Section K: Persons Served Records

POLICY STATEMENT: Person Served Records

Adopted by the Board of Directors 02/24/2017

It is the policy of Open Options to create and maintain person served and administrative records in such a fashion as to ensure accuracy, clarity, and concise information, and to protect the confidentiality and privacy of individually identifiable health information in compliance with federal and state laws. Procedures governing the use and disclosure of protected health information (PHI) shall conform to the requirements of HIPAA (45 CFR Section 164.502 et. seq.) as well as applicable state laws and regulations. Procedures shall be established to:

a) Provide for regular and ongoing review of person served records to ensure that such records contain current, accurate, clear, and concise information and to ensure the presence of all material required by accreditation standards, contractual agreements with funding sources, and applicable state and federal laws;
b) Provide reasonable safeguards to protect the confidentiality and security of protected health information both within organization facilities and when working outside of organization facilities, and to safeguard against the possibility of loss or destruction;
c) Ensure that person served records and their contents will remain intact for a mandated timeframe (as dictated by contract or applicable regulations) and that destruction of person served records is conducted in such a manner as to safeguard the confidentiality of PHI.
d) Identify those records maintained by the organization that meet the definition of "designated record set" covered by the HIPAA Privacy Rule.
e) Provide to all persons served (or legal guardians, if applicable) access to the most current Notice of Privacy Practices, and to make a good faith attempt to have each person served/guardian acknowledge the Notice of Privacy Practices.
f) Obtain written authorization of the person served/guardian prior to using or disclosing protected health information for reasons other than treatment, payment, or operations, and as required by state law.
g) Verify identities of persons/organizations requesting information prior to disclosing protected health information.
h) Ensure that information disclosed is the minimum necessary to fulfill the purpose of the disclosure.
i) Provide Privacy training for all members of the workforce, including employees, volunteers, and student interns, as required by HIPAA.
j) Obtain a confidentiality agreement for outside business associates who have access to protected health information.

Open Options is committed to protecting the rights of persons served including specific rights related to the privacy of their records. Procedures shall ensure that:

a. A person served may access his or her own records as defined and allowed by law,
b. A person served (or legal guardian) who believes that information contained in the designated record set is incomplete or inaccurate may request an amendment or correction to the information, with recognition that such amendments may be limited or restricted as defined in such procedures, the Notice of Privacy Practices, or as allowed by law,
c. A person served (or legal guardian) may request specific restrictions on the use or disclosure of protected health information, with recognition that the organization is not required to agree to the requested restriction in accordance with federal regulations. (45 CFR Section 164.522 (a).)

d. A person served (or legal guardian) may receive a written accounting of disclosures made by this organization in accordance with federal law (45 CFR 164.528.)

PERSON SERVED RECORDS: CONTENT, REVIEW, RETENTION AND DESTRUCTION

PROCEDURES - All Programs

The Director of Community Living and Support Coordination in conjunction with the President/CEO shall designate the content of person served records in order to ensure the presence of all material required by state and federal laws, contractual agreements with funding sources, and accreditation standards, as well as information needed to provide adequate and reasonable treatment to individuals receiving services. Designated employees will be responsible for the overall control of the case record process and the implementation of organization standards and procedures for case records of the services they supervise.

Upon admission, a person served file shall be constructed by the designated employee according to the Person Served Record contents. All forms should be completed in their entirety - if information is not available it shall be marked "information not available."

Pertinent information on each person served shall be gathered at the time of admission for inclusion in the person served file and/or for records maintained at the administrative offices. Such information, including electronic files, shall be kept in lockable storage. Electronic files shall be kept on a password-protected computer.

Case Record Review

In keeping with the policy of the organization to provide for the regular and ongoing review of person served case records, department directors shall establish a process for the systematic review of case record adequacy. Where case record design and requirements vary between programs (e.g. community living and targeted case management) different processes may be necessary and function separately. Case record review systems may use peer reviewers, a committee, or outside consultants and must:

a. Review an appropriate sample of case records and provide a report of deficiencies to responsible employees.
b. Provide for follow-up on deficiencies noted and the correction of those deficiencies;
c. Conduct a periodic audit with HIPAA regulations;
d. Conduct a periodic review of the policies and procedures for person served record construction and maintenance, their adequacy to meet internal needs and, the standards of the Missouri Department of Mental Health, Kansas Social and Rehabilitation Services (as applicable) and CARF, and make recommendations to the appropriate employee(s) regarding these processes.

Retention and Destruction

Person served records and their contents will be retained for a period of seven years from the date of closing or discharge, unless otherwise stipulated in contracts with funding sources. Accounting of disclosures of information shall be retained at the administrative offices for a minimum of six years. Records shall be stored in a lockable office or file room. Overflow and inactive records may be stored off-site in a secure storage facility.

Destruction of person served records containing protected health information shall be conducted in a manner which safeguards the confidentiality of the information contained in the record. The following guidelines shall apply:

1. For paper documents, destruction shall render the document(s) unreadable. Appropriate methods may include shredding, pulping or pulverizing the document(s).
2. For electronic records, destruction shall be conducted in such a manner that the information cannot be retrieved. Appropriate methods may include overwriting the data, reformatting the disk, or physical destruction. Simply deleting the file does not destroy the data.
3. If services are contracted for the destruction of records, the contracting entity shall adhere to the terms of a business associate agreement in conformance with HIPAA regulations.

