate and implement a Corrective Action Plan. The Security or Privacy Officer shall obtain the advice and guidance of Legal Counsel and approval of the CEO of HCBS Provider, Inc. to administration team in formulating and implementing the Corrective Action Plan. The Corrective Action Plan shall be designed to ensure that the specific issue is addressed and, to the extent possible, that similar

problems do not occur in other departments or areas. The Security or Privacy Officer shall document the corrective action taken by using the appropriate forms and documentation procedures.

(a) Possible Criminal Activity. If the investigation reveals possible criminal activity (conduct which is intentional, willfully indifferent, or with reckless disregard for the Law), the Organization shall:
  (i) Immediately stop the activity related to the problem until the offending practice is corrected;
  (ii) Initiate appropriate disciplinary action against the person or persons whose conduct appears to have been intentional, willfully indifferent, or with reckless disregard for the Law;Make such notification to any Federal (Office for Civil Rights – OCR for HIPAA) or Pennsylvania Regulatory or Prosecutorial Authorities as Legal Counsel advises; and
  (iii) Promptly undertake an appropriate program of education to prevent future similar problems.

(b) Other Noncompliance. If the investigation reveals noncompliant conduct which does not appear to be intentional, willfully indifferent, or with reckless disregard for the Law, the Organization shall the above steps (i – iv.) also apply.
  (i) Monitoring.

Any issue for which a Corrective Action Plan is implemented shall be specifically targeted for monitoring and review as part of future audits.

Prevention

If a Security or Privacy Event Investigation points out a systemic deficiency in the Organization's policies or procedures or standards or if there have been similar incidents previously, the Security or Privacy Officer, with the advice of Legal Counsel and the approval of the CEO of HCBS Provider, Inc. to administration team, will recommend and institute appropriate changes to the applicable policies, procedures and training programs to prevent the problem from recurring, and privacy policies and procedures will be amended accordingly. The Security or Privacy Officer will review the record of the Investigation and the pertinent privacy policies and procedures, and may interview personnel and examine other documents to determine what additional steps need to be implemented to avoid similar future violations. All workforce members or Contractors will be promptly notified of any resulting changes to the Security or Privacy policies, procedures and standards.

Education

All workforce members shall be educated and trained at new hire and on a routine basis on the Sanctions, Enforcement and Discipline related to privacy and security violations. Documentation of this education shall be maintained along with other privacy and security training.

Legal Counsel

Where appropriate, the Security or Privacy Officer shall consult with the Organization's Legal Counsel regarding the appropriate corrective action to be taken for a violation.

E. Related Policies

- 21s – HIPAA Violation and Breach Reporting
- 7s - Confidentiality of PHI
- 34s -- Workforce Training Policy HIPAA
- List additional related policies: none

F. Related Forms

- AAs – Release of Information, Patient Rights and Breach Log
- Bs – Security or Privacy Event Reporting Form
- Cs –Security or Privacy Event Investigation Form
- Ns – Privacy Event Investigation Form
- List additional related forms: none

G. References

- For CEs: 45 CFR §164.530 (e)(1)
- For BAs: 45 CFR §164.504(e)(2)(ii)(B)
- Security Rule: 45 C.F.R. § 164.314(a)
- Stericycle Online Security Risk Assessment (SRA)
- SRA Line Item Numbers: B11, B12, b13
- List additional related references: none

Table of Example Security or Privacy Violations and Discipline

Level of Violation	Example	Minimum Disciplinary or Corrective Action
Careless without intent to harm	• Failing to log-off/close or secure a computer with PHI (Protected Health Information) displayed in a public area • Leaving a copy of PHI in a public area (such as an alcove on a floor) • Dictating or discussing PHI in a public area (lobby, hallway, cafeteria, elevator) • Leaving hospital payment or employee information in a public are (such as registration desk).	Organization Staff: First offense: written warning in personnel file (resulting in a .5% decrease on evaluation) Second offense: final written warning Third offense: termination Medical Staff: All matters shall be referred the Medical Staff bylaws for Corrective Action

Willful - acted deliberately with the intention to harm	• Sharing ID/Password with another co- worker or encouraging a coworker to share ID/Password • Sharing payroll information other than your own with another employee • Inappropriate access or allowing inappropriate access to PHI • Inappropriate disclosure or use of PHI • Giving an individual access to use your electronic signature • Using PHI for personal gain • Tampering with or destroying PHI or other Hospital information in an inappropriate manner • Repeated indirect violations	Organization Staff: 1st offense: Suspension or initiate termination of employment* • Medical Staff: All matters shall be referred to the Medical Staff bylaws for Corrective Action** • *** Individuals may be subject to civil and/or criminal liability** • ****Medical Staff members will be reported to licensing board and may be subject to civil and/or criminal liability**

HHS, OCR or Other Regulatory Investigations

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

11/28/2021

C. Purpose

The purpose of this policy is to provide guidance on managing investigations from HHS (Health and Human Services) Office for Civil Rights (OCR) or other privacy and / or security regulators and enforcement agencies.

D. Policy

It is the policy of this Organization to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS, OCR or other regulatory bodies. And to not impede or obstruct any HIPAA privacy / security related investigations conducted by one of these agencies. Also to provide all documentation or assistance required by law or regulation in connection with any HIPAA related investigations conducted by one of these agencies.

The Office for Civil Rights (OCR) enforces HIPAA Privacy and Security violations and may act from complaints filed by individuals or upon internally generated Audits. Remember that OCR-initiated actions are from the United States Federal venue and are to be taken very seriously. Rules of procedure, response dates and formats are to be followed to the letter.

HHS / OCR investigations for Privacy and Security should trigger litigation response processes, with Legal Counsel involvement if the risk is deemed at a level to warrant their involvement. Litigation Response procedures should work to keep the records in question (and their associated meta-data) secure while also preventing spoliation of evidence (unauthorized withholding, hiding, altering, or destroying).

OCR will notify the Covered Entity (CE) via letter when an allegation of a HIPAA violation is issued. To the extent practical, OCR will seek the cooperation of the CE to informally resolve complaints. For example, OCR can provide technical assistance to help a covered entity voluntarily comply with the Privacy and Security Rules.

A CE has the right to respond to an allegation by submitting evidence to OCR indicating; the alleged violation did not occur as described by the complainant; the action complied with Privacy and Security Rules; or the CE has taken prompt and effective action to correct the non-compliance. The last allegation response listed, taking corrective action, is very important to document in your response.

If the CE and OCR are unable to resolve the matter voluntarily, and if OCR's investigation results in a finding that the CE is not complying with the Privacy and Security Rules, HHS may initiate formal enforcement action which may result in the imposition of monetary penalties. Further, certain violations of Privacy and Security may result in criminal prosecution by the US Department of Justice. Penalties will vary significantly depending on factors such as the date of the violation, whether the CE knew or should have known of the failure to comply, or whether the CE's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

A penalty will not be imposed for violations in certain circumstances such as if:

- The failure to comply was not due to willful neglect and was corrected during a 30-day period after the entity knew or should have known the failure to comply had occurred (unless the period is extended at the discretion of OCR); or
- The Department of Justice has imposed a criminal penalty for failure to comply.
- A penalty may be reduced by OCR if the failure to comply was due reasonable cause and the penalty would be excessive given the nature and extent of the non-compliance.
- Before OCR imposes a penalty, it will notify the CE and provide the CE with an opportunity to provide written evidence of those circumstances that would reduce or bar a penalty. This evidence must be presented to OCR within 30 days of the notice. In addition if OCR states that it intends to impose a penalty, a CE has the right to request an administrative hearing to appeal the proposed penalty.

Sample Real-World OCR Data Request Addendum

The following questions have been included in OCR Privacy Investigations.

Sample Data Request Language from an OCR Letter

1. Please submit the additional documentation requested below to support the Organization's position. You will have 20 days from the date of the data request letter to submit the evidence.

2. Please state your internal Policies and Procedures regarding the use and disclosure of PHI pursuant to 45 C.F.R. §* 164.502 (a) and 164.502 (h). If said policy is in writing, please submit a copy of the internal document.

