**Purpose:**

The intent of these procedures is to establish criteria for safeguarding confidential information and to minimize the risk of unauthorized access, use, or disclosure. These procedures will be followed exactly by all persons covered under the organization’s HIPAA policies and procedures, and are required in order to comply with HIPAA.

**Guiding Principle:**

1. To ensure clients or participants can receive an accounting of disclosures of their protected health information, not including disclosures for purposes of treatment, payment or health care operations. Disclosures to business partners must be included in the accounting. Under the Health Insurance Portability and Accountability Act, covered entities must give clients or participants an accounting of disclosures, if requested. Clients or participants may request an accounting of disclosures that were made up to six years prior to the date of request.
2. The organization must take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of confidential information.
3. Safeguarding confidential information – organizational workplace practices
   1. Paper Communications and Records:
      1. Provide a list of measures that the organization is implementing to reasonably ensure the privacy of paper communications and records.
   2. Oral Communications and Records:
      1. Provide a list of measures that the organization is implementing to reasonably ensure the privacy of oral communications and records.
   3. Visual Communications and Records:
      1. Provide a list of measures that the organization is implementing to reasonably ensure the privacy of visual communications and records.
4. Safeguarding confidential information – The organization’s administrative safeguards
   1. Provide a description of measures the organization is implementing to reasonably safeguard files (i.e. individual passwords).

**Procedures for Implementation of the Safeguards:**

1. Maintain an accounting of disclosures of protected health information on each client or participant for at least six years.
2. Information that must be must be maintained (tracked) and included in an accounting:
   1. Date of disclosure.
   2. Name of individual or entity that received the information and their address, if known.
   3. Brief description of the protected health information disclosed.
   4. Brief statement of the purpose of the disclosure [or a copy of the individual’s written authorization] or a copy of the individual’s written request for disclosure.
   5. Multiple disclosures to the same party for a single purpose [or pursuant to a single authorization] may have a summary entry. A summary entry includes all information (2 a-d) for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.
3. Information that is excluded from the accounting and tracking rule are disclosures made:
   1. Prior to compliance deadline or prior to the entity’s date of compliance with the privacy standards.
   2. To law enforcement or correctional institutions as provided in state law.
   3. For facility directories.
   4. To the individual client or participant.
   5. For national security or intelligence purposes.
   6. To people involved in the client or participant’s care.
   7. For notification purposes including identifying and locating a family member.
   8. For treatment, payment, and healthcare operations.
   9. [Pursuant to an individual’s authorization]
4. All other disclosures of protected health information must be tracked. Disclosures are not limited to hard-copy information but any manner that divulges information, including verbal or electronic data release.
5. Disclosures may be tracked by a variety of internal processes that ensure accurate and complete accounting of disclosures.
   1. Computerized tracking systems that have the ability to sort by individual and/or date.
   2. Manual logs with one log per client or participant maintained in the client or participant’s health record using the organization’s “Disclosure Log”*.*
   3. Authorization forms maintained in the client or participant’s health record.
6. All systems must be maintained and accessible for a period of at least six years to meet the requirement of providing an accounting of disclosures for that time period.
7. Disclosures that are not accompanied by an authorization or a written request must be tracked by alternative computerized or hard-copy mechanisms.
8. A client or participant may make the request for an accounting in writing or orally. If the request is made orally, the department must document such on the general “Authorization” form or a “Request for an Accounting of Disclosures” form*.* The department must retain this request and a copy of the written accounting that was provided to the client or participant, as well as the name/departments responsible for the completion of the accounting.
9. A client or participant may authorize in writing that the accounting of disclosures be released to another individual or entity. The request must clearly identify all information required to carry out the request (name, address, phone number, etc.).
10. Provide the individual with an accounting of disclosures within 60 days after receipt of the request.
    1. If the accounting cannot be completed within 60 days after receipt of the request, provide the individual with a written statement of the reason for the delay and the expected completion date. Only one extension of time, 30 days maximum, per request is permitted.
    2. Requests can cover a period of up to six years prior to the date of the request.
11. Provide the accounting to the individual at no charge for a request made once during any twelve-month period. A reasonable fee can be charged for any additional requests made during a twelve-month period provided that the individual is informed of the fee in advance and given an opportunity to withdraw or modify the request.
12. Maintain written requests for an accounting and written accountings provided to an individual for at least six years from the date it was created.
    1. Maintain the titles and names of the people responsible for receiving and processing accounting requests for a period of at least six years.
13. Safeguarding confidential information – Organizational workplace practices
    1. Paper Safeguards
       1. Files and documents being stored:
          1. Provide a list of measures that the organization is implementing to reasonably safeguard files and documents that are being stored.
       2. Files and documents awaiting disposal/destruction:
          1. Provide a list of measures that the organization is implementing to reasonably safeguard files and documents that are awaiting disposal/destruction.
       3. Shredding of files and documents authorized consistent with record retention requirements:
          1. Provide a list of guidelines that the organization is adopting with regards to shredding documents to reasonably ensure the privacy of those documents.
    2. Verbal Safeguards
       1. Organization staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs, and should be aware of risk levels.
          1. Locations of verbal exchange with various risk levels:
             1. Low risk: interview rooms, enclosed offices and conference rooms.
             2. Medium risk: employee-only areas, telephone and individual cubicles.
             3. High risk: public areas, reception areas and shared cubicles housing multiple staff where clients or participants are routinely present.
    3. Visual Safeguards
       1. Organization staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure.
       2. Computer screens: The organization must ensure that confidential information on computer screens is not visible to unauthorized persons. Suggested means for ensuring this protection include:
          1. Provide a list of guidelines that the organization is to reasonably ensure the privacy of information on computer screens.
       3. Paper documents: Organization employees must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

# Organization staff must take special care to ensure the protection and safeguarding of, and the minimum necessary access to, paper documents containing confidential information that are located on:

* + - * 1. Desks
        2. Fax machines
        3. Photocopy machines
        4. Portable electronic devices (e.g., laptop computers, palm pilots, etc.)

# Computer printers

# Common areas (e.g., break rooms, stairwells, restrooms, elevators, etc.)

1. Safeguarding confidential information – Organization administrative safeguards
   * 1. Provide a list of guidelines that the organization is to reasonably safeguard confidential information

**Related HIPAA Policies:**

* HIPAA Privacy Policy
* Minimum Necessary Information Policy
* Enforcement Sanctions and Penalties for Violations of Individual Privacy Policy

## Related HIPAA Forms and Documents:

* Request for an Accounting of Disclosures
* Disclosure Tracking Log
* Safeguards Assessment Tool
* Guidance for Managers and Supervisors

## Contact(s)

* Privacy Officer

Contact Information