4. Records of destruction shall be maintained, including a description of the records, date of destruction, method of destruction, and person supervising the destruction.

CONFIDENTIALITY OF PERSON SERVED RECORDS

PROCEDURE - All Programs

In accordance with applicable State and Federal laws, all information regarding past, present, or pending persons served of any organizational program shall be maintained in the strictest confidence.

Privacy and confidentiality of person served records shall be consistent with regulations as set forth by Missouri Statute 630.140, Kansas Administrative Regulations and the Health Insurance Portability and Accountability Act of 1996 (45 CFR Sections 164 et. seq.) Such information and records include, but would not be limited to name, age, family names, diagnosis, placement history, place of employment, physical health data, hobbies/interests.

Information and records shall not be released or disclosed without a properly executed "Authorization for Exchange of Information" which is dated, time-limited, not to exceed one year in duration, signed by the person served or legal guardian, and which specifically lists the type of information to be shared. There are limited exceptions to the requirement for an Authorization for Exchange of Information. Refer to Procedures for Authorization for Release of Information in this manual.

Storage and Confidentiality

Person Served Records in a program site owned or leased by the organization shall be retained in a lockable room or locked cabinet. Access to the records is limited. The Division Directors shall designate access levels to person served records for positions under their supervision. Records shall not be removed from the facility except by employees in the line of job duties, and only with the approval of the supervisor of the location. Medical records shall not be removed while the person served is at home. Medical records may be removed while accompanying a person served to a medical appointment, or for a short period (with the approval of the supervisor of the location) while the person served is not home.

Person served records which are stored electronically shall be stored on a computer device using a password. Employees should not share their password with others. Electronic storage media containing protected health information shall be stored in a lockable room or cabinet.

Working files which are kept at individual person served homes may contain protected health information. The person served will determine a secure location in his/her home for storing confidential information. If requested, a locked cabinet shall be used and/or reasonable safeguards shall be put in place to protect the confidentiality and security of the information. The person served shall receive training regarding access to and confidentiality of all such information.

Employees Working Away from a Facility Setting:

- Employees working away from a facility setting should take with them only the amount of confidential/protected health information necessary to carry out their duties.

- Documentation on equipment such as laptops, papers, PDA's, and documentation kept in binders, briefcases, etc. should be kept secured from access by persons without authorization to the protected health information. Employees are expected to take reasonable measures to secure such equipment and material in all locations, including the employee's home and vehicle. Electronic devices must be password protected.

- Documentation containing protected health information should be viewed in the most private setting possible. While working with confidential information, employees should keep the information in line of sight or within arm's reach, and cover documents which are not in immediate use.

- Conversations in which confidential information is discussed should occur in the most private setting possible. Employees should make every effort to keep the volume level of conversations low enough so as not to be overheard. Whenever possible, conversations should involve only the first name or initials of the individual.

- When discussing confidential/protected information over the telephone, it is preferable to use a regular landline telephone or digital wireless telephone, as these devises cannot be easily monitored. Analog cellular and cordless telephones should be used for communicating confidential information only when necessary.

- When using the services of an interpreter for individuals with hearing or linguistic impairments, the interpreter should be certified or licensed. In the absence of verified certification or licensure, the interpreter should be informed of, and agree to, confidentiality guidelines in writing. The interpreter should not be an immediate family member or close family friend of the individual unless the individual who is the subject of confidential information consents.

- When sending or receiving confidential/protected health information via fax, employees should verify the fax telephone number to which the information is being sent, and if the fax machine is not in a secure location, the employee should take reasonable steps to ensure that the information is received only by the intended party. For example, whenever possible, the person receiving the fax should be notified that it is being sent and be available at the fax machine for immediate pick-up.

PERSON SERVED RECORDS –CONTENT, STORAGE, ACCESS

PROCEDURES - Community Living and Support Services

The designated Direct Support Manager for each program or living unit is responsible for the overall control of the case record process and the implementation of organization standards and procedures for case records of the services they supervise.

Upon admission, a person served file shall be constructed by the Division Director according to the Person Served Record contents. All forms should be completed in their entirety - if information is not available it shall be marked "information not available."

Storage and Confidentiality

In homes owned or leased by the organization, the Person Served Record shall be retained in the home in a lockable room or locked cabinet. Access to the records is limited - see also Confidentiality Procedure. The room or cabinet shall remain locked when not under the direct supervision of the employee(s) on duty. Records shall not be removed from the house except by employees in line of job duties, and only with the approval of the Manager or designee. No copies of the records shall be made by anyone without a properly executed release of information form.

In service locations not owned or leased by the organization, (such as the Community Integration Program or ISL locations) the permanent Person Served Record may be retained in the home according to the person served's preference or may be kept in the applicable program office in lockable storage. The permanent Person Served Record shall not be removed from the office, nor shall copies be made, except by employees in the line of job duties with permission of the Division Director or designee. No copies of any Person Served Record shall be made except by employees in the line of job duties.

Outdated materials may be removed from the Person Served Record and filed in designated overflow files in the home in accordance with supplemental purging procedures. Overflow filing can be done only under the direction of the Direct Support Manager to maintain the record's size and status. Overflow files shall be kept secure under lockable storage.