3. Please submit a copy of the Organization's internal safeguards, policies, and procedures that it has implemented pursuant to the Privacy Rule at 164.530(c). Indicate the dates of any redrafting of the policies since April 14, 2003.

4. Please state whether you conducted an internal investigation of the allegations contained in this complaint, if so, please submit a copy of your findings and state, in detail, any corrective action(s) taken by the Organization. If no corrective action was taken, please state the reason(s) why.

5. Please submit an access audit of Individuals Name electronic medical record showing which

employees of the Organization accessed his records during Time Period.

6. Please submit an Accounting of Disclosures for Individuals Name designated record set pursuant to 45 C.F.R. § 164.528.

7. Please state whether the Organization has provided training to all members of its workforce on the Policies and Procedures with respect to PHI in compliance with 45 C.F.R. § 164.530 (b)(i) of the Privacy Rule.

8. Please submit a copy of the Organization's internal policies and/or procedures regarding sanctions against employees who violate any of the provisions of the Privacy Rule pursuant to 45 C.E.R. § 164.530 (e)(1), including, but not limited to, verbal or written reprimands, mandatory training, suspension, and/or termination.

9. Please state whether any employees were sanctioned by the Organization in compliance with 45 C.F.R. §164.530 (e)(l) due to the allegations contained in this complaint, including the date the sanction occurred and the type of sanction enacted. If no sanction occurred, please state the reason(s) why no employees were sanctioned.

10. Please outline steps you are willing to take resolve the situation described in the complaint (i.e. retraining employees, polish existing privacy policies, sanction the employees making the disclosures, etc.).

Additional possible sample language:

1. Submit a copy of the internal policies and/or procedures regarding sanctions against employees who violate any of the provisions of the Privacy Rule pursuant to 45 C.F.R. § 164.530 (e)(1), including, but not limited to, verbal or written reprimands, mandatory training, suspension, and/or termination.

2. Please state whether your company has provided training to all members of workforce on the policies and procedures with respect to protected health information in compliance with 45 C.F.R. § 164.530 (b)(1) of the Privacy Rule. Please specify the date of the last training and provide verification that your workforce received training

3. Please outline steps you are have taken and/or are willing to take resolve the situation described in the complaint (i.e. retraining employees, provide access to PHI, issue an apology letter, polish existing privacy policies, sanction the employee(s) making the disclosures, etc.).

If an Investigation Is On-site

Workforce members who are designated to assist with these types of investigations conducted must adhere to the following:

- Cooperate, but do not volunteer information or records that are not requested.
  - Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D.,

call legal counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. Ensure that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.)

- Have at least one, if not two witnesses available to testify as to your requests and their responses.
- Ask for the name and telephone number of the lead investigator's supervisor, but only if, in your judgment, his/her demeanor indicates that you can ask such a question without engendering "hard feelings." Under no circumstances should you take any action to escalate tensions, except if you genuinely doubt the identity or authority of the investigators.
- Determine if there are any law enforcement personnel present (i.e., FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation.
- Permit the investigators to have access to protected health information ("PHI"), in accordance with the Organization's Notice of Privacy Practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.
- Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
- Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that the organization must provide witnesses to be questioned during the initial phase of an investigation.
- Do not instruct employees to hide or conceal facts, or otherwise mislead investigators.
- Ask the investigators for documents related to the investigation. For example, request:
    - Copies of any search warrants and/or entry and inspection orders
    - Copies of any complaints
    - A list of patients of interest
    - A list of documents/items seized
- Do not expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
- Don't leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- Don't offer food (coffee, if already prepared, and water, if already available, is ok). Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.
- Don't be "chatty." Only tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

Omnibus Enforcement Updates

- Enforcement provisions are very 'legal' in scope; consider involving legal counsel,

especially if any there is possible willful neglect.

- OCR currently conducts a preliminary review of every complaint received and proceeds with the investigation in every eligible case where its preliminary review of the facts indicates a possible violation of the HIPAA Rules.
    - OCR will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.
        - OCR would have continued discretion with respect to investigating any other complaints.
        - OCR may on a case-by-case basis expand the preliminary review and conduct additional inquiries for purposes of identifying a possible violation due to willful neglect.
        - Complaint investigations and compliance reviews clarify that OCR generally conducts compliance reviews to investigate allegations of violations of the HIPAA Rules brought to their attention through a mechanism other than a complaint.
        - Complaints or Compliance Reviews can be the basis of an investigation.
- Although OCR will encourage voluntary corrective action; enforcement can also skip right to civil or criminal penalties if they determine the need to, they are not required to work with the CEs / BAs for resolution rather than having to exhaust all informal efforts, especially for willful neglect.

Factors Considered in Determining the Amount of a Civil Money Penalty

- The general factors the Secretary of HHS will consider in determining a CMP (Civil Monetary Penalty).
    - The nature and extent of the violation
        - Time period during which the violation(s) occurred and the number of individuals affected
        - The nature and extent of the harm resulting from the violation
    - The history of prior compliance with the HIPAA (and administrative simplification) including violations by the covered entity or business associate
    - The financial condition of the covered entity or business associate
    - Such other matters as justice may require.
- The facts of the situation will determine whether reputational harm has occurred, such as whether the unlawful disclosure resulted in adverse effects on employment, standing in the community, or personal relationships.
    - In determining the nature and extent of the harm involved, the Organization may consider all relevant factors, not just those expressly included in the text of the regulation.

E. Related Policies

- 7s - Confidentiality of PHI
- 21s - HIPAA Violation and Breach Reporting
- List additional related policies: none

F. References

- Sample OCR Communication alleging HIPAA Privacy non-compliance, received November

2009.

- OCR Privacy investigation letter from late 2009
- 45 C.F.R. Part 160 Administrative Simplification: Enforcement Interim Final Rule
- Omnibus Privacy Final Rule Modifications, January 2013
- Subtitle D of the HITECH Act, sections 13400–13424
- Sample OCR Communication alleging HIPAA Privacy non-compliance, received November 2009.
- OCR Privacy investigation letter from late 2009
- 45 C.F.R. § 164.528
- 45 C.F.R. § 164.502 (a) & 45 C.F.R. § 164.502 (h)
- 45 C.F.R. § 164.530(c)
- 45 C.F.R. § 164.530 (b)(i)
- 45 C.E.R. § 164.530 (e)(1)
- 45 C.F.R. §164.530 (e)(l)
- 45 C.F.R. § 164.308, § 164.310, and § 164.312, others
- Stericycle Online Security Risk Assessment (SRA)
- SRA Line Item Number: B9
- List additional related references: none

Home Community Based Services Provider, Inc.

NOTICE OF PRIVACY PRACTICES

(includes Omnibus changes as of March 2013)

Effective Date: 11/28/2021

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

If you have any questions about this Notice of Privacy Practices ('Notice'), please contact:

Privacy Officer: Cathy Stein, CEO

Phone Number: 610-453-5005

Section A: Who Will Follow This Notice?

This Notice describes Home Community Based Services Provider, Inc. (hereafter referred to as 'Provider') Privacy Practices and that of any workforce member authorized to create medical information referred to as Protected Health Information (PHI) which may be used for purposes such as Treatment, Payment and Healthcare Operations. These workforce members may include:

- all departments and units of the Provider.
- any member of a volunteer group.
- all employees, staff and other Provider personnel.
- any entity providing services under the Provider's direction and control will follow the terms of this notice. In addition, these entities, sites and locations may share medical information with each other for Treatment, Payment or Healthcare Operational purposes described in this Notice.

Section B: Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive at the Provider. We need this record to provide you with quality care and to comply with certain legal requirements. This Notice applies to all of the records of your care generated or maintained by the Provider, whether made by Provider personnel or your personal doctor.

This Notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information.

We are required by law to:

- Make sure that medical information that identifies you is kept private;
- Give you this Notice of our legal duties and privacy practices with respect to medical information about you; and
- Follow the terms of the Notice that is currently in effect.

