

EPISCOPAL SOCIAL SERVICES/Sheltering Arms

Client Privacy, Confidentiality and HIPAA

Episcopal Social Services (ESS) supports the maintenance of all personal and private information, including Protected Health Information (PHI), in a confidential manner for clients and staff, in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and other relevant law (e.g. HIV information, Substance Abuse information, maintenance of Clinical Progress Notes), as well as the ethics of good case practice. This policy applies to all ESS and affiliate staff, interns, volunteers, consultants and business associates. Confidential information includes verb oral, written, and electronic information.

- Program Directors insure that its program practices adhere to the legal requirements around confidentiality of the government agency to which it is accountable, as well as to the HIPAA.
- Each program has a written Privacy, Confidentiality and HIPAA policy, which adhere to agency policy, the HIPAA and the policy of the government agencies to which it is accountable.
- Program Directors insure that all his/her program staff knows, understands, and adheres to the agency and program policies around privacy and confidentiality.
- Program Directors insure that procedures are in place to insure that clients receive Notice of ESS HIPAA, Privacy, and Grievance procedures and sign receipt of such notice.
- Staff is informed that any questions related to HIPAA, privacy and confidentiality should be discussed with a supervisor or director prior to any release of information. Inquiries should also be directed to the ESS' designated Privacy Officer.
- All staff is responsible for all reporting of suspected HIPAA violations to the designated HIPAA Privacy Complaint Official.
- Upon request from a client, staff must provide a list of disclosures of that client's confidential information. Program Directors must be informed of all such requests and staff should consult with the agency's designated Privacy Officer as needed.

Disclosure of Confidential Information:

- Except when required or permitted by law or court order, confidential information is not disclosed to any third party without written consent from the individual to whom the information refers. In the case of a minor, parent/guardian consent is required unless the minor has capacity to consent and is permitted by law to consent.
- Written consent must include (See ESS HIPAA compliant consent form in **Appendix E**):
 - The information being requested
 - Purpose of the use or disclosure
 - Who may use or disclose the information
 - Who may receive the information
 - Expiration date or event
 - Individual's signature and date
 - Statement regarding individual's right to revoke authorization
 - Statement regarding individual's right to refuse to sign authorization
 - Statement regarding the conditions under which Re-disclosures is not protected
- Written consent forms cannot be signed by clients unless all information is filled in on the form.

- Except when required or permitted by law or court order, any information, written or verbal received from a third party will not be re-disclosed without explicit permission from the client and only if necessary for the provision of services.
- In the event that a staff member receives confidential client material from a third party in error, not pertaining to one of their clients, staff should immediately notify the sender and forward to the appropriate recipient, shred or return the material pending outcome of the discussion with the sender.
- Discretion should be used in communication of confidential information to third party with the idea in mind to disclose “the minimum amount necessary” - that information either required by law or court order or necessary to meet service needs.
- When sending or faxing confidential material, a “confidential” stamp or cover sheet with a confidentiality statement (see below) must be used to indicate the confidential nature of the material.
- No e-mail should be sent w/ client identifying information in the subject line.
- All fax and e-mail communications should be sent with the following confidentiality statement: “This communication, together with any attachments hereto or links contained herein, is for the sole use of the intended recipient(s) and may contain information that is confidential, privileged, or legally protected, and as such is not a public document. If you are not the intended recipient, you are hereby notified that any review, disclosure, copying, dissemination, distribution or use of this communication is STRICTLY PROHIBITED. If you have received this communication in error, please notify the sender immediately by return e-mail message and delete the original and all copies of the communication, along with any attachments hereto or links herein, from your system.”
- Communication among ESS staff (including between departments) around confidential matters will be conducted on an as needed basis and in a secure location, for the purpose of meeting service needs or enforcement of agency policy and practice. Discussions involving clients should not be done in any public forum, including but not exclusive of restrooms, hallways and elevators.
- No material should be posted or left visible in a public location with client names or other identifying information.
- ESS staff is expected to know and follow applicable laws around confidentiality specific to certain medical/service issues (e.g. HIV status, substance abuse).

Access to Files

- Access to case files is given only to staff assigned to a case, their chain of command, other department staff providing direct service to the client, the Quality Improvement Department, authorized government staff from the government agencies which oversee the program or those to whom the governing agency permits access, and authorized Council on Accreditation staff (COA) on site.
- All files must be maintained in locked cabinets and not be visible or unmonitored when not in use.
- Clients are permitted access to their case files upon reasonable request and in the presence of agency personnel and with careful attention paid to protection of confidentiality of other family members whose private information may be contained in the file. Such requests should be handled by the Program Director of above, in consultation with the designated Privacy Officer for ESS.
- Clients are permitted to add statements to their file and be informed of any responses to their statements added to the file. In the unlikely event that reviewing a file could be harmful for the

client or family member, the agency must proceed in accordance with the law in denying access. At the very least, an entry into the record must be made by a program director or above documenting the reason for denial of client access to their file.

- In order to prevent access to confidential information by unauthorized users, client-related documents should be saved to the user's H: Drive and never to a public folder or drive.
- Staff should not leave a work station with a computer unlocked, and if more than a brief absence from the work station is planned, staff should log off.
- Use of any computer system, CONNECTIONS or other program/agency program or database, for any purpose other than to service assigned clients or maintain ESS records is prohibited.
- Supervisors should be granted access to all workers documents in the event of absence of the worker, planned or unplanned.
- Upon cessation of employment from ESS, staff will relinquish access to any case-related information immediately and access passwords will be disabled.
- Any subpoena or governmental request for case material should be immediately brought to the attention of the Program Director or above in the chain of command, in the absence of the Program Director. The Program Director conferences the request with his/her chain of command before responding to the subpoena or government request. As needed, Senior Management will review the request with agency attorneys prior to responding.
- Carrying of case files off site presents an automatic risk of breach of client confidentiality and is not permitted unless a specific circumstance (e.g. court appearance) warrants it. Case files can only be transported off site with permission of a Supervisor or Director.

Record Retention and Disposal

- All programs will store and retain closed files for at least 10 years after case closing unless otherwise mandated by law. All programs store, retain and expunge closed files in accordance with its program mandates.
- Closed files may be stored off-site via procedure outlined by the Operations Department. A log must be kept by the program/department of all material housed in off-site storage, with specific information as to case/file name and box identification number, as well as date of delivery to storage site. Directors are responsible for monitoring storage and expungement schedules for closed files.
- Disposal of any written material with identifying and/or confidential information will be done by shredding.
- Electronic files will be retained and disposed of in accordance with Information Management procedures overseen by the MIS Department.
- Financial and Human Resources personnel files are retained and disposed of in accordance with the procedures described in the Finance and Human Resources manuals.