Upon discharge or death of a person served, the current Person Served Record shall be transferred to the appropriate program location. Records of discharged persons served shall be kept secure and stored at a storage location. The entire record shall be retained by the agency for seven years, after which time the records any be transferred to the appropriate Regional Center of the Department of Mental Health, or the referring funding source, or destroyed in accordance with these procedures. Copies of person served identification data and discharge summaries may be retained for reference. Transfer of the remaining record shall be documented in writing with an employee signature.

Person served access to records

In many circumstances, a person served may access information from his/her file upon request. However, in some instances, the person served (or legal guardian) must make a formal request for access to his or her records. The following procedures shall apply:

1. If for any reason a person served's right to review his or her own records has been limited, this must be noted on the Person Served Information Sheet in the beginning of the Case Record. Employees must review this information before permitting any access to records.

2. A person served or legal guardian must make a written request to access person served records for the following purposes: for access to inspect the records or sections thereof, or to receive copies of the person served record or sections thereof. The "Request for Person Served Access to Their Protected Health Information" form shall be provided to facilitate the request. Employees may assist with completing the request. The request form shall be forwarded to the Director within one working day. Upon receipt of the request, the Director shall follow procedures included in this manual under "Request for Person Served Access to Protected Health information".

3. When a person served (or legal guardian) requests access to simple information contained in his/her file, or when sharing information from the person served record is a normal part of service delivery, designated employees may provide access to the information. Some examples of this include: review of progress on Individual Support Plan for monthly/quarterly reviews, an inquiry by the person served regarding dates of admission, employment, or participation in outside programs or services, and inquiry by the person served regarding a health treatment or medication, and inquiry by the person served regarding financial issue contained in the person served record. A person served may receive verbal information of this type, or view corresponding records in his/her own file at the person served's request. It is important for the employee to offer explanation, interpretation and support while a person served is accessing such case file information. The Person Served Support and ISP Data entries should be noted that the person served requested and reviewed the file on that date.

PROCEDURES - Community Living programs

All employee entries in person served records shall be designated by the employee acknowledgement through the Therap documentation system. The "initial key" is utilized on medication charts and data charts.

Employees on duty shall be responsible for making daily entries into person served records in Therap to ensure prompt and ongoing communication of daily events and concerns of persons receiving services. Entries shall be objective, written in third person point of view, and shall describe events and behaviors in as specific a manner as possible.

In Group Homes and for persons served in Supported Living, the following procedures apply:

- ISP Data entries are made daily (on all shifts) or at each contact with the person served or support sources. All employees on all shifts must complete ISP Data entries. ISP Data entries should contain information regarding programs, activities, interactions, learning opportunities and supports provided.
- Data Collection Forms may be used to track progress and collect specific information about individual's skills, behaviors, and progress. Data forms may correspond directly to the Individual Support Plan, and/or track "baseline" information in specific areas. The applicable data forms must be completed the employees involved on their assigned shifts. The frequency of data should be specified on an individualized basis.
- When an employee receives a health complaint or observes health symptoms or administers any form of treatment, this should be made in the Therap documentation system under "Medical." Entries should be made periodically (at least monthly) to note the individual's health status, even if no health concerns are present. Entries should be made in the Therap documentation system under "Appointments" for each contact with physicians/health care professionals. Injuries and illnesses not otherwise meeting reportable criteria for an event report are to be documented on the ISP data under "Medical."
- Medication Administration Record Forms shall be completed in accordance with Medication Administration Procedures of this policy and procedure manual.
- Seizure Reports and Menses Reports are completed at the time of occurrence.
- Person Served Weight records are completed monthly unless greater frequency is of benefit to the person receiving services. In Programs serving People with Prader-Willi Syndrome, weight records are completed per

specific procedures in that section of this manual. In instances when it is physically impossible to conduct monthly weights, weight will be recorded if it can be obtained during physician visits.

- Forms listed above may in some cases be maintained in a "working file" and transferred to the permanent Case Record on a monthly or quarterly basis.

For Community Integration (Off-site Day Hab) and services provided on a "Unit of Service" basis, the following procedures apply:

- ISP Data entries are made at each contact with the person served or support sources. ISP Data entries should contain information regarding programs, activities, interactions, learning opportunities and/or supports provided.
- Data Collection Forms may be used to track progress and collect information about individual's skills, behaviors, and progress, along with documentation of services delivered. Data forms may correspond directly to the Individual Support Plan, and/or track "baseline" information in specific areas. The frequency of data should be specified on an individualized basis.
- When an employee receives a health complaint or observes health symptoms or administers any form of treatment, this should be made in the Therap documentation system under "Medical." Entries should be made periodically (at least monthly) to note the individual's health status, even if no health concerns are present. Entries should be made in the Therap documentation system under "Appointments" for each contact with physicians/health care professionals. Injuries and illnesses not otherwise meeting reportable criteria for an event report are to be documented on the ISP data under "Medical."
- Medication Administration Record Forms shall be completed in accordance with Medication Administration Procedures of this policy and procedure manual. This form is not required for individuals who self-administer medication.
- Seizure Reports and Menses Reports are completed at the time of occurrence.