Section C: How We May Use and Disclose Medical Information about You

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

- **Treatment.** We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, health care students, or other Provider personnel who are involved in taking care of you at the Provider. For example, a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. In addition, the doctor may need to tell the dietitian if you have diabetes so that we can arrange for appropriate meals. Different departments of the Provider also may share medical information about you in order to coordinate different items, such as prescriptions, lab work and x-rays. We also may disclose medical information about you to people outside the Provider who may be involved in your medical care after you leave the Provider.

- **Payment.** We may use and disclose medical information about you so that the treatment and services you receive at the Provider may be billed and payment may be collected from you, an insurance company or a third party. For example, we may need to give your health plan information about surgery you received at the Provider so your health plan will pay us or reimburse you for the procedure. We may also tell your health plan about a prescribed treatment to obtain prior approval or to determine whether your plan will cover the treatment.

- **Healthcare Operations.** We may use and disclose medical information about you for Provider operations. These uses and disclosures are necessary to run the Provider and make sure that all of our patients receive quality care. For example, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for you. We may also combine medical information about many Provider patients to decide what additional services the Provider should offer, what services are not needed, and whether certain new treatments are effective. We may also disclose information to doctors, nurses, technicians,

health care students, and other Provider personnel for review and learning purposes. We may also combine the medical information we have with medical information from other Providers to compare how we are doing and see where we can make improvements in the care and services we offer. We may remove information that identifies you from this set of medical information so others may use it to study health care and health care delivery without learning a patient's identity.

- **Appointment Reminders.** We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at the Provider.

- **Treatment Alternatives.** We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.

- **Health-Related Benefits and Services.** We may use and disclose medical information to tell you about health-related benefits or services that may be of interest to you.

- **Fundraising Activities.** We may use information about you to contact you in an effort to raise money for the Provider and its operations. We may disclose information to a foundation related to the Provider so that the foundation may contact you about raising money for the Provider. We only would release contact information, such as your name, address and phone number and the dates you received treatment or services at the Provider. If you do not want the Provider to contact you for fundraising efforts, you must notify us in writing and you will be given the opportunity to 'Opt-out' of these communications.

Authorizations Required

We will not use your protected health information for any purposes not specifically allowed by Federal or State laws or regulations without your written authorization; this includes uses of your PHI for marketing or sales activities.

- **Emergencies.** We may use or disclose your medical information if you need emergency treatment or if we are required by law to treat you but are unable to obtain your consent. If this happens, we will try to obtain your consent as soon as we reasonably can after we treat you.

Psychotherapy Notes

Psychotherapy notes are accorded strict protections under several laws and regulations. Therefore, we will disclosure psychotherapy notes only upon your written authorization with limited exceptions.

- **Communication Barriers.** We may use and disclose your health information if we are unable to obtain your consent because of substantial communication barriers, and we believe you would want us to treat you if we could communicate with you.

- **Provider Directory.** We may include certain limited information about you in the Provider directory while you are a patient at the Provider. This information may include your name, location in the Provider, your general condition (e.g., fair, stable, etc.) and your religious affiliation. The directory information, except for your religious affiliation, may also be released to people who ask for you by name. Your religious affiliation may be given to a member of the clergy, such as a priest or rabbi, even if they do not ask for you by name. This is so your family, friends and clergy can visit you in the Provider and generally know how you are doing.

- **Individuals Involved in Your Care or Payment for Your Care.** We may release medical information about you to a friend or family member who is involved in your medical care and we

may also give information to someone who helps pay for your care, unless you object in writing and ask us not to provide this information to specific individuals. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.

- **Research.** Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another, for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with patients' need for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, but we may, however, disclose medical information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave the Provider. We will almost always generally ask for your specific permission if the researcher will have access to your name, address or other information that reveals who you are, or will be involved in your care at the Provider.

- **As Required By Law.** We will disclose medical information about you when required to do so by federal, state or local law.

- **To Avert a Serious Threat to Health or Safety.** We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

- ### Email Use.
  Email will only be used following this Organization's current policies and practices and with your permission. The use of secured, encrypted e-mail is encouraged.

Section D: Special Situations

- **Organ and Tissue Donation.** If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

- **Military and Veterans.** If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

- **Workers' Compensation.** We may release medical information about you for workers' compensation or similar programs.

- **Public Health Risks.** We may disclose medical information about you for public health activities. These activities generally include the following:
  - to prevent or control disease, injury or disability;
  - to report births and deaths;
  - to report child abuse or neglect;
  - to report reactions to medications or problems with products;

- to notify people of recalls of products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and
- to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

- **Health Oversight Activities.** We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

- **Lawsuits and Disputes.** If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

- **Law Enforcement.** We may release medical information if asked to do so by a law enforcement official:
  - in response to a court order, subpoena, warrant, summons or similar process;
  - to identify or locate a suspect, fugitive, material witness, or missing person;
  - about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
  - about a death we believe may be the result of criminal conduct;
  - about criminal conduct at the Provider; and
  - in emergency circumstances, to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

- **Coroners, Medical Examiners and Funeral Directors.** We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients of the Provider to funeral directors as necessary to carry out their duties.

- **National Security and Intelligence Activities.** We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

- **Protective Services for the President and Others.** We may disclose medical information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

- **Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary for the institution to provide you with health care, to protect your health and safety or the health and safety of others, or for the safety and security of the correctional institution.

Section E: Your Rights Regarding Medical Information about You

You have the following rights regarding medical information we maintain about you:

- **Right to Access, Inspect and Copy.** You have the right to access, inspect and copy the medical information that may be used to make decisions about your care, with a few exceptions. Usually, this includes medical and billing records, but may not include psychotherapy notes. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request.

- We may deny your request to inspect and copy medical information in certain very limited circumstances. If you are denied access to medical information, in some cases, you may request that the denial be reviewed. Another licensed health care professional chosen by the Provider will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

- **Right to Amend.** If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Provider. In addition, you must provide a reason that supports your request.

- We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:
    - Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
    - Is not part of the medical information kept by or for the Provider;
    - Is not part of the information which you would be permitted to inspect and copy; or
    - Is accurate and complete.

- **Right to an Accounting of Disclosures.** You have the right to request an 'Accounting of Disclosures'. This is a list of the disclosures we made of medical information about you. Your request must state a time period which may not be longer than six years and may not include dates before April 14, 2003. Your request should indicate in what form you want the accounting (for example, on paper or electronically, if available). The first accounting you request within a 12 month period will be complimentary. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- **Right to Request Restrictions.** You have the right to request a restriction or limitation on the medical information we use or disclose about you for payment or healthcare operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had. In your request, you must tell us what information you want to limit, whether you want to limit our use, disclosure or both, and to whom you want the limits to apply (for example, disclosures to your spouse). We are not required to agree to these types of request. We will not comply with any requests to restrict use or access of your medical information for treatment purposes.

You also have the right to restrict use and disclosure of your medical information about a service or item for which you have paid out of pocket, for payment (i.e. health plans) and operational (but not treatment) purposes, if you have completely paid your bill for this item or service. We will not accept your request for this type of restriction until you have completely paid your bill (zero balance) for this item or service. We are not required to notify other healthcare providers of these restrictions, that is your responsibility.

- **Right to Receive Notice of a Breach.** We are required to notify you by first class mail or by email (if you have indicated a preference to receive information by email), of any breaches of Unsecured Protected Health Information as soon as possible, but in any event, no later than 60 days following the discovery of the breach. “Unsecured Protected Health Information” is information that is not secured through the use of a technology or methodology identified by the Secretary of the U.S. Department of Health and Human Services to render the Protected Health Information unusable, unreadable, and undecipherable to unauthorized users. The notice is required to include the following information:
    - a brief description of the breach, including the date of the breach and the date of its discovery, if known;
    - a description of the type of Unsecured Protected Health Information involved in the breach;
    - steps you should take to protect yourself from potential harm resulting from the breach;
    - a brief description of actions we are taking to investigate the breach, mitigate losses, and protect against further breaches;
    - contact information, including a toll-free telephone number, e-mail address, Web site or postal address to permit you to ask questions or obtain additional Information.

In the event the breach involves 10 or more patients whose contact information is out of date we will post a notice of the breach on the home page of our website or in a major print or broadcast media. If the breach involves more than 500 patients in the state or jurisdiction, we will send notices to prominent media outlets. If the breach involves more than 500 patients, we are required to immediately notify the Secretary. We also are required to submit an annual report to the Secretary of a breach that involved less than 500 patients during the year and will maintain a written log of breaches involving less than 500 patients.

