A logo for a mountain company

Description automatically generated

POLICY AND PROCEDURE ON PHI, CLIENT RECORDS, HIPAA, AND CONFIDENTIALITY

**Policy:** Client records will be maintained in an organized, accessible, and confidential manner.

All information of people receiving services and the Person-Centered Support Plan are considered Protected Health Information and shall be kept confidential.

It is the policy of this agency that this information be conveyed in understandable terms so that any person receiving services and/or their guardians or authorized representatives know and fully understand it. Clarification on any part of the policy and procedure is always available upon request.

**Definitions: HIPAA-** HIPAA is the Federal Health Insurance Portability and Accountability Act 1996.The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

**PHI-** Protected Health Information (PHI) means individually identifiable health information, including, without limitation any information, whether oral or recorded in any form or medium that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Protected Health Information (PHI) includes, but is not limited to, any information defined as Individually Identifiable Health Information pursuant to 42C.F.R. § 160.103.

**Privacy Rule**- The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those health care providers that conduct certain health care transactions electronically. HHS published the Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, healthcare clearinghouses, and healthcare providers who conduct the standard healthcare transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003.

**Security Rule**- HHS published a final security rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005.

**Procedure:**

1. All confidential information will be safeguarded and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will be followed.
2. Records shall be made available for review at Pikes Peak Respite Services to authorized persons (person receiving services, their parent, guardian or Legally Authorized Representative within their scope of authorization) within a reasonable period of time as negotiated by the agency and the party seeking access, within 5 business days when possible.
3. An individual designated by Pikes Peak Respite Services shall be responsible for the record at all times during the examination of the record by entities other than employees of that agency.
4. At no time may a person examining a record remove anything from it or otherwise make changes in it, except as stipulated below:
5. The person seeking or receiving services, parent of a minor, guardian or authorized representative, if within the scope of his/her authority, objects to any information contained in the record, he/she may submit a request for changes, corrections, deletions, or other modifications.
6. The person seeking or receiving services, parent of a minor, guardian or authorized representative as appropriate, shall sign and date the request.
7. Pikes Peak Respite Services administrator will make the final determination regarding the request and will notify the requesting party of the decision.
8. If Pikes Peak Respite Services administrator denies the request, then the requestor has the right to have a statement regarding their request entered into the record.
9. Records or portions of records may be photocopied or otherwise duplicated only in accordance with written agency procedures, and any fee for duplication shall be reasonable pursuant to section 24-72-205, C.R.S., A person receiving services is entitled to one free copy of any information contained in his/her record. Agency records are the property of Pikes Peak Respite Services.
10. Any potential HIPAA breaches will be evaluated with the following criteria:
    1. The HIPAA Breach Notification Rule requires covered entities to notify affected individuals; HHS; and, in some cases, the media of a breach of unsecured PHI. Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.
    2. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
       1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
       2. The unauthorized person who used the protected health information or to whom the disclosure was made;
       3. Whether the protected health information was actually acquired or viewed; and
       4. The extent to which the risk to the protected health information has been mitigated.
    3. Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.
    4. There are three exceptions to the definition of “breach.”
       1. The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
       2. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
       3. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.
11. Breach Notification Requirements:
    1. Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.
    2. Individual Notice- Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information.
       1. This individual notice shall be provided in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
       2. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible:
          1. a brief description of the breach
          2. a description of the types of information that were involved in the breach
          3. the steps affected individuals should take to protect themselves from potential harm
          4. a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches
          5. contact information for the covered entity (or business associate, as applicable).
    3. With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate.  Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.
    4. Media Notice
       1. Covered entities that experience a breach affecting more than five hundred (500) residents of a State or Jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or Jurisdiction.
       2. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area.
       3. Media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.
    5. Notice to the Secretary
       1. In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information.
       2. Covered entities will notify the Secretary by visiting the HHS web site and [filling out and electronically submitting a breach report form](https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html).
       3. If a breach affects five hundred (500) or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than sixty (60) days following a breach.
       4. If, however, a breach affects fewer than five hundred (500) individuals, the covered entity may notify the Secretary of such breaches on an annual basis.
       5. Reports of breaches affecting fewer than five hundred (500) individuals are due to the Secretary no later than sixty (60) days after the end of the calendar year in which the breaches are discovered.
       6. Webpage to submit breach notification: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>
    6. Notification by a Business Associate- If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach.
       1. A business associate must provide notice to the covered entity without unreasonable delay and no later than sixty (60) days from the discovery of the breach.
       2. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.
    7. Administrative Requirements and Burden of Proof
       1. Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach.
       2. Maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required:
          1. its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure.
          2. the application of any other exceptions to the definition of “breach.”
       3. Covered entities are also required to comply with certain administrative requirements with respect to breach notification as outlined in this policy and procedure.
       4. All employees, providers, and volunteers of Pikes Peak Respite Services shall receive training on this policy and procedure and training on HIPAA and Confidentiality.
       5. Any employee, provider or volunteer found to be improperly handling HIPAA protected information shall receive corrective action up to and including termination.