Forms referenced above may in some cases be maintained in a "working file" and transferred to the main Case Record on a monthly or quarterly basis.

For any program location, if the Therap system is unavailable, employees should complete all required documentation using ISP Data entry sheets. Entries shall be written in blue or black permanent ink, in a legible manner. Documentation should include:

- the name, date of birth, the DMH ID of the person served
- the date and time of the shift beginning
- the date and time of the shift ending
- the first and last name of the employee completing the documentation

When Therap becomes available, the employee completing the written documentation should then transfer the data into Therap.

For all Community Living Services, under the direction of the Division Director the following information shall be reviewed and updated in the person served case record file within 30 days of the implementation of the Individual Support Plan:

- The person served information sheet, including all identifying information, names of contact persons, etc., and photograph if not current.
- Authorizations for Exchange of Information / consent forms
- Inventory of valuables
- The Person Served Information / Medical sheet

- The financial information survey, including current status of insurances and benefits.
- The training/Employment Record
- Annual assessments, which may include Risk Assessment, Medication Administration Assessment, Money Management Assessment, Stay Home Alone Assessment, Toxic Substance Evaluation, Water Temperature Evaluation, etc., as applicable for the individual person served.

At the time of the new Individual Support Plan, the Person Served Record will be updated and information from the previous year(s) will be removed from the record and stored in secure overflow files. Information regarding the release/disclosure of PHI, including Authorization forms, will be forwarded to the administrative office for retention. The Director of Community Living will designate a schedule for removal of outdated records and maintenance.

Person served records which are received from outside the agency (e.g., by mail or fax) shall be filed in the permanent record within seven days of receipt.

If "working files" are maintained, (files for training data, medication charts, etc.,) records and forms from these working files shall be placed in the permanent file within 30 days of completion or at each Individual Support Plan monthly review period. These records shall be reviewed by the Direct Support Manager on a regular basis to ensure adherence to agency standards.

PERSON SERVED RECORDS: AUTHORIZATION FOR EXCHANGE OF INFORMATION

PROCEDURE - All Programs

Information and records shall not be released or disclosed without a properly executed "Authorization for Exchange of Information" which is dated, time-limited, not to exceed one year in duration, signed by the person served and/or legal guardian, and which specifically lists the type of information to be shared. There are limited exceptions to the requirement for an Authorization for Exchange of Information:

a. The person served and his/her legal guardian;
b. Employees of the referring funding source as obligated by contract (for example, the examples of Missouri Department of Mental Health or its designated representatives);
c. Personal physicians authorized by the person served or guardian; and other medical or paramedical persons responsible for providing health care services to the person served (in most cases this will be required by the physician in order for them to share information with them);
d. An attorney authorized by the person served or guardian, or appointed by the court;
e. Law enforcement officials or public health officers, but only to the extent necessary to carry out the responsibilities of their office, and such entities shall be obligated to keep such information confidential;
f. To authorities responsible for investigating reports of abuse, neglect, or violations of person served's rights;
g. Pursuant to an order of a court or administrative agency of competent jurisdiction;
h. For purposes of treatment, payment or health care operations, insofar as such disclosures are consistent with state and federal law.

When employees encounter a party who has an earnest and legitimate interest in a person served but who does not fall under the guidelines listed a-h above, and is not covered by an authorization form (e.g. volunteer agencies,

church members, etc.) the employee may describe the services of Open Options, state that we are obligated under law to hold personal information confidential, and state that further information must come from the person served or his/her guardian.
If the person served wishes, an authorization for release of information may be completed to share information with these individuals in the future.
Authorization for Exchange of Information Forms will be filed in the person served's case record. The Division Director or his/her designee will be responsible for the proper execution of the form, including the update and/or addition of any applicable authorizations. All information on the form must be filled out completely before the individual signs the form.

When information is disclosed to outside parties who are not covered by an authorization and the information is not disclosed for the purposes of treatment, payment or operations, employees disclosing the information will enter the applicable information in the person served's case record. Such disclosures made for administrative purposes may be entered on Disclosure Tracking record in the administrative office.

Overflow files of Authorization for Exchange of Information Forms and Disclosure Tracking Forms shall be forwarded to the Division Director on an annual basis.

Verification of Identity of Requestor
When an employee receives a request for information about a person served, the following steps should be taken before confirming that the individual receives or has received services from the organization:

a. Check the person served record to determine if there is an active authorization for the exchange of information with the person or entity requesting the information.

b. If there is an authorization, but the employee is unfamiliar with the person or entity requesting, the employee should ask for some verification that the person is the appropriate person. The employee may confirm the person's identity by asking for identification, asking the person served to identify the person, etc. If the request is being made by telephone, the employee should ask to call the person back with the information and confirm the telephone number by checking the person served record.

c. If there is not an authorization to release information to the person or entity, or if the employee believes that the request is questionable in any manner, the request should be referred to the Division Director or his/her designee. Employees and members of the Board of Directors of Open Options of Greater Kansas City are considered to be members of the organization's workforce and therefore an authorization is not required for communication of protected health information. However, information used and disclosed among members of the workforce should be the minimum necessary to fulfill the purpose of the use or disclosure. Employees are expected to use reasonable and professional judgment in communications with both internal and external parties, and reasonable efforts will be made to limit access to protected health information to only the amount of PHI that is needed to carry out duties. Person served information shared with Board members should be general and without reference to names if possible. Actual review of written person served records by Board members must be authorized by the full Board.