- **Right to Request Confidential Communications.** You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or hard copy or e-mail. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

- **Right to a Paper Copy of This Notice.** You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice. You may obtain a copy of this Notice at our website. hcbsprovider.com

To exercise the above rights, please contact the individual listed at the top of this Notice to obtain a copy of the relevant form you will need to complete to make your request.

Section F: Changes to This Notice

We reserve the right to change this Notice. We reserve the right to make the revised or changed Notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current Notice. The Notice will contain on the first page, in the top right hand corner, the effective date. In addition, each time you register at or are admitted to the Provider for treatment or health care services as an inpatient or outpatient, we will offer you a copy of the current Notice in effect.

Section G: Complaints

If you believe your privacy rights have been violated, you may file a complaint with the Provider or with the Secretary of the Department of Health and Human Services;

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

To file a complaint with the Provider, contact the individual listed on the first page of this Notice. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

Section H: Other Uses of Medical Information

Other uses and disclosures of medical information not covered by this Notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

Section I: Organized Healthcare Arrangement

The Provider, the independent contractor members of its Medical Staff (including your physician), and other healthcare providers affiliated with the Provider have agreed, as permitted by law, to share your health information among themselves for purposes of treatment, payment or health care operations. This enables us to better address your healthcare needs.

HIPAA Security and Privacy Awareness Workforce Training Policy

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

11/28/2021

C. Purpose

This policy establishes the Organization Security (and Privacy) Awareness Training Program in order to establish and promote the highest levels of security and privacy compliance and protections for all protected health information (PHI) accessed, used and disclosed by workforce members.

D. Policy

The Organization's Privacy and Security Officer(s) are responsible for providing direction and oversight of the provision of workforce privacy and security training.

The Organization recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations and that it must comply with HIPAA regulations in reference to the training of workforce members, in accordance with the requirements at § 164.530(b) and§ 164.308(a)(5). This Organization believes effective and complete HIPAA training programs, in combination with appropriate HIPAA resources, can significantly reduce the possibilities of HIPAA violations and breaches of confidential information. HIPAA training, at minimum, shall include the basics of HIPAA regulations and best practices; the basics of HIPAA's privacy and security requirements and restrictions; and review of relevant and appropriate policies and procedures related to HIPAA compliance. Regular messages and reminders in reference to HIPAA security awareness, as well as those related to privacy, will also be utilized. HIPAA awareness resources should strive to maintain a high level of HIPAA awareness amongst the workforce members, and a protective attitude toward confidential data on an ongoing, daily basis.

Workforce members will be trained at new hire training. All workforce member training shall be tailored to job roles, responsibilities and access rights to PHI, including methods of and requirements for authentication (i.e. logons).

Workforce members shall have training annually or upon material changes introduced by regulation, if their duties are impacted by these regulations. Exceptions to these training timing cycles may occur if material changes make additional training necessary during the time between regular training cycles and schedules. Also there may be requirements from OCR (Office for Civil Rights), State Agencies or other similar bodies that mandate additional or custom training. All additional training will be facilitated in compliance with requirements generated by that action.

Documentation of this training must be kept in an organized reproducible manner for a period of not less than six (6) years. Records of all workforce training shall be kept and produced upon request by regulators or other authorized parties.

Note: While Business Associates may not be technically required under HIPAA regulations to train their workforce it can be implied that this is a safeguard and a necessary part of a Business Associates privacy compliance program and may be included in BA Agreements; therefore BA workforce members should be trained in the same manner and frequency as Covered Entities.

none, they are contracted with HCBS Provider, Inc

E. Related Policies, Materials and Forms

- HIPAA Privacy and Security Awareness Training Presentation for Workforce Members
- HIPAA Workforce (Privacy Training) – Test and Test Key
- HIPAA Workforce (Security Training) –Test and Test Key
- 7s – Confidentiality of PHI
- 21s – HIPAA Violation and Breach Reporting
- 26s – Sanctions, Enforcement and Discipline
- 6s – Appropriate Access to PHI by Workforce
- 115s – Access Controls Policy
- List additional policies, materials and forms: none

F. References

- Stericycle Online Security Risk Assessment (SRA)
- SRA Line Item Numbers: B12, B46, B47, B48, B49, B51, B52, B53, B54, B55, B56, B75
- 45 CFR Parts 160 and 164 (HIPAA) §164.530
- 45 CFR § 164.308(a)(5).
- OCR Business Associates FAQ
- Bricker and Eckler Attorneys at Law web reference regarding BA training: Published on the Bricker and Eckler Website, Adapted by CompliancePro Solutions on September 14, 2011
- The Administrative Requirements: Training Section 164.530(b)
- As Contained in the HHS HIPAA Privacy Rules:
    1. *Standard: training*. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.
    2. *Implementation specifications: Training*.
        i. A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
            A. To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
            B. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
            C. To each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

ii. A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

Business Associate Training Requirements

Comment: Some commenters were concerned that there was no proposed requirement for business associates to receive training and/or to train their employees. The commenters believed that if the business associate violated any privacy requirements, the covered entity would be held accountable. These commenters urged the Secretary to require periodic training for appropriate management personnel assigned outside of the component unit of the covered entity, including business associates. Other commenters felt that it would not be fair to require covered entities to impose training requirements on business associates.
Response: We do not have the statutory authority directly to require business associates to train their employees. We also believe it would be unnecessarily burdensome to require covered entities to monitor business associates' establishment of specific training requirements. Covered entities' responsibility for breaches of privacy by their business associates is described in §§164.504(e) and 164.530(f). If a covered entity believes that including a training requirement in one or more of its business associate contracts is an appropriate means of protecting the health information provided to the business associate, it is free to do so.

Digital Copier and Device Privacy

A. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members (i.e. employees, contractors and volunteers) who utilize digital printers, photocopiers, scanners or other medical devices with internal hard drives or memory.

B. Create / Revision Date

11/28/2021

C. Purpose

To define guidelines for managing digital devices with the intent to prevent Protected Health Information (PHI) breach and / or HIPAA violations arising from PHI storage on the hard disk drives or memory of these digital devices.

D. Policy

The Organization has adopted this policy to ensure that PHI is not wrongfully disclosed by way of stored images or data memory within digital copiers, printers, scanners, medical devices, and fax machines.

Since 2002, most digital printers, photocopiers, scanners and fax machines have been manufactured to operate with an internal hard drive or memory that captures images of every document processed. Safeguards to protect information on these devices must be followed to prevent possible HIPAA violations and/or breaches caused by theft, unauthorized access, use, or disclosure; improper modification or destruction of data.

As a general rule, the Organization requires all copier, scanner and medical device companies to sign Business Associate Agreements and acknowledge that their technicians are trained on secure management of PHI.

E. Procedures

Information security policies and safeguards for protecting data stored on digital copiers and other devices may include the use of automated software routines that wipe clean any stored images on a routine basis. NOTE: NIST 800-66 guidance for destruction must be followed. Other mechanisms for securing data may include the use of passcodes or encryption of all images on these disks. Again, NIST 800-66 encryption guidelines should be utilized to create *secured PHI* or destruction of stored images by technicians on scheduled or on-demand basis.

Procedures for new equipment procurement

a. When buying or leasing new equipment, investigate and evaluate manufacturer options for securing data on digital devices. Ensure that sales representatives selling/leasing the equipment are aware of the Organization's security concerns and requirements.

b. Procure software or other mechanisms that, ideally, destroy or encrypt according to NIST 800-66 guidelines (creating *secured PHI)* stored images immediately after each use or on a set basis, such as daily.
c. Set-up routine maintenance procedures to investigate whether or not this image destruction is occurring.

For existing equipment (already purchased)

a . Investigate with the vendor of the product the status of stored images and hard drives within each copier, scanner and medical device.
b . Determine if auto destruction or encryption routines are available for each unit and institute if possible.
c . Ensure that routine and on demand maintenance visits by technicians address this issue.
d . Never allow any equipment that may have hard drives to leave the premises without ensuring that all stored images have been destroyed or encrypted.

