| Policy Number: HC-4 | Page: 1 | Of: 2 |
|---|---|---|
| Title: Confidentiality Safeguards (Oral & Written) | | |
| Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC | | |
| Effective Date: 01/19/2021 | | |
| Reviewer/Job Title: Director of Operations | | |

## (A) CONFIDENTIALITY SAFEGUARDS (ORAL & WRITTEN)

HCBDD shall maintain appropriate physical, technical, and administrative safeguards to safeguard Paper and Oral PHI.

1) **Safeguards for Electronic PHI**. The HIPAA Security policies detail physical, technical and administrative safeguards to protect electronic PHI. In addition, these policies detail some of the physical security measures for paper records.
2) **Oral Privacy**
   A) Employees shall be aware of safeguarding oral communications. This includes being aware of surroundings, and using appropriate volume when speaking to prevent others from overhearing conversations.
   B) Employees shall refrain from holding conversations in common areas where individuals receiving services or visitors can overhear PHI.
   C) Discussions concerning individuals should be done in a private area and discussions must be limited to "need to know" information for purposes of providing the best services.
   D) Overheard conversations are not to be shared or repeated.
   E) When in a public place, any cell phone conversations should be conducted in a manner so as not to divulge PHI to bystanders.
3) **Safeguards for Written PHI**
   A) **Control of the Original Paper Records**
      i) The HIPAA Privacy Officer shall be responsible for administering the security controls for paper record storage.
      ii) Case and School records shall be kept in a locked and secured area. Employees requiring access to these records shall have a key and/or combination for the storage room or cabinet.
      iii) Paper files shall be put away promptly when not being used.
      iv) Original paper records shall not be removed from the building without the authorization of the superintendent, privacy officer or designee.
   B) **Other use and storage of paper records**
      i) Employees should minimize the use of hardcopy PHI.
      ii) Personal appointment books with names of Individuals being served should be safeguarded while away from the office. It is best to avoid putting last names in appointment books if possible.
      iii) Hardcopy reports and redundant copies of records personally maintained should be kept in a locked file drawer.
   C) **Faxing Procedure**

i) When faxing a document with PHI, use a cover sheet which indicates that information is confidential, protected under state and federal laws, and not to be re-disclosed.
ii) Care should be taken to transmit fax to the proper recipient.
iii) Faxed documents should not be left at a common fax machine.

D) **Printing and Copying PHI**
i) Printers and copiers used for printing of PHI should be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied is required to be strictly monitored.
ii) PHI printed to a shared printer should be promptly removed.
iii) The Privacy Officer shall monitor all printer and photocopier acquisitions. In the event that this equipment includes internal storage devices, which retain images of photocopies made, the asset shall be managed by the Director of Operations, especially upon disposal to insure destruction of any PHI contained in its storage.

E) **Transportation/outside use of documents with PHI**
i) Caseworkers and other employees who remove documents from the facility, to conduct fieldwork, for example, are responsible for safeguarding these documents.
ii) When leaving documents unattended in a personal vehicle, the vehicle should be locked. Preferably, the documents and/or their container should not be visible.
iii) If any documents with PHI are lost or stolen, the incident should be immediately reported to a supervisor.

F) **Visibility of records and other PHI**. All employees using records for individuals and other paperwork with PHI shall arrange these items so that PHI is not readily visible to other individuals receiving services/visitors, especially in high traffic areas such as reception area.

G) **Shredding**. Unneeded paper documents containing PHI shall be destroyed by shredding.

H) **Destruction of PHI in non-paper formats**. Any written PHI in non-paper formats, such as imprints on carbon films used in fax machines, should be destroyed appropriately.

I) **When leaving for the night**, all employees shall clean their desks of PHI to reduce exposures to cleaning personnel and others who may have access to the facilities at night.

J) **Confidentiality with Cleaning Personnel**. Cleaning personnel with access to the facility should be placed under a confidentiality agreement.

4) **Compliance Audits/Facility Review**. At least annually, the HIPAA Privacy Officer shall audit staff compliance with these guidelines. The audit shall consist of a walk-through of the facility, with observations recorded, such as placement of desks, location of computer equipment, any papers with PHI that would be visible to a visitor, etc. The results shall be discussed with the appropriate employee, and any appropriate actions taken.

5) **Enforcement**. All supervisors are responsible for enforcing this policy. Employees who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

6) **Annual Review**. These safeguards shall be reviewed and updated annually.