HIPAA

Release of Confidential Client or Participant Information

This policy is designed to ensure Paraquad's compliance with the guidelines set forth in the Health Insurance Portability and Accountability Act of 1996 and the Missouri Data Breach Notification Law. Reasonable safeguards must be in place to ensure that such information is disclosed only when necessary, and that only the minimum amount of information necessary to achieve the purpose is disclosed.

General Guidelines:

For purposes of compliance with HIPAA, staff shall consider protected information to be any and all information regarding participants receiving any services through Paraquad.

Protected information includes:

- Name and address
- Employer/Occupation
- Names of relatives
- DOB/SSN/DCN
- Telephone number
- Case file number
- Diagnosis/Treatment/Procedures
- Plan of care

Reasonable safeguards for protecting PHI include:

- Speaking quietly when discussing a participant with family members or co-workers in a public area;
- Avoiding the use of the participant's name in public areas;
- Posting signs to remind employees to protect participants' confidentiality;
- Isolation and/or locking of file cabinets and records rooms;
- Avoiding leaving documents containing protected information where others can see them;
- Avoiding leaving protected information on a computer monitor where others can view it;
- Provision of additional security, such as passwords, on computers containing confidential information;
- Limiting access to participant information to those who need the information to perform their job duties;
- Requiring a written consent form from the participant before releasing any documentary information or speaking with a third-party about the participant, other than family members or health care providers.

Staff may orally coordinate services if the conversation is kept private by use of a closed office or lowered voices. Information may be discussed in a group setting where it is reasonable to assume that the individual consents to the disclosure, for example, in a group peer counseling session.

Staff may discuss the participant's information over the phone with the participant, family members or a health care provider. Staff should limit information left on an answering machine to the caller's name, organization and other information necessary to confirm an appointment, or ask for a call back. A message may be left with a family member if reasonable care is used to limit the information given to only what is necessary, and in the participant's best interest.

Staff should accommodate all reasonable requests by participants regarding confidentiality, for example, sending information in a plain envelope. Participants can be asked to use a sign-in sheet if they are not required to state the purpose of the visit.

Release of information must be limited to the minimum necessary to accomplish the intended purpose. This standard does not apply to:

- Disclosures to or requests by a health care provider for treatment purposes;
- Disclosures to the individual who is the subject of the information;
- Use or disclosures made pursuant to an individual's authorization;
- Use or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules;
- Disclosures to the Dept. of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes;
- Uses or disclosures that are required by other law.

For routine disclosures, each department must develop procedures that identify the person or class of persons who need information to carry out their job duties, the types of information needed and conditions appropriate to such access. When the entire record is needed, the departmental procedures must state so explicitly and include a justification. For non-routine disclosures, the department manager should consult the Privacy Officer on a case-by-case basis for an individual determination.

Record Keeping
A record of all disclosures of health information, including copies of any releases signed by the participant, must be kept in the participant file for seven years.

Personal Representatives
Generally, a personal representative stands in the shoes of the participant and has the same right to disclosure. If the participant is an adult, a personal representative is the person who has a health care power of attorney, a general power of attorney, or guardianship. If the participant is a minor, a personal representative is a parent, guardian or other person with legal authority to make health care decisions for the child. However, the disclosure need not be made if a staff member suspects the personal representative of abuse, neglect, or endangerment of the participant.

Business Associates
A person or entity working with Paraquad to assist in carrying out functions for which a participant's health information is necessary is considered a "business associate". Staff must obtain assurance from all such business associates that they will comply with HIPAA guidelines to protect privacy of participants, *e.g.*, interpreters or personal care assistants (PCAs) hired by Paraquad for events. Paraquad's contract with a business associate must: describe permitted and required uses of protected health information by the business associate; provide that the business associate will not use or

further disclose the protected health information other than as permitted or required by contract or as required by law; and require the business associate to use appropriate safeguards to prevent use or disclosure of the protected health information other than as provided for by the contract.
When a staff member learns of a violation by the business associate of the contract, Paraquad must take reasonable steps to remedy the violation and, if such steps are unsuccessful, terminate the contract. If this is not possible, Paraquad must report the problem to the HHS Office of Civil Rights. Staff should consult the Privacy Officer immediately if this situation occurs.

Marketing

Staff cannot provide protected information to another party for "marketing" purposes without the express consent of the participant. There are exceptions to this general rule, if the product or service being marketed is for the care and benefit of the participant. Staff should consult the Privacy Officer to confirm whether a certain situation falls within this exception.

Public Health Entities

Information may be disclosed to a public health entity for purposes of preventing or controlling disease, injury or disability. A public health entity is an agency or authority of the United States government, a state, territory, political subdivision of a state or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. Examples of public health entities include the FDA, OSHA, and the Centers for Disease Control and Prevention.

General Exceptions

Staff may disclose protected information to report child abuse or neglect, to protect persons at risk of contracting or spreading a disease, and to comply with workers compensation laws. Staff should contact the Privacy Officer for an opinion on whether a given situation constitutes an exception before making any disclosures.

Notice to Participants
Staff must provide notice of uses of confidential information to participants and inform them to contact the Privacy Officer with questions about this policy and/or HIPAA privacy guidelines.

Facsimile Cover Sheets and Email
The following paragraph will be added to all facsimile cover sheets and email messages used to transmit health information of participants:

This fax/email from Paraquad is confidential, privileged, and intended only for the use of the recipient noted above. If you are not the intended recipient or the employee or agent responsible for delivering this information to the intended recipient, unauthorized disclosure, copying, distribution, or use of the contents of this transmission is strictly prohibited. If you have received this message in error, please notify the sender immediately by calling 314-289-4200.

Employee Education
All employees and new hires (including temporary employees and volunteers) are given a copy of this policy and an acknowledgment form to sign indicating that they have read and understand this

policy. Any employee or volunteer found to have knowingly and willfully violated this policy will be subject to disciplinary and/or legal action.

When in Doubt, Ask

While Paraquad is required to take reasonable steps to safeguard the health information of participants, perfection is not expected. If any staff member is unclear about whether to disclose a particular piece of information or needs clarification of this policy, the Privacy Officer should be consulted before making any disclosures of information.

Breach Notification

A data breach is any impermissible acquisition, access, use, or disclosure of unsecured protected health information. It is presumed to be a breach unless Paraquad can demonstrates there is a low probability the PHI has been compromised or an exception applies.

Staff must immediately notify the Privacy Officer upon the discovery of a data breach. Paraquad is required to inform affected individuals when a data breach involving their personal information occurs. The Privacy Officer will be responsible for issuing a notification letter to affected individuals.

Security Rules

Paraquad maintains reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic PHI.