Equipment that is to be sold, traded, or disposed of

a. Determine the hard drive and stored image status of any machines to be sold, traded or disposed of before they leave the Organization property.
b. Ensure any hard drives are completely scrubbed clean (preferably according to NIST 800-66 destruction guidelines) prior to leaving the Organization's property.
c. Hard drives may be crushed or rendered unusable through certified destruction as an alternative to scrubbing.

F. References

- Stericycle Online Security Risk Assessment tool (SRA)
- Omnibus Final Rules
- (SRA) Line Item: C.25
- List additional references: none

Email Policy

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 supportive staff, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Create / Revision Date

11/28/2021

C. Policy

The Organization's electronic mail has become an integrated tool in Organization business processes. This policy defines the requirements for email usage at the Organization. Electronic mail is designed to facilitate business communications and is not to be used in a way that may be disruptive, offensive to others or harmful to morale. Particular care must be given restricting the amount of PHI contained in any emails to the HIPAA Minimum Necessary and all emails containing PHI must be secured. This policy and all related procedures define the minimum requirements for Organization email usage and are applicable to all Organization workforce members.

D. Purpose

The HIPAA Security Rule specifies that covered entities must "implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.", and "implement procedures to verify that a person or entity seeking access to ePHI is the one claimed." The purpose of this policy is to define appropriate standards for secure and effective use of the Organization electronic mail systems, and to comply with the privacy and security standards of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, including updated HIPAA Laws, Rules and Regulations and State Statutes and Regulations concerning the privacy and security of PHI.

E. Procedures

General Use – Email

Organization email systems shall be used primarily for business use. Personal use of Organization email systems shall be limited to a level that does not impede worker productivity. The content of all emails shall be used in a way that does not disrupt or offend others, harm morale or create security exposures. Members of the Organization workforce shall ensure that the business information contained in email messages is accurate, appropriate and lawful. When sending email attachment files, caution shall be taken by members of Organization's workforce that the correct file is being attached. Recipient's authentication shall be performed (by the sender) prior to the transmission of all Organization emails to ensure that the content is only accessible by the intended recipient.

User Responsibilities

The user is any person who has been authorized to read, enter, or update information created or transmitted via Organization electronic mail system. Electronic mail is to be used as a business tool to facilitate communications and the exchange of information needed to perform an employee's job. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any business activity.

Users have an obligation to use email appropriately, effectively, and efficiently. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

Organization email accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

Right to Monitor Email and Communications

Management reserves the right to audit an employee's email and communication system files (including email files). Messages generated within and/or transmitted through Organization email and/or communication systems are to be considered neither private nor confidential. Organization reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its email or communication systems for any purpose. Upon separation of service, members of the Organization workforce shall not retain any rights to contents of the Organization email and/or communications systems. Additionally, all messages distributed via Organization email and communication systems (including through non-Organization email addresses) are subject to monitoring by Information Technology (IT), and disclosure to law enforcement or government officials or to other third parties through subpoena or other processes.

Electronic mail information is occasionally visible to IT staff engaged in routine testing, maintenance, and problem resolution. Staff assigned to carry out such assignments will not intentionally seek out and read, or disclose to others, the content of email.

Management must advise and receive approval from the Human Resources Department, in conjunction with the HIPAA Security Officer, as appropriate, of their intent to review an employee's messages prior to accessing employee files.

Prohibited Uses

Certain activities are prohibited with regard to use of Organization email and communication systems. The list below provides a framework for activities that fall into the category of unacceptable use. This list is not exhaustive and Organization has the right to decide any activity is inappropriate at its discretion:

1. Using Organization email and communication systems for effecting security breaches or disruptions of network communication.
2. Engaging in any activity that is illegal under local, state, federal or international law while utilizing any Organization IT system or data.
3. Copying or transmission of any document, software or other information

protected by copyright and/or patent law, without proper authorization by the copyright or patent owner;

4. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.
5. Use of email system for unauthorized solicitation of funds, political messages, gambling, commercial, or illegal activities.
6. Disclosure of an individual's personal information or a patient's protected health information (PHI) without appropriate authorization.
7. Transmission of information to individuals inside or outside the Organization without a legitimate business need for the information.
8. Use of email addresses for marketing purposes without explicit authorization from the target recipient.
9. Forwarding of email from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the Organization without the express authorization of counsel.
10. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication.
11. Obtaining access to the files or communications of others with no substantial ORGANIZATION business purpose and beyond the individual's "need to know".
12. Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.
13. Sending external transmission of confidential information via Organization email and communication systems, including email attachments without proper authorization, authentication and encryption.
14. Excessive personal use and/or unethical use of Organization's email and communication systems.
15. Using Organization's electronic mail and other information systems, such as communication, in a way that may be disruptive, offensive to others or harmful to morale.
16. Opening, responding to, or forwarding email messages from any unknown source.
17. Displaying or transmitting sexually explicit images, messages, games, cartoons or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, marital status, veteran status, age, disability or religious or political beliefs. Email is subject to the Organization policy and procedures governing sexual harassment and discrimination. Sending or forwarding offensive material violates this policy as well as the business use policy.
18. Using Organization email and communication systems to solicit others for commercial ventures, religious or political causes, outside organizations not approved of by Organization, or in any other non-job-related situations.
19. Circumventing user authentication or physical security controls to access Organization email and communication systems.
20. Copying, transmitting or providing information about Organization email and communication systems to any individual without proper authorization.

This list is not considered all-inclusive or collectively exhaustive. Further questions regarding appropriate use of electronic mail should be directed to the employee's supervisor or Organization HIPAA Security Officer.

Confidentiality of Electronic Mail

Users of Organization electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore, users are to utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents. When email is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information.

These safeguards are as follows:

- Information considered confidential or sensitive should be protected during storage of the data utilizing encryption or password protection that ensure the information is not accessed by anyone other than the intended recipient.
- Any PHI transmitted must be the Minimum Necessary amount, as defined by HIPAA Policy.
- Confidential or sensitive information may be distributed to multiple recipients.
- Confidential or sensitive information is to be distributed only to those with a legitimate need to know.

The following internally generated notation is to be included on all email messages, including external email messages:

Confidentiality Notice: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

Please be aware that email communication can be intercepted in transmission or misdirected. Your use of email to communicate protected health information to us indicates that you acknowledge and accept the possible risks associated with such communication. Please consider communicating any sensitive information by telephone, fax or mail. If you do not wish to have your information sent by email, please contact the sender immediately.

Retention of Electronic Mail

Generally, email messages constitute temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of an email message, it may be considered a more formal record and should be retained pursuant to the Organization's record retention schedules.

Email will not be routinely made a part of any client's medical records by Organization. Email will be included in medical records only if there is a note otherwise documented in the medical record indicating that this copy is necessary and there is a direct relationship to care rendered during the encounter for which the medical record is serving as the business record documenting that care. The clinician recording the note about the email is responsible for making sure a copy of the email is placed into the medical record.

Electronic mail that users wish to or are required to retain must be moved to a permanent folder on their workstation.

Electronic mail tape back-ups are performed on a regular basis for the purpose of business recovery. Electronic mail data that could be used or relevant to an OCR investigation is retained for 6 years.

Organization Electronic Mail of Protected Health Information (PHI)

Emailing confidential patient information necessary for the performance of your job is specifically authorized within the Organization network if minimally necessary information is sent. Any email communication of confidential patient information (protected health information) to non Organization personnel or Organization personnel outside the Organization network is specifically disallowed, except under the following conditions:

1. The request for this type of release has been forwarded to Clinical Resource Systems/Health Information Management for review and processing.
2. The Patient/Designated Representative has signed a valid authorization specifically allowing such communication, and has been informed of all potential security risks and that this mode of transmission may not be secure. Organization staff will document such authorizations in the clinical record.
3. Verbal authorizations will be documented and witnessed on an authorization form by CRS/HIM, but are not considered an optimal method to communicate an authorization. If it is impractical to forward to CRS/HIM the request and rather than a verbal authorization, the e-mail authorization procedure listed below should be used.
4. The communication to an authorized recipient is accomplished in a way that it would be impossible to determine the identity of the patient if it were illegitimately intercepted.
5. The Patient/Designated Representative must be informed that the authorization to release may be revoked at any time in writing, except to the extent it has been acted upon. The authorization will be effective only long enough to answer the purpose for which it is given, and no further confidential information will be released without the execution of an additional authorization.