PERSON SERVED RECORDS: MINIMUM NECESSARY STANDARD

PROCEDURE: All Programs

Protected health information means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

In accordance with federal law (45 CFR Section 164.502 et.seq.), the organization is required to use, disclose or request only the minimum amount of protected health information (PHI) necessary to accomplish the intended purpose of the use, disclosure or request. In simple terms, protected health information should be used and shared only on a "need to know" basis.

The organization and its workplace will make reasonable efforts to ensure that when information is used or disclosed, only the minimum necessary PHI is disclosed, used or requested. Employees are expected to use reasonable and professional judgment in communications with both internal and external parties, and to utilize procedures in this manual related to disclosure, and authorization for disclosure, of protected health information.

Reasonable efforts will be made to limit access to protected health information to only the amount of PHI that is needed to carry out duties. These efforts will include periodic review of information access through the mechanism of Case Record Review, under the direction of the Director of Community Living.

Exceptions to the minimum necessary standard include:

- disclosures to the individual who is the subject of the information
- disclosures made under a written authorization, which will specify the information being disclosed
- disclosures to or requests by healthcare providers for treatment purposes
- disclosures required for HIPAA compliance in billing (standardized transactions)
- disclosures made to HHS/OCR pursuant to a privacy investigation
- disclosures otherwise required by the HIPAA regulations or by other law

Any questions regarding this procedure should be directed to the Director of Community Living.

PERSON SERVED RECORDS: DESIGNATED RECORD SET

PROCEDURE - All Programs

The term "designated record set" includes any item, collection or grouping of information that includes protected health information and is maintained, collected, used or disseminated by the organization for person served care or payment decision making including:

a. Person Served Therap documentation, Case Records, Medical Records, and billing records about persons served maintained by the organization.

b. Enrollment, payment, claims, and case or medical management record systems maintained by the organization.

Information that is <u>not</u> part of the Designated Records Set is defined as follows:

- Any documents that are used for census information, quality assurance or quality improvement, peer review, intra-agency communication and correspondence (paper or electronic), abuse/neglect investigations, incident/injury reports, event reports, audits, or various electronic databases etc. which are not used to make decisions regarding an individual person served, shall not be considered as part of the designated records set.

- Working files, either paper or electronic, are not included as part of the designated records set. Working files are typically used by employees in the completion of routine duties away from the designated records set or outside of a facility-based setting. Working files may consist of copies or records that are included in the designated records set. Examples of this information may include, but not be limited to, copies of current Individual Support Plan, behavior support plans, correspondence, etc.

- Psychotherapy notes are not included in the designated records set (psychotherapy notes are defined in 45 CFR Section 164.501, and are to be kept separate from the medical record.) The organization does not routinely maintain psychotherapy notes as defined.

- The designated record set shall be created, stored, released, transported, copied, and destroyed in accordance with these policies and procedures.

PERSON SERVED RECORDS: NOTICE OF PRIVACY PRACTICES

PROCEDURE - All Programs

The Notice of Privacy Practices is a document outlining adequate notice of the uses and disclosures of protected health information that may be made by the organization, including the person served's rights and the organization's duties in accordance with HIPAA (45 CFR Section 164.520.)

At the date of first delivery of service, the person served (or their legal representative/guardian) will be presented with the Notice of Privacy Practices. First delivery of service is defined as follows:

- Community Living programs: The date of admission to the program
- Family Support Programs: The date initial contact, by telephone or in person, with an eligible person served who wishes to receive formal service from the organization.
- Targeted Case Management: The date of first billable contact whether in person or by telephone.
- SeniorLink Programs: The date of initial assessment

The Acknowledgment Signature Page of the Notice should be signed by the person served (and/or legal representative) and placed in the Person Served Record. When the first delivery of service is conducted by telephone, the Notice of Privacy Practices will be mailed to the person served within one working day of the initial service delivery, with a request that the person served sign and return the Acknowledgment Signature Page. A notation will be entered into the person served record indicating the date that the Notice was mailed to the person served.

If a person served wishes to receive the Notice of Privacy Practices by e-mail, the person served may submit an email request to the Privacy Officer. The Director will request acknowledgment by e-mail and document such in the person served record.

A copy of the current Notice of Privacy Practices will be posted at the Administrative Offices and in each group facility owned or leased by the organization.

Updates to the Notice of Privacy Practices must be developed and/or approved by the organization's Privacy Officer. When a material change is made, the organization will make the revised Notice available upon request, and the revised Notice will be posted at facilities and on the web site.

PERSON SERVED RECORDS: PRIVACY AND SECURITY TRAINING

PROCEDURE - All Programs

In accordance with HIPAA regulations, all members of the workforce must be trained on policies and procedures with respect to health information, and on vulnerabilities of protected information and ways to ensure the protection of information. The workforce includes employees, volunteers, student interns, and other persons whose performance of work is under the direct control of the organization.

Initial HIPAA training for existing employees/workforce members shall be mandatory. Employees, volunteers and students will receive training as part of their orientation. The orientation must occur within 30 days of hire.

