Policy: Protected Health Information (PHI)

HOH will take reasonable steps to limit the use of, disclosure of, and requests for Protected Health Information (**PHI)** to the minimum necessary to accomplish the intended purpose.

PROCEDURE:

1. **PHI** will be kept private and secure. The Privacy Officer (usually also the Nurse Manager) will conduct regular risk assessments to ensure the privacy and security of all **PHI** collected and maintained by HOH.

2. Electronic records will be password protected. Other records will be maintained in secure files and kept in locked file cabinets and/or rooms. Access to **PHI** will be limited to personnel who have a reasonable need to use such information.

3. Use or disclosure of **PHI** will be allowed to occur without the client's prior authorization when undertaken for purposes of services related to HOH's operations. For other uses or disclosures, HOH will seek prior authorization from the client, except when such use or disclosure may be required by law, required for public health reasons, required to avert a threat of harm to the client or a third person, or when other circumstances may reasonably warrant such use or disclosure without prior authorization.

4. Each client will be given a written **Notice of Privacy Practices** (**NPP**) describing how health information may be used or disclosed by HOH. The **NPP** should also include a description of the instances in which advance authorization for use or disclosure may or may not be sought and a description of the steps that the client may exercise with respect to her own health information.

5. Written authorization will be obtained from each client for any use or disclosure of health information for which such prior authorization is warranted as described above. See form: ***Authorization for Release of Health Information***. (page 79)

6. Any outside disclosure of health information will be limited only to the minimum amount of information that is reasonably necessary to accomplish the specific purpose(s).

7. For each client, an accounting will be made of each outside disclosure of health information and those records will be kept for at least 7 years after the last disclosure. The Privacy Officer shall prepare such accounting.

8. Each client will be notified that she may inspect and copy her health information, that she may request restrictions on the use or disclosure of her health information, that she may request amendments to her health information and that she may find out what disclosures have been made to outside persons. Requests for inspection and copying shall be responded to within 30 days. Requests for restrictions on use and disclosure or requests for amendments of health information shall be responded to within 60 days. In the event of denial of any requests to restrict the usage or disclosure of health information or the denial of any requests to amend health information, the client will be given a written notice of such denial and an explanation of the reasons. The Privacy Officer shall handle all such requests.

9. Privacy and security of **PHI** shall be promoted by the following:

- Making sure no **PHI** is viewable or accessible by other clients or 3rd parties;

- Speaking quietly when discussing or talking with a client in the reception area, a waiting room, hallway or other public area;
- Posting signs to remind staff/volunteers to protect client confidentiality;
- Isolating or locking file cabinets or records rooms and limiting access to same;
- Providing additional security, such as passwords, on computers/networks maintaining **PHI** and having staff turn their computers off when away from their desks.
- Limiting whom within the entity has access to **PHI**, based on who needs access to perform their job duties. Only doctors, nurses, or others involved in services may have access to the entire medical record, as needed.
- Only authorized personnel shall have access to the online database and the database must be password protected.
- Maintaining a secure firewall and routinely reviewing information system activity in order to detect any breach in the firewall.
- If questioned about a client's record, and there is not an existing written authorization, the correct response is: "Due to confidentiality, I cannot verify the client has ever been seen or treated at HOH, nor can I tell you that the requested records are on file."

10. HOH and its Business Associates shall not offer **PHI** for sale or use it to fundraise or market. In the event HOH wants to use a client's story for promotional material, a signed release must be obtained from the client and all identifying information removed prior to publication. See Form: ***Media Consent and Release Form*** (page 83)

11. If HOH's copier is a digital copier, the security features on the copier must be used to protect **PHI**. At least monthly and before all service calls, the Privacy Officer shall securely overwrite the entire hard drive. If a copier has a hard drive, it shall be removed prior to selling and/or returning to another party.

12. When upgrading systems and software, the Privacy Officer must perform an appropriate technical evaluation to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the internet.

13. Clients will be given an opportunity on the Request for Services form to indicate how HOH may contact them, via, phone, text, email, or mail. The client has a right to request to receive confidential communications by alternative means or at alternative locations.

14. ultrasound reports sent off-site, whether electronically or physically, to a Physician to review shall have all **PHI** removed and a case ID provided in place of the client's name.

15. All HOH employees and volunteers will be trained concerning these procedures.