Note: Certain protected health information (PHI) require special consents, e.g. PHI related to HIV, genetic testing, venereal disease, psychotherapy notes, drug/alcohol. Emailing confidential information of this type is specifically prohibited by the organization workforce.

All misdirected email containing PHI must be documented and reported in accordance with the *Information Security - Breach Notification Policy*.

Email Authorization Procedure

This procedure is recommended as opposed to verbal authorizations to communicate PHI and patient information by email only if CRS/HIM reviews are not practical for a given circumstance.

Organization may obtain informed consent from a patient or designated representative through email by conducting the following consent exchange upon presentation of a patient query (this example is for an email exchange):

I will be happy to respond to your query but to do so by email you must provide your consent, recognizing that email is not a secure form of communication. There is some risk that any protected health information that may be contained in such email may be disclosed to, or intercepted by unauthorized third parties. I will use the minimum necessary amount of protected health information to respond to your query.

If you wish to conduct this discussion by email, please indicate your acceptance of this risk with your email reply. Alternatively, please call my office to arrange a phone conversation or office visit.

Note: Extra care should be taken by the sender to assure that the sender is confident of the correspondent's identity, that any PHI be kept to a minimum and that, as with phone or fax based exchanges, this consultation be documented in the patient's record if appropriate. Further, even when requested by a patient, the provider should decline to use email and refer to phone or office visit if she or he has any concerns about any aspect of the exchange.

Responsibilities:

Organization MANAGEMENT

Organization Management shall ensure their staff adheres to the requirements outlined in this policy and all subordinate procedures related to email and communication systems. Management must immediately report any known or suspected breach of security policy to the HIPAA Security Officer.

Organization WORKFORCE

All workforce members shall comply with this policy and all referenced policies to ensure privacy of sensitive information. Members of the Organization workforce shall report any known or suspected breach of this policy and/or its subordinate procedures to management or the HIPAA Security Officer.

Organization BUSINESS ASSOCIATES

All business associates of ORGANIZATION shall comply with this policy to ensure the privacy and security of protected health information (PHI). Any known breach, shall be immediately reported to the HIPAA Security Officer.

Organization INFORMATION TECHNOLOGY (IT)

Organization Information Technology (IT) shall maintain and update all policies related to email and communication system usage to ensure that they are comprehensive and consistent with local, state, federal and international law. IT shall ensure that all responsibilities for carrying out the requirements outlined within this policy are delegated to qualified staff. IT reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its email or communication systems for any purpose. The HIPAA Security Officer shall be made aware of any breach of security policy and advise Human Resources as to the severity of the breach.

Accountability

All Organization workforce members with access to Organization information systems who are found to be in violation of any part of this policy are subject to disciplinary action, up to and including termination of employment or contract and legal action. IT will immediately suspend email system access privileges to any authorized user when unacceptable use severely impacts system performance or security. Retaliatory action shall not be taken against individuals who identify and/or report violations of security policy.

F. Related Policies

- 21s - Breach Determination and Reporting
- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- 26s - Sanctions, Enforcement and Discipline
- List additional related policies: none

G. References

- HIPAA Security Rule 45 CFR §164.308
- Stericycle Online HIPAA Security Risk Assessment (SRA)
- SRA Line Item Number: D34
- NIST 800-53 Recommended Security Controls for federal Systems
- 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information
- List additional references: none

Business Associate 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. 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

11/28/2021

C. Purpose

The purpose of this policy is to provide guidance on management of the Organization's Business Associates (BAs) and their Contractors.

D. Policy Statement

a. This Organization establishes and maintains relationships with Business Associates that are in full compliance with all the requirements of HIPAA.
b. Business Associates must access, use and disclosure PHI (Protected Health Information) strictly in accordance with the written Business Associate Agreement (BAA) they maintain with this Organization.
c. Under HIPAA Omnibus Privacy Final Rule the definition of a Business Associate includes an entity that 'creates, receives, maintains, or transmits' protected health information on behalf of a Covered Entity (CE).
d. The definition of a Business Associate includes a 'subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate'. Subcontractor means: 'a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.'
e. A CE may treat a contractor who has his or her duty station onsite at a covered entity and who has more than incidental access to PHI as either a member of the CE workforce or as a BA for purposes of the HIPAA Rules.
f. An external researcher is not a BA of a CE by virtue of its research activities, even if the CE has hired the researcher to perform the research. This is an example of a technical change or clarification; sites may need legal guidance in this area if in it is question.
g. The responsibility for maintaining compliant relationships with our Business Associates shall reside with our designated HIPAA (Privacy and/or Security) Officer(s), who shall ensure that all aspects of our Business Associate relationships are compliant and who shall ensure that Protected Health Information is properly protected and safeguarded by our Business Associates.
h. Business Associates are responsible for their Contractor's HIPAA compliance, however the Covered Entity sets the guidelines and ultimately the levels of HIPAA compliance the Contractors must also meet by way of specifics called out in our Business Associate Agreement language.
i. The duties and responsibilities of the designated Privacy and/or Security Officer(s) managing Business Associate compliance includes seeing that:

i. PHI is protected and safeguarded in a HIPAA compliant manner (and according to other applicable regulations, if any) by our Business Associates and their Contractors.
ii. Business Associate Agreements meet all HIPAA requirements and standards, including HITECH Act regulations and the requirements of applicable State laws.
iii. Business Associates have proper and appropriate safeguards in place for the PHI they manage and PHI managed by their Contractors.

j. Business Associates must comply with HIPAA and report to this Organization, in its role as a Covered Entity, any privacy and security events (or incidents) they discover that could be determined to be a 'Violation' or 'Breach' as defined under HIPAA and outlined within the Business Associate Agreement. Business Associates must immediately report their own 'events' (or incidents) that need investigation (within the BAA allowable timeframe) and those of their Contractors as well.
k. The BAA shall guide the roles and responsibilities of our Organization, the Business Associate and their Contractors, including Breach determination and notification for which HIPAA allows options where BAs may be designated to perform Breach determination or reporting. Under all circumstances this Organization retains control of the final Breach determination and reporting, even if Business Associates are allowed or required to perform them.
l. All 'Patients' Rights' are also required of Business Associates. Amendments, restrictions on the use or disclosure of PHI, Accounting of Disclosures, Confidential Communications, and Right to file complaints with OCR (Office for Civil Rights) are all required of Business Associates as they are of Covered Entities, if applicable to the roles performed by the BA.
m. This Organization shall assess and monitor our Business Associates' privacy and security safeguards. Business Associates must assess and monitor their Contractors according to their roles. Business Associates and their Contractors are required to follow all HIPAA Privacy and Security rules as applicable to their roles.
n. All BAs and their Contractors are responsible for following *Minimum Necessary* guidelines as required for their roles.
o. A person or entity becomes a BA by definition, not by the act of contracting (or operating under an agreement with a CE). Liability for impermissible uses and disclosures attaches immediately when a person or entity creates, receives, maintains, or transmits PHI on behalf of a CE or BA and otherwise meets the definition of a BA.
p. PHI created, received, maintained, or transmitted by a Business Associate may not necessarily include diagnosis-specific information, such as treatment information and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a CE, then it is PHI by definition and it must be protected by the BA in accordance with the HIPAA Rules and its Business Associate Agreement.
q. Per the HIPAA Omnibus Final Rules issued in January of 2013, Business Associates are directly liable under HIPAA Rules.
    - BAs are directly liable under the Privacy Rule for uses and disclosures of protected health information that are not in accord with its Business Associate agreement (BAA) or the Privacy Rule.
    - BA is directly liable for providing information to OCR for investigations and notifying CEs of potential violations.
    - BA is directly liable for failing to utilize *Minimum Necessary.*
    - For impermissible uses and disclosures of PHI.
    - For a failure to provide breach notification to the covered entity.
    - For a failure to provide access to a copy of electronic protected health information to either the covered entity, the individual, or the individual's designee (whichever is specified in the BAA).
    - For a failure to disclose protected health information where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules.