Additional mandatory training shall occur whenever there is a material change in the organization's privacy-related policies and procedures, or as determined by the organization's privacy and/or security officers.

The organization will maintain attendance records for internal privacy and security training in the employee's personnel file for a period of seven years.

PERSON SERVED RECORDS: REQUEST FOR PERSON SERVED ACCESS TO PROTECTED HEALTH INFORMATION

PROCEDURE - All Programs

Individuals receiving services have ongoing access to information in their records and may request to see or have information explained at any time. A person served who has or is receiving services from the organization, or their legal guardian, must request in writing for access to inspect, or receive copies of Protected Health Information except in those instances covered by Federal Regulation and outlined in these Procedures and/or the Notice of Privacy Practices acknowledged at admission, and must further specify the exact information requested for access.

The "Request for Person Served Access to Their Protected Health Information" form shall be provided to facilitate the request. Employees may assist in initiating the process requesting access to Protected Health Information.

All requests by persons served (or their legal guardian) for PHI must be forwarded to the Privacy Officer or Division Director (or his/her designee) for action.

If it is acceptable after discussion with the person served, the organization may provide a summary of the PHI to the person served. If the summary is acceptable, the person served's agreement to a summary shall be documented in writing in the record as a check in the appropriate box in the "Request for Person Served Access to Their Protected Health Information" form. The person served's agreement to any costs associated with the summary shall be documented in the record as a check in the appropriate box in the "Request for Person Served Access to Their Protected Health Information" form. The form shall be filed in the person served's medical record.

The request shall be processed in the format requested i.e. paper files, computer disk, etc, if possible, and in a timely consistent manner according to established timeframes but not more than 30 days after receipt of the request.

If the record cannot be accessed within the 30 days, the timeframe may be extended once for no more than an additional 30 days with notification in writing to the individual outlining reasons for the delay and the date the request will be concluded.

Requests for Access to Protected Health Information may be denied without a right to review as follows:

a. If the information conforms to one of the following categories: psychotherapy notes; information compiled for use in a civil or administrative action or proceeding; or information that would be prohibited from use or disclosure under the Certified Laboratory Information Act (CLIA) laws and regulations;
b. If the person served is participating in research related treatment and has agreed to the denial of access to records for the duration of the study;
c. If access is otherwise precluded by law;
d. If the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
e. If the facility has been provided a copy of a court order from a court of competent jurisdiction which limits the release or use of PHI.

Requests for Access to Protected Health Information may be denied provided the individual is given a right to have the denial reviewed as follows:

a. A licensed health care professional based on an assessment of the particular circumstances, determines that the access requested it reasonably likely to endanger the life or physical safety of the person served or another person.
b. The organization may deny the person served access to PHI if the information requested makes reference to someone other than the person served and a licensed health care professional has determined that the access requested is reasonably likely to cause serious harm to that other person.
c. The organization may deny a request to receive a copy or inspect PHI by a personal representative of the person served if the facility has a reasonable belief that the person served has been or may be subjected to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the individual; and the organization (acting on professional judgment) decides that it is not in the best interest of the person served to treat that person as the person served's personal representative.

Denial of Access

Upon denial of any request for access to PHI, in whole or in part, a written letter shall be sent to the person served, or other valid representative making the request for access, stating in plain language the basis for the denial.

If the person served has a right to a review of the denial as outlined above, the letter shall contain a statement of how to make an appeal of the denial including the name, title, address, and telephone number of the person to whom an appeal should be addressed. This letter shall also address the steps to file a complaint with the Secretary of HHS.

If the information requested is not maintained by the organization, but it is known where the person served may obtain access, the organization must inform the person served where to direct the request for access.

Appeal and Review of Denial of Requests

A person served or legal guardian has the right to appeal the decision to withhold portions or all of the record for safety or confidentiality reasons.

The appeal shall be submitted in writing to the Director of Community Living who will designate a non-involved administrative employee to coordinate the appeal process. The appeal process will include review by qualified professionals to determine the appropriateness of the denial.

If the reviewer determines that the initial denial was appropriate, the person served must be notified in writing, using plain language that the review resulted in another denial of access. The notice must include the reasons for denial and must describe the process to make a complaint to the Secretary of HHS.

If the denial was not appropriate, the reviewer shall refer the request to the Director of Community Living or designee for action. If access is denied to any portion of the PHI, access must still be granted to those portions of the PHI that are not restricted. The reviewer's decision is final.

Provision of Access and Fees

Requested information must be a part of a designated record set. If the requested information is maintained in more than one designated record set or in more than one location, the organization only needs to produce the information one time in response to the request.

If the requested information is maintained electronically and the person served requests an electronic or faxed copy, the organization will accommodate the request if possible and should explain the risk to security of the information when transmitted as requested.

If the information is downloaded to an external hard source, the person served should be advised in advance of any charges for the hardware.

If the information is not available in the format requested, the organization must produce a hard copy document or other format agreed upon by the person served and organization. Any requests for accommodations shall be sent or given in writing to the Director of Community Living. The organization will make reasonable effort to provide the information in an accessible format and will notify persons served in advance of any associated fees.

The fees charged will be a reasonable amount based on standard business practices.

