

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Name:**  | **Use and Disclosure of Protected Health Information (PHI)**  | **Date Revised:**  | **2/2020** |
| **Purpose:** | **Protocol How Client PHI Can Be Used and Disclosed**  | **Board Approval:** |  |

**Policy:**

Greater New Beginnings (GNB) complies with legal standards governing the use and disclosure of Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In accordance with HIPAA Privacy Rule 45 CFR § 164.530(b)(1), all staff members will be trained on the policies and procedures with respect to PHI as necessary and appropriate for the individual to carry out their functions at GNB.

**Procedure:**

1. **Training.** All Greater New Beginnings employees are required to receive HIPAA compliance training upon hire and annually thereafter. Additionally, Quality Assurance staff who will process requests for releasing PHI to outside parties and/or entities will receive additional training on such processes. All trainings will be documented and stored in the staff member’s personnel file. The Executive Director/Administrator, or their designee, shall have monthly oversight of all employee’s compliance with training requirements. If a staff member is found to be out of compliance, their supervisor will be notified and an immediate plan will be made to get the staff’s training up to date.
2. **Use and Disclosure of Protected Health Information:** GNB staff are expected to adhere to the following procedures in using electronic and inter-office communication:
	1. When addressing an email, staff are to always double check the “To” section as reassurance that the email is going to the appropriate person.
	2. Refrain from using any identifying information of the subject matter in the subject line of email communication. Use of initials is permitted.
	3. Staff are to use BCC’s and CC’s appropriately when sending out email communication.
	4. When responding to a group email, staff need to be mindful of whether they are responding to “all” or to the individual who initiated the email.
	5. Information, when electronically transmitted via the internal GNB secure network email, is confidentially protected through electronic safeguards managed by the organization. Additionally, the practice of using a Confidentiality Notice below the signature line for all emailed material is required by all GNB staff, as demonstrated below:
		1. Confidentiality Notice:  This e-mail is a secured data transmission for Protected Health Information (PHI) as defined by the Healthcare Information Portability and Accountability Act (HIPAA), and it is the responsibility of all parties involved to take all reasonable actions to protect this message from non-authorized disclosure. If you are not the intended recipient, you are hereby notified that any unauthorized review, use, disclosure, copying, distribution or reliance upon the contents of this e-mail is strictly prohibited. If you have received this message in error, please reply to the sender and destroy all copies of the original message. Disclosure of the information contained herein could subject the discloser to civil or criminal penalties under state and federal privacy laws.
	6. Information, when electronically transmitted to an email address outside of GNB’s secure email network, will be protected via an encrypted and password protected attachment. No confidential client information will be contained in the subject line or body of any email going to outside parties.
	7. Information, when electronically transmitted via fax, is protected by the practice of using a cover sheet for all faxed material that contains who the fax is for and a statement of confidentiality mentioned above.
	8. Staff are not to leave confidential documents unattended on printers or faxes nor should confidential documents be left out in the open, especially face-up.
	9. All inter-office mail that contains confidential documents are placed in “confidential” marked envelopes and placed in the appropriate staff member’s mail folder in the locked mail file within the central office.
	10. Confidential documents that are unneeded are securely shredded immediately
	11. When working on a computer, the monitor should be placed in a manner where passersby cannot readily view information and shall be locked by the staff member before leaving the work station unattended.
	12. When staff members are discussing a client, conversations need to be conducted behind closed doors in private.
	13. Greater New Beginnings protects the confidentiality of information about clients and assumes a protective role regarding the disclosure of confidential information. During the performance of duties, GNB employees necessarily become aware of personal or confidential information about clients. This information shall be held in strict confidence and shall not be discussed with anyone, including co-workers, family members and/or friends except on a professional, need-to-know and authorized basis. Additionally, employees may not publish or post personal or confidential information, including photos, recordings or videos, about clients in any social media format. Photos, recordings or videos of clients may be published in sanctioned GNB publications, such as brochures, newsletters, etc. only if prior informed, written permission is granted by either the client and/or client’s authorized representative and/or client’s parent/guardian.
	14. Furthermore, GNB employees may not divulge personal information concerning a client to the newspaper, television or radio media by telephone, in writing or in person. All such inquiries will be directed to the Executive Director. The QA Compliance Manager or Head of Service, or in his/her absence, the Facility Manager shall receive and sign for any subpoena or request for court records that is served to Greater New Beginnings.