- For a failure to provide an accounting of disclosures.
- For a failure to comply with the requirements of the Security Rule. Business Associates remain contractually liable for other requirements of the BAA.

r. Business Associate Agreements shall be documented and maintained, as all documentation used for HIPAA compliance in regards to the Business Associates or their Contractors, according to the HIPAA documentation policies, with a minimum retention of six (6) years.

E. Related Documents

- 29 -- Business Associate Agreement
- List additional related documents: none

F. References

- HIPAA Omnibus Privacy Final Rules – Issued January 2013
- Stericycle Online Security Risk Assessment tool
- Stericycle Online Privacy Risk Assessment tool

 45 CFR 164.302 - 164.318

- PRA Line Item: I.1, I.2, I.3, I.4, I.5, I.6, I.7, I.8, I.9, I.10, J.3
- SRA Line Item: E.1, E.2, E.3, E.4, E.5, E.6, E.7, E.8, E.9
- List additional references: none

Metadata, Non-text Data, Photo, Video and Audio Management

A. Coverage

Home Community Based Services Provider, Inc. (hereafter referred to as the 'Organization') workforce members that 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

11/28/2021

C. Purpose

The purpose of this policy is to provide guidance on the use and management of metadata, non-text data, photographs, videos and audio files.

D. Policy Statement

Documentation of Patient Care

In facilities where patient photography is used routinely to document patient care, the practice of patient photography in healthcare operations should be included in the HIPAA-mandated notice of information practices, as well as in the consent for treatment signed on admission. It is advised that a consent paragraph be inserted into the standard admission consent form. If images will be routinely recorded as part of a diagnostic or therapeutic procedure, this language may be incorporated into the consent form for that procedure.

- Healthcare providers should have written policies addressing (1) circumstances under which patient photography is permitted, (2) patient consent, (3) ownership, storage, and retention of the images, and (4) patient authorization for the release and/or use of images outside the organization
- Generally, the patient or his or her legal representative should give written consent before photography is done by anyone other than a friend or family member of the patient.
- Consent Form Policy Statement: HCBS Provider, Inc. does not post pictures of clients
    - The patient or responsible party must be informed prior to the photography of the use and purpose of the picture.
    - The patient or responsible party has the right to refuse.
    - The patient or responsible party has the right to withdraw consent at any time by contacting the compliance officer or appropriate workforce member.
- Requests for external disclosures of clinical photography that are not for treatment, payment, or operations require the patient's informed consent prior to the release. Examples or external disclosures requiring authorization include, but are not limited to:
    - Requests by law enforcement
    - Requests by social services
    - Requests by marketing
    - Newborn photographs available for purchase
- Photographs, videotapes, and other images should be clearly identified with the patient's

name, identification number, and date, and stored securely to protect confidentiality. If used to document patient care, they should be kept for the same time period state law requires medical records to be kept.

- Written authorization from the patient or his or her legal representative should be required before photographs, videotapes, or other images are released to outside requestors.
- List the circumstances where photography (and / or video or imaging) is allowed.
- Patient photos, videos and other imagines which can identify the patient are sensitive and must be correctly authorized and managed.
- Photographs, videos and other individually identifiable images are to be listed as components of the Organization's Legal health record.
- Training on the issues of photograph and image handling should be included in HIPAA-mandated privacy and security training of the work force, extended work force, Business Associates and Contractors.
- This Organization's Business Associate Agreements obligate Business Associates and any subcontractors to the same privacy standards regarding patient photography as those of the covered entity.
- Ownership of all photographs, videos and other identifying images is to be addressed by record type as a part of the inventory managed for these items.
- All photos, videos, and other images should be stored in a manner that ensures timely retrieval when requested. All recordings should be identified with the patient's name, identification number, and the date on which the recording was made. The name of the photographer or recorder may also be included. Because photographs, videotapes, and other images used to document patient care may be considered part of the patient's record, they should be kept for the same time period state law requires medical records to be kept.
- Unless otherwise required by federal or state law, photographs, videos, scans, and other images should not be released to outside requestors without specific written authorization from the patient or his or her legal representative. The authorization should state that the patient agrees to have the photographs released to the requestor and the purpose for which they will be used.
- If the patient wants the photographs for his or her own use, a copy may be provided unless otherwise prohibited by state law. Only the information pertaining to the persons who consented to the disclosure may be released. Editing or other means of protecting the information and images of the non-consenting parties must be done to protect their confidentiality. Patients may be charged a reasonable fee to cover the cost of duplication.
- Malpractice cases commonly use videotapes that contain a potentially questionable medical incident. There are many pros and cons to having a video recording of a special event or procedure, our Organization is aware of the liability risks involved. Videotaping surgery, childbirth, etc. must be performed according to procedure. These procedures will be used consistently to avoid charges of 'hiding' images in cases that may have involved malpractice.
- Document every video recording in the medical record. A videotape can be used to prove innocence as well as guilt and both parties are entitled to complete, unedited copies.
- Do not offer souvenir copies of facility-made videotapes.

Mobile devices (i.e. cell phones) offer unique challenges to healthcare providers and great care must be taken in their management. Their ability to take pictures or images of not only people, but of documents and computer screens is of concern.

- The use of mobile devices (i.e. cell phones) as imaging devices is strictly prohibited by practice staff.
- While it is impossible for this Organization to control mobile devices (cell phones) that may enter the practice by patients and families, the use of mobile devices as an imaging device must follow the guidelines as outlined in this policy. If at any time it is determined by this Organization that the imaging process is not in the best interest of the patient or organization,

the Organization may request the individual processing the images to discontinue. Failure to comply with this request by workforce members may result in the full force of sanctions as proscribed by policy.

- Failure to follow the clinical photography policy may result in the corrective sanctions up to and including termination.
- Examples of inappropriate photographs include a:
    - Physician using a personal digital camera in the ICU to take a patient's picture
    - Nurse using a general surgical authorization as consent for release of a clinical photograph in a nursing publication
    - Resident using a photograph in a research paper published in a national magazine without authorization
    - Physical therapist using a personal mobile device to take a picture of an interesting skin infection.
    - Workforce member taking pictures of PHI, sensitive or otherwise individually identifiable information as their own copy of files

Procedures and inventory tracking tables (i.e. IT DRS and devices containing PHI catalogs) to manage non-text data must include, but not be limited to:

- Equipment and media type evaluation. This policy and procedure investigates the type of non-text media device uses, including its ease of access, interoperability, and the ease of data transfer for long-term storage. Long-term retrievability and release of the non-text data is also a factor for consideration.
- Metadata and non-text data are to be examined for this Organization's Legal Health Record definition and inventory, but are not necessarily released upon routine disclosure request. There are many reasons these items may fall into eDiscovery, but minimum necessary is certainly one of them.
- Individual device operation and function. Details for each device that generates non-text media. Specific procedures address how the device interfaces or communicates with the EHR.
- Retention, retrieval, release, and destruction. Guidance on how long the non-text media is retained, how it will be stored, and the methods used for retrieval and release. This procedure can also address how non-text media will be securely destroyed per HIPAA / NIST guidelines once the retention period has elapsed.
- Non-text data needs to be confidential, secure, and readily available. This Organization ensures that every information system containing non-text data has the capabilities and controls necessary to effectively manage that data.
- There are four main types of non-text media commonly generated in healthcare organizations for clinical purposes: image, audio, video, and application media. These types of non-text media are expected to continue growing as technology advances.
    - Image media (e.g., jpeg, tiff, png files) include still images such as x-rays and photographs. Simple photo files are a single digital photo image such as those taken in a dermatology or pediatric clinic to document a rash or other ailment prior to treatment. Layered photo files are used when there is an overlay of annotations or drawings on a printed photo. Layered annotations are common in plastic surgery clinics and other cosmetic service clinics to document the "before" status and to illustrate the plan.
    - Audio media (e.g., wav, wma, mp3 files) are non-text media types that capture sounds, including heart sound files or voice recordings for speech therapy. Similar to other media, there are many different formats for capturing sound.
    - Audio files, such as transcription are typically not maintained after report generation (and authorizing signature) and may be discarded according to the Organization's documentation and retention polices.