PERSON SERVED RECORDS: REQUEST FOR AMENDMENT TO PROTECTED HEALTH INFORMATION

PROCEDURE: All Programs

Persons served have a right to request an amendment to information about them in a designated record set, if the person served believes that the information is incomplete or incorrect. In accordance with HIPAA regulations, amendments to protected health information may be limited or restricted as defined in this procedure, the Notice of Privacy Practices, and as allowed by law.

a. A person served, or legal guardian, who believes information in their health records in incomplete or incorrect, may request an amendment or correction of the information. For minor discrepancies, i.e. typos, misspelled name, wrong person served may approach the author of the entry (or the date, etc., the supervisor of the location), point out the error, and ask the author to correct it.
1) The entry author/supervisor agrees, the entry can be corrected according to best documentation practices by drawing a single line through the error, adding a note explaining the error (such as "wrong date" or "typo"), date and initial it, and make the correction as close as possible to the original entry in the record.
2) Any information added to a Individual Support Plan in the regular course of business in not considered an amendment. An example would be when a person served provides the name of a new private physician whom he/she sees or changes of address for family members, etc.

b. All other requests for amendment to PHI shall be in writing and provide a reason to support the amendment. Specifically, any request should be supported by documentation of any incorrect information or incomplete information.

1) The "Request for Amendment to Protected Health Information" form shall be provided to facilitate the request. Employees may assist in initiating the process requesting amendment to PHI and a copy shall be provided to the person served.

2) All requests for amendment of PHI must be forwarded to the Director of Community Living or designee who will route the original request to the author of the PHI or that individual's supervisor.

3) If the author/supervisor chooses to add a comment to the request form, a second copy of the form will be given to the person served with author's comments.

4) This request shall be processed in a timely consistent manner, according to established timeframes, but not more than 60 days after receipt of the request.

5) If the request for amendment cannot be processed within the 60 days, the timeframe may be extended no more than an additional 30 days with notification in writing to the individual outlining reasons for the delay and the date the request will be concluded.

6) If a person served with a guardian requests an amendment, a letter is to be sent to the guardian stating that the person served is requesting an amendment, and further requesting that the guardian complete the Request for Amendment form.

c. If the request is granted, the organization shall:

1) Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment, and then document the change in the same section of the record as the original information.
2) Inform the person served that the amendment is accepted.
3) Obtain the authorization of the person served to notify all relevant persons or entities with whom the amendment needs to be shared.
4) Within a reasonable time frame, make reasonable efforts to provide the amendment to the persons identified by the person served, and any persons, including business associates, that the covered entity knows has been provided the PHI that is the subject of the amendment and who may have relied on or could foreseeably rely on the information to the detriment of the person served. A reasonable time frame is defined as attempts to complete this process within 60 days of the date of the amendment to the record.
5) If the amendment affects a service for which billing or a charge has already been submitted, then the billing must be reviewed to see if it should be amended or changed as well to reflect the new information.

Denial of Request for Amendment of Protected Health Information

a. The organization may deny the request for amendment to PHI if:

- the health information that is the subject of the request:
- Was not created by the organization. However, if the person served can provide reasonable proof that the person or entity that created the information is no longer available to make the amendment, and the request is not denied on other grounds, this organization must amend the information.
- Is not part of the medical information kept by or for the facility.
- Is not part of the information that the person served would be permitted to inspect and copy under HIPAA regulations.
- Is accurate and complete.

b. If the organization denies the requested amendment, it must provide the person served with a timely, written denial, written in plain language that contains:

- The basis for the denial;

- The person served's right to submit a written statement disagreeing with the denial and how the person served may file such a statement;
- The name, title, address, and telephone number of the person to whom a statement of disagreement should be addressed;
- The steps to file a complaint with the Secretary of HHS;
- A statement that if the person served does not submit a statement of disagreement, the person served may request that the organization provides the Request for Amendment and the denial with any future disclosures of PHI. (See "Statement of Disagreement of Denial" below, for further information).
- A copy must also be provided to the guardian, if applicable; to parents(s), if applicable; or to DFS if that agency has legal and physical custody of the juvenile.

Statement of Disagreement of Denial

a. Persons served shall be permitted to submit to the organization a written statement disagreeing with the denial of all or part of a requested amendment, and the basis for the disagreement. This statement of disagreement shall be limited to one page.
b. The statement of disagreement shall be submitted in writing to the Director of Community Living.
c. The Director of Community Living may prepare a written rebuttal to the statement of disagreement and must provide the person served with a copy of the rebuttal.
d. The organization must identify the record of PHI that is the subject of the disputed amendment and append or link (by cross- reference) the request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the organization rebuttal statement if any.
1) If the person served has submitted a statement of disagreement, the organization must include the documents in (d), or an accurate summary of the information, with any subsequent disclosure of the PHI to which the disagreement relates.
2) If the person served has not submitted a written statement of disagreement, the organization must include the person served's request for amendment and its denial, or an accurate summary of the information, with any subsequent disclosure of PHI only if the person served has requested it.
e. If the organization receives information from another facility of an amendment of a person served's PHI, the PHI from that sending facility must be amended in written or electronic form.

The Director of Community Living will maintain a file tracking Requests for Amendments and actions taken in conjunction with this procedure.