	15. When a question arises regarding the possible conflict between confidentiality and reporting or court testimony obligations, GNB employees should consult with their supervisor. Breach of confidentiality shall result in immediate disciplinary action, up to and including discharge. Confidentiality is of the utmost importance within the agency.
	16. Greater New Beginnings staff will inform clients when it may be legally or ethically permitted or required to release such information without their consent, under the following conditions:
		1. When permitted or required by law, regulation or court order, confidential information may be released without the authorization of the client and/or client’s parent/legal guardian and/or authorized representative. In this case, the client will still be informed that the information will be shared and GNB will maintain documentation in the client’s file.
		2. *Mandatory reporting -* All GNB staff are considered mandatory reporters and, therefore, must report any and all reasonable suspicions of child abuse to the proper authorities. The Child Abuse and Neglect Reporting Act (CANRA) can be found in Penal Code 11164 to 11174.3. In terms of confidentiality, mandated reporters are protected by CANRA, which states that the name of the mandated reporter is strictly confidential, although it is provided to investigative parties working on the case. Under state law, mandated reporters cannot be held liable in civil or criminal court when reporting as required; however, under federal law mandated reporters only have immunity for reports made in good faith.
		3. *Duty to warn -* Mental health professionals, including social workers, are required to breach confidentiality if the client poses an imminent threat to either himself/herself, the professional, or an identifiable third party. If, during the course of therapy, a clinician assesses a client as a danger to someone, he or she has a duty and is legally compelled to warn the intended victim. It also protects clinicians from prosecution from breach of confidentiality if they have reasonable suspicion that the client might be a danger to himself or others. warn the intended victim or others likely to apprise the victim of the danger, to notify the police, or to take whatever steps are reasonably necessary under the circumstances.
			1. There are several factors to consider in determining the degree of danger a person may pose to himself/herself, a third party and/or the community. These include:
				1. Person’s history of violence and/or threats of violence
				2. Assessing person’s current desire/ideation, plans, means, access to means and intent
				3. Considering risk factors in current situation, such as intoxication or substance abuse, current or history of high anxiety episodes, a recent change in status (break-up or divorce, death of a loved one, loss of job, expulsion from school, etc.), no current support structure, paranoia, victim of abuse at home or school, etc.
3. **Authorization and Revocation to Use and Disclose Protected Health Information**
	1. Authorization – Upon intake and as necessary throughout the client’s course of treatment, specific individuals or parties may be identified as important support persons in the client’s life. In order to facilitate the most comprehensive treatment, the clinician may deem it necessary to conduct interviews, include in treatment sessions, or to collaborate ongoing treatment planning with the identified support person, party, or external organization. Prior to requesting or exchanging any information with this outside person or party, a valid and complete Use and Disclosure of Protected Health Information Authorization form will be completed.
	2. Revocation – The client has the right to revoke that permission for use and disclosure, in writing, at any time. If permission is revoked, Greater New Beginnings will no longer use or disclose health information about the client for the reasons covered by the written authorization. As outlined in the agency’s Notice of Privacy Practices, GNB is unable to take back any disclosures already made with the client’s, or their authorized representative’s, permission.
4. **Releasing Client Records**
	1. Releases of protected health information will be processed by trained staff in the Quality Assurance department. Once a request for information is obtained, the requestor will be asked to submit the request in writing with a valid Authorization to Use or Disclose Protected Health Information, clearly indicating the records or type of information being requested.
	2. GNB upholds a duty to protect the confidentiality and integrity of confidential medical information as required by law and professional ethics, thereby operating under the minimum necessary rule. Accordingly, the request will be carefully reviewed by the trained Quality Assurance staff for validity and it will be determined what records or type of information should be released, if any, based on the purpose of the request. As appropriate, only select information or a summary of treatment will be released, rather than the entirety of a document.
	3. Once the identified information is prepared to be disclosed, the administrative staff will release the records in one of the following approved methods:
		1. Encrypted and password protected email
		2. Fax
		3. Certified mail, requiring a signature for delivery
		4. In person pick-up
	4. After the records are released, the Quality Assurance staff will record the disclosure in the PHI Disclosure Log according to Greater New Beginnings’ Tracking and Accounting of Disclosures Policy.