12. Each person in service will have an individual Client Record containing, as applicable:
    1. Service Plans (SP) from the Case Management Agency (CMA)
    2. Internal PASA SP outlining
       1. services being rendered
       2. frequency of those services
       3. likes and dislikes of the person receiving services
       4. goals the person has to increase independence with their service
       5. a tracking sheet to monitor the progression of these goals.
    3. Interdisciplinary Team (IDT) notes, as applicable
    4. Case manager visit notes, as applicable
    5. Individualized Service notes
       1. to utilize internal methods to track member progress on reaching individualized goals for their services and behaviors
       2. in addition to tracking goals, the agency shall also track the scope of frequency, and duration of the service to verify that services are being provided in a manner that supports the goals of the individual
    6. Incident Reports
    7. Assessments, as applicable
    8. Progress Summaries
    9. Informed Consents or Notices, as applicable
    10. Human Rights Committee (HRC) reviews and recommendations, as applicable
    11. Community Access and Participation records, as applicable for residential services
    12. Fire Drills and Emergency Plan reviews, as applicable
    13. Physicians orders and MARs for anyone receiving medication administration support
    14. Comprehensive Medical Records, as applicable, for residential services
        1. Physicians Orders
        2. Annual Physical Exams
        3. Primary Care Physician exam records
        4. Immunization and lab records
        5. Special studies and diagnostic records
        6. Dental
        7. Vision
        8. Medical Specialists (neurology, cardiology, dietician, etc)
        9. Mental Health
        10. Therapies (Occupational, Physical, Speech)
        11. Adaptive equipment and medical device assessments and annual reviews
        12. Medication Administration Records
    15. Previous Year’s documentation
    16. CES, SLS, Day program services billed at Incremental units of service shall have documentation with the following contained:
        1. Location of service provided.
        2. Time and date service was provided, including beginning and end time.
        3. Name of individual rendering service.
        4. Service(s) rendered, and the exact nature of the specific tasks performed that align with the service definition(s) in 8.7500.
        5. Documentation of any changes in the Member’s condition or needs and action taken because of the changes.
        6. Units of service provided.
    17. Residential services billed at per-diem (daily) units of service shall have documentation with the following contained:
        1. Medication Administration Record (MAR) if applicable.
        2. Daily attendance tracker.
        3. Notes, which shall include:
           1. Activities Member participated in.
           2. Respite services or overnight stays elsewhere if applicable.
13. The current and previous year’s information will be maintained in each person’s individual Client Record. Documentation older than that will be archived for three (3) years following termination of services or the death of the person or as otherwise outlined in the Archiving and Purging policy and procedure.
14. Documentation of services provided will be reviewed monthly prior to submission for billing:
    1. Documentation will be reviewed to ensure it is completed as intended.
    2. Any corrective action or retraining will be completed in a timely manner with the employee/contractor.
    3. During this monthly review, Utilization of service hours will be calculated to ensure the person in service is receiving the hours outlined in the SP.
    4. Utilization will be reviewed prior to the next SP so changes needed for particular units can be requested based on the person’s desires and preferences.
15. Service documentation will be analyzed with documentation maintained in the Client Record
    1. Monthly data and documentation will be reviewed to monitor progress towards the person’s goals and ensure employees/contractors are documenting as the program outlines.
    2. Any corrective action or retraining will be completed in a timely manner with the employee/contractor.
    3. Data and documentation will be reviewed quarterly so that goals and objectives can be revised as they are/aren’t met.
    4. Care plans will be reviewed with the person in service on an annual basis, prior to the person’s SP, to decide if the program should be continued, modified, or if something different should be implemented.
16. Incident Reports (IRs) will be written as needed, see Incident Reporting Policy and Procedure.
    1. IRs will be maintained in each person’s Client Record
    2. Any follow up requested or required for the individual incident will be documented on the IR and maintained in the Client Record
    3. IRs will be tracked and reviewed agency wide at least quarterly for trends and to identify any problematic areas requiring corrective action
    4. Documentation of the quarterly IR review, tracking and trending along with any follow up recommendations and corrective actions taken will be maintained separate from the Client Record and can be found in the Incident Management Record
17. Informed Consents will be completed for any psychotropic medications that agency employees/contractors are responsible for administering. Informed Consents will be reviewed, updated and signed at least annually, or anytime the medication or dosage change. Psychotropic medications require HRC review.
18. Informed Consents will be completed for any Restrictive Procedure outlined in the person’s SP that Pikes Peak Respite Services is responsible for implementing. Informed Consents will be reviewed, updated and signed at least annually. Restrictive Procedures require a Care Plan, documentation of services related to the restrictive procedure and HRC review.
19. Rights Modifications require HRC review. Rights Modifications will have Informed Consent. Informed Consents will be completed by Pikes Peak Respite Services then supplied to the case manager to obtain the consent. Once completed the case manager will return the signed consent so Pikes Peak Respite Services can file it in the client record. Informed Consents will expire annually.
20. Safety Control Procedures will require informed consent. Informed Consents will be completed by Pikes Peak Respite Services then supplied to the case manager to obtain the consent. Once completed the case manager will return the signed consent so Pikes Peak Respite Services can file it in the client record. Informed Consents will expire annually. SCPs require HRC review.
21. As applicable for Comprehensive services, Fire drills and Emergency plan reviews will be completed following the person’s Health and Safety Plan and documented at least quarterly in each person’s individual file.
22. Community access and participation along with interactions with natural supports will be documented for people in comprehensive services. If a person chooses not to participate in an offered activity, the opportunity will be documented as well. These records will be maintained in each person’s individual file.
23. At the end of the SP year, all data and documentation will be moved to the back of the file to make room for the upcoming SP year. Any previous data/documentation from the year before that will be removed and archived.
24. All agency staff, providers, and contractors will take the HIPAA and Confidentiality training within 90 days of hire. Everyone with access to client records will follow HIPAA and Confidentiality standards

**Reference:**  The Health Insurance Portability and Accountability Act of 1996

Section 8.7402

Section 8.7408

Section 8.7500

HCPF Informational Memo 24-018

Incident Reporting Policy and Procedure

Archiving and Purging Policy and Procedure

10 C.C.R. 2505-10 Section 8.605

10 C.C.R. 2505-10 Section 8.606