HUMAN RESOURCE POLICIES

PROTECTION, SECURE TRANSFER & RETENTION OF CLIENT RECORDS POLICY

Approval Date: August 30, 2019	**Approved by:** President & CEO
Revision Dates:	
CCA Accreditation Standards: ORG-SYS-3.1	
Cross Reference:	

POLICY

Boost CYAC takes measures to protect all client files and records. All hardcopy files and records are stored in locked filing cabinets. All electronic files and records are on a secure section of the Boost CYAC network with only authorized personnel having access (all files are password-protected). Electronic files and records may be securely stored on password-protected USB keys under the supervision of the appropriate manager. Appropriate measures are taken to ensure access to records is limited on a need-to-know basis to protect against any unauthorized access and exposure and to prevent the loss and destruction of files and records.

This policy provides guidance on the protection, retention and destruction of clinically sensitive materials, including physical and electronic client records.

PROCEDURE

PROTECTION OF CLIENT RECORDS

1. Client records are stored in locked program specific filing cabinets on site. Keys to filing cabinets are stored in a combination lock key cabinet, which can only be access by authorized leadership and clinical staff.
2. Upon accessing a client record, staff are responsible for returning the filing cabinet key to the lock box immediately.
3. Staff are responsible for returning any client records to the filing cabinets at the end of the working day.

SECURE TRANSFER OF CLIENT FILES

1. Client records that are authorized to be shared with an external parties may be transferred in the following ways:
    a. **By Mail**: in a secure envelope and delivered using registered mail or a courier and confirmation of receipt obtained from the recipient.
    b. **By Fax**: using a Boost CYAC cover sheet which is marked confidential and has a privacy statement on it.
    c. **By Email**: sent from a Boost CYAC email account and with a privacy statement attached. All documents must be password protected and the password sent in a secondary email to the recipient.
2. Transferring client files off site.

Some staff may need to transfer clinical files off site, including but not limited to another community agency, courthouse or their home office. In these situations, staff must take steps to protect the security of the client file at all times.

This includes:

- keeping files on their person at all times when out in the community
- keeping files in a locked container in their home office.
- not leaving files in their car during the day or overnight
- only accessing client files in the community, in a private setting, where confidentially can be maintained.
- Returning files to the Boost CYAC office as soon as possible, ideally at the start of the next business day.

3. All security breaches must be reported to the Program Manager and the President & CEO immediately.

RETENTION OF CLIENT RECORDS

1. When a client file is closed for active service, it will remain on site for a period of two (2) years. The Program Manager is responsible for separating client records that have reached this timeline and making arrangements with administrative staff to transfer them securely off site to an approved records management facility. Client files are maintained indefinitely.
2. With client consent, electronic recordings of client session may be kept for the purposes of training and supervision. Program Managers are responsible for keeping audiotape, videotape or CD's in a locked cabinet. Upon completion of supervision or training, or at client termination, the electronic recording is erased.