PERSON SERVED RECORDS: REQUEST FOR RESTRICTION ON THE USE OR DISCLOSURE OF INFORMATION

PROCEDURE - All Programs

Persons served have the right to request specific restrictions on the use or disclosure of information. In accordance with federal HIPAA regulations, (45 CFR Section 1 64.522(a)), our organization is not required to agree to requested restrictions on the use or disclosure of protected health information.

Request For Restriction On Use Of Disclosure Or Protected Health Information
a. Persons served (or legal guardian if applicable) shall indicate their request for restriction on the use or disclosure of their PHI using the "Request to Restrict Information" form.
b. The requested restrictions must be provided in writing, signed and dated by the person served or personal representative.

Agreement or Denial of Request

a. The Director of Community Living or designee, must receive the written request. The Director of Community Living, in consultation with the President / CEO, shall determine whether it will be approved.
1) If approved, the organization must implement the restriction.
2) The Director of Community Living or designee will identify the restriction on the face sheet of the person served's record.
b. The organization's agreement or refusal of the request shall be documented on the request form, signed and dated by the Director of Community Living or designee.
c. The original will be filed in the Person Served Record for permanent retention.
d. A copy of the approved or denied form will be provided to the person served.

Termination of Restriction
The organization may terminate the agreement to a restriction if:

- The person served agrees to or requests the termination in writing.
- The person served orally agrees to the termination and the oral agreement is documented.
- The facility informs the person served that it is terminating its agreement to a restriction and that such termination is only effective with respect to PHI created or received after it has so informed the individual.
- When any of the above criteria are met, the restriction will be removed, and the form will be dated and signed by the Director of Community Living.
- If the restriction was identified on the face sheet of the person served's record, that identification shall be removed by the Director of Community Living or designee.

Emergency Exception

If the organization has agreed to the restriction, but the person served who requested the restriction is in need of emergency treatment, and the restricted PHI is needed to provide the emergency treatment, the organization may disclose that PHI to a health care provider to provide such treatment.

If such PHI is disclosed in an emergency situation, the organization must require that the health care provider to whom the information was disclosed not further use or disclose that PHI.

PERSON SERVED RECORDS: REQUEST FOR ACCOUNTING OF DISCLOSURES

PROCEDURE – All Programs

All disclosures of PHI need to be accounted for upon the request of the individual. This is not limited to hard copy information but any manner of communication that discloses information, **including** information given verbally. However, the following list of exceptions to this requirement does <u>not</u> require tracking or need to be accounted for upon the request of the individual:
1. Disclosures made according to a properly executed Authorization for Exchange of Information.
2. Disclosures made for treatment, payment, and healthcare operation purposes as set out in 45 CFR § 164.502.
3. Disclosures made to the person served. (45 CFR § 1 64.502).
4. Disclosures made for facility directory purposes, if utilized (45 CFR § 164.510).
5. Disclosures made for national security / intelligence purposes. (45 CFR § 164.512 (k)(5)).
6. Disclosures made to correctional institutions or law enforcement officials. (45 CFR § 164.51 2(k)(5)).
7. Disclosure made prior to the date of compliance with the privacy standards, meaning prior to April 14, 2003.
8. There are further exceptions for disclosures to health oversight agencies (see section 1 64.52 8 (a)(2)(i) et seq.). Please contact the Director of Community Living should this situation arise.

Employees will document required disclosures (both verbal and written) made in the regular course of business in the Person Served Record. Disclosures made for administrative purposes may be tracked separately through the

Administrative Office. Overflow documents relating to disclosures, including person served authorizations, will be filed in the administrative office for a period of six years.

Process for Requests: The person served (or legal guardian) must make a written request for an accounting of disclosures to the Director of Community Living or designee. The request shall be on the Request for Accounting of Disclosures Form. Employees may assist the person served in completing the form if requested to do so.

The Director of Community Living has 60 days after receipt for such an accounting to act on that request for an accounting disclosure. If the organization has disclosed information to a business associate regarding the person served requesting the accounting, then the organization must request an accounting of disclosures of that person served's information from that business associate, who has 20 calendar days to provide the accounting. The facility may request one 30-day extension, which is allowed, but the person served must be informed in writing:

a. Of the delay:
b. The reason for the delay,
c. The date the accounting will be provided, and
d. Such notification to the person served or person requesting the accounting of disclosures of any delay must take place within the 60-day timeframe.

The following required content shall be included in the Accounting of Disclosures:
a. The name and identification number of the person served whose PHI was
Disclosed.
b. Date of Disclosure.
c. Name and address, if known, of the entity or person who received the PHI.

d. Brief description of the PHI disclosed.
e. Brief statement of purpose that reasonably informs the person served what the purpose was for the disclosure, or provide the person served with a copy of the authorization, or provide the person served with a copy of the written request for disclosure

If multiple disclosures are made to the same entity or person for the same reason, it is not necessary to document items (A-D) for each disclosure. The organization may document instead the first disclosure., the frequency or number of disclosures made during the accounting period, and the date of the last disclosure in the accounting period.

Costs: The organization must provide the first accounting of disclosures free of charge in any 12-month period. For any subsequent requests, a fee can be charged. Before charging a fee, the Director of Community Living must inform the person served and allow them the opportunity to withdraw or modify their request to avoid or reduce the fee.

The organization must retain a copy of the written accounting that is provided to the person served in the person served's medical record.