- Video media (e.g., wmv, mov files) contain a time-varying picture image that uses color and coordinated sound. Examples include maternal ultrasounds, fetal monitors, and electrocardiogram activity. Subtypes describe how the video media are formatted, which can range from actual time-varied pictures and tracings to animated drawings. Examples of clinical uses for video files include the capture of a patient's gait when adjusting prosthetic devices and recording patient observations in behavioral health settings.
- Application media (e.g., Octet-Stream, PostScript) do not fit into the media categories previously mentioned. These media and data must be managed for compliance as are similar or related file types.

Documentation and management of all metadata, non-text data, pictures, video and related times will be managed for proper disclosure, investigated for possible wrongful disclosures and breaches and all compliance with privacy and Security regulations. This Organization's Privacy and Security officers share these duties

E. Policy Discussion

Metadata

Metadata can be thought of as data about data (i.e. indexing information, audit logs and data / time stamps on electronic signatures) is increasingly becoming important to not only the provision of care, but also the legal considerations of record management. Metadata may be routinely released upon request, but more often is left for eDiscovery processes. Metadata must be catalogued and evaluated with many of the same rules applying as do for Non-text (see below). Retention of metadata may or may not follow typical retention guidelines for other data types. The most important considerations for metadata retention are the legal record and regulatory timeframes. Legal health Record definitions may call for 10 year retention, whereas HIPAA requires 6. In this case the metadata probably should be kept for the entire 10 years. Metadata should be considered key data for court cases.

Non-text Data

This Organization is establishing policies and procedures for non-text data that establish clear criteria for retention and destruction, storage, access controls, and tracking of access and disclosures. This Organization has listed each type of non-text data as to whether it is included or excluded from the DRS (Designated Record Set). If non-text data are included in the DRS, decisions relating to retention, destruction, reproduction, and disclosure should mirror those applied to the designated record set. These decisions may differ if non-text data are excluded from the designated record set.

Non-text data must be treated as PHI containing individual identifiable health information. As such, it must follow the same state and federal retention requirements for PHI. Non-text data must be easily retrievable and reproducible in a timely fashion to meet individual requests as well as for business operations and compliance needs (e.g., outside audits, accreditation). Note: disaster recovery processes must also be included as part of the retention, retrieval, and reproduction policies.

Photography, Video and Other Types of Imaging

The use of patient photography, videotaping, digital imaging, and other visual recordings during patient care is commonplace. For example, scopes and surgical equipment may provide the capability of routinely recording events on videotape or digital media. Families may wish to record a child's delivery, and physicians and practices are increasingly use videotapes for seminars, teaching, and community education. Although patient photography may be fairly common, liability issues need to be considered and federal regulations observed.

Without proper precautions during a healthcare encounter, patient photography may make a healthcare provider liable for invasion of privacy. Courts have imposed liability primarily when the provider has exploited the patient for commercial benefit. However, courts have also imposed liability when the patient's name or likeness was used for non-commercial purposes, finding that even taking a picture without the patient's expressed consent was an invasion of privacy.

Healthcare providers may be subject to liability for publishing photographs or other images under the type of invasion of privacy known as public disclosure of embarrassing private facts. Before allowing patient photography, healthcare providers should consider why it is being done and how the images will be used.

Regulatory

HIPAA standards for privacy of individually identifiable health information address photographs and similar images both directly and indirectly. For example; health information as a concept implies inclusion of patient photography, meaning photography or other patient imaging can create individually identifiable information. If a limited data set is to be created photos, videos and images that can serve to identify the patient, especially full face views, must be removed. These images must also be considered for removal under the minimum necessary rule. HIPAA requires patient authorization for the release of protected health information, which includes patient photography, for purposes beyond treatment, payment, and healthcare operations.

Accreditation

The Joint Commission on Accreditation of Healthcare Organizations advises organizations to obtain informed consent from patients for purposes of patient photography. In the event that films are obtained prior to securing patient consent, the films should be sequestered from use or release pending receipt of an appropriate consent. The Joint Commission further advises that a confidentiality commitment be signed by anyone conducting filming or videotaping. This would be especially important to recognize when outsiders are involved because many organizations already require employees to sign annual confidentiality statements that should include patient photography within the commitment.

Uses of Photographs, Videos and Other Imaging Documentation of Abuse or Neglect

Laws in most jurisdictions require healthcare providers to report cases of actual or suspected abuse or neglect of children or adults. HIPAA provides for variation in state laws. Providers should check their state laws for specifics. Generally, photographs taken to document abuse or neglect do not require consent from the patient or his or her legally authorized representative. Such photographs may be submitted with the required report to the investigating agency, but they should not be used for other purposes (such as teaching) without authorization.

Research

Photographs taken as part of a research protocol should be approved by an institutional review board (IRB) or privacy board, as termed by HIPAA. Consent for such photography should be incorporated into the consent form the patient signs to participate in the research protocol. The HIPAA-directed privacy board (or IRB) should be directly involved in decisions related to practices regarding the collection and release of patient photography.

Medical Education, Teaching, or Publicity

Written authorization should be obtained before photographing patients for medical education, staff teaching, or publicity purposes. The patient or his or her legal representative should sign and date the authorization form. Anyone other than the patient who has the legal authority to sign should indicate his or her relationship to the patient. The signature should be witnessed, and the witness' signature should be included on the authorization form. The signed authorization form should be filed with the patient's health record. A new authorization form should be signed for each new series of photographs taken by individuals other than those named in prior authorizations. The authorization given for photography remains valid unless and until the patient or his or her legal representative withdraws or restricts the authorization.

Media or Law Enforcement

When representatives from the news media or law enforcement agencies ask to photograph a patient, permission may be given if (1) the patient's physician does not feel it would be detrimental to the patient and (2) the patient or his or her legal representative signs a written authorization form agreeing to the photography. HIPAA supports the patient's authority to grant authorization, provided no state laws to the contrary exist.

Photography of Newborns

If facilities routinely take photographs of newborns to give or sell to parents, consent should be obtained before this is done. A separate consent form may be used or a brief consent statement to this effect may be incorporated into the standard admission form.

Family

Consent is not needed for photography done by the patient's family members or friends as addressed in the provider's policies or procedures. If parents want to videotape a child's delivery, for example, it may be helpful to provide them with written information prior to the delivery. Allowances to discontinue taping if the physician deems it necessary should be included.

Telemedicine or Internet

Consent should be obtained before any photographs or other images are used in telemedicine or on the Internet. The images, along with the complete medical record, should be encrypted to protect the patient's privacy. The technology used in some telemedicine and the Internet may not support the media originally used to record the patient data. Video, scans, or photo images may have poor resolution resulting in misinterpretations. Quality monitoring should be performed periodically to verify the quality of images transmitted.

F. Related Procedures

- List specific procedures related to metadata management
- List specific procedure related to Non-text management
- List specific procedures related to patient photography, video and other individually identifiable imaging
- Inventory DRS components of metadata, non-text data, photos, videos and other individually identifiable images
- Inventory where and when photos, videos and other individually identifiable images may be utilized

G. Related Polices and Forms

- 6s - Appropriate Access to PHI by Workforce
- 2s - Documentation for Security and Privacy Compliance
- Retention Policy
- 8s - Minimum Necessary
- Consents and Authorizations for Photo's, Video's and other individually identifiable images
- 26s - Sanctions, Enforcement and Discipline
- List additional related policies: none

H. References

- Stericycle Online Security Risk Assessment™ (SRA)
- SRA Line Item Numbers: C23
- 45 CFR §164.302 - §164.318, 160.103, 164.514(b)(2)
- AHIMA Practice Brief Nov-Dec 2011 'Managing Non-text Media In Healthcare Practices'

- AHIMA Practice Brief 2002: Patient Photography, Videotaping, and Other Imaging
- List additional references: none

