**Creation Date:** June 2014

**Effective Date**: June 2014

**Last Review Date:** April 2015

L**ast Revised Date:** May 2015

**Next Review Date**: December 2015

**Reviewed by**: **Confidential Administrative Records**

1. **POLICY:**

1. Proactive Home Care also ensures the maintenance and transfer of both written and spoken information. Proactive Home Care Services, Inc. will ensure compliance with the Health Information Privacy and Security provisions of Public Law 104-19, commonly known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other federal and state laws related to the privacy and security of health information.
2. Proactive Home Care Services, Inc. is committed to preserving and protecting the privacy of all health information to the highest degree. Proactive Home Care Services, Inc. has adopted the HIPAA Privacy Rule and Security Compliance Rule of Georgia to ensure that it is in compliance with the requirements of the privacy and security provisions of HIPAA.
3. **PROCEDURES:**
4. Personal Individual Information:
5. Proactive Home Care will maintain files/records on each individual/staff in Proactive Home Care’s central office;
6. Files are confidential and not accessible to unauthorized users (anyone not having granted access to individual’s personal information or one that is not an employee of the managerial office staff of Proactive Home Care);
7. Files will remain locked and secured at all times with access only to authorized personnel of Proactive Home Care;
8. When disclosure is allowed, the original individual file will be examined only under supervision of Proactive Home Care staff;
9. The individual file will not be removed from Proactive Home Care premises unless authorized by the Director
10. The individual’s file will not be a public record.
11. All Service Related Information:
12. There are several federal laws and regulations relating to privacy that affect healthcare organizations in addition to the HIPPA privacy standards. Proactive Home Care will comply with federal laws addressing privacy issues. State laws, however, will be pre-empted unless they are more stringent than HIPPA, or if they fit within an exception.
13. Special Categories:
14. Deceased Individuals - Proactive Home Care will Use and Disclose Protected Health Information (PHI) of a deceased individual in the same manner as any other individual.
15. Personal Representatives - Proactive Home Care will treat an individual’s Personal Representative as the Individual for purposes of this Health Information Privacy and Security Compliance Rules. Proactive Home Care may, however, elect not to treat a person as the Personal Representative of an individual if:
16. Proactive Home Care has a reasonable belief that:
17. The individual has been, or may be, subjected to domestic violence, abuse, or neglect by such person; or
18. Treating such person as the Personal Representative could endanger the individual.
19. Proactive Home Care, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the Individual’s Personal Representative.
20. Adults:

If under Georgia law a person has authority to act on behalf of an individual who is an adult in making decisions related to health care, Proactive Home Care will treat such person as a Personal Representative with respect to Protected Health Information (PHI) relevant to such Personal Representation.

If under Georgia law an executor, administrator, or other person has authority to act on behalf of a deceased individual, or on behalf of a individual’s estate, Proactive Home Care will treat such person as a Personal Representative with respect to Protected Health Information (PHI).

1. Training will be provided to all Proactive Home Care staff
2. Posting of the Notice of Privacy Practices in a prominent place
3. Maintenance of the individual’s/representatives signed acknowledgement of receipt of the notice of Privacy Practices in the individual’s file.
4. Provisions of the rights of individuals regarding their Protected Health Information (PHI) as defined in federal and state laws and in HIPAA, including but not limited to:
5. **PHI Release:**
6. Access by individuals to Protected Health Information:

a. Right of access - Each individual served by Proactive Home Care has the right to access and obtain a copy of their Protected Health Information (PHI).

1. Conditions on providing Confidential Communications:
2. Proactive Home Care will require the individual to make a request for a confidential communication described in writing.
3. Proactive Home Care will condition the provision of a reasonable accommodation on:
4. Information as to how payment, if any, will be handled; and
5. Specification of an alternative address or other method of contact
6. Proactive Home Care will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
7. Proactive Home Care’s Protected Health Information policy will require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
8. Right to request restriction of access by others – Proactive Home Care agrees to restriction if the individual who requested the restriction is in need of emergency medical treatment and the restricted Protected Health Information is needed to provide the emergency treatment. Proactive Home Care will use the restricted Protected Health Information or disclose such information to provide treatment to individual.
9. Corrective Actions for sanctions of employee(s) as necessary, mitigation of harm to any individual and preventing risks to Protected Health Information (PHI).

F. A record of all disclosures of Protected Health Information (PHI) will be kept in the file record of each individual served by Proactive Home Care Services so that Proactive can provide an accounting of disclosures to the individual for six (6) years from the current date. The record will include:

a. Date of disclosure;

b. Name of person or agency who received the Protected Health Information (PHI);

c. A brief description of the Protected Health Information (PHI) disclosed;

d. A copy of written request disclosure; and

e. Written authorization from the individual, parent, or legal guardian to disclose Protected Health Information (PHI).

G. Authorization of release of information will be obtained when Protected Health Information (PHI) of individual information is to be released or shared between organizations or with others outside Proactive Home Care. All applicable Proactive Home Care’s policies and procedures and HIPAA Privacy Rules related to disclosure and authorization of Protected Health Information are followed.

Information contained in each release will include: See attachment A

a. Specific information to be released or obtained;

b. The purpose of the authorization for release of information;

c. To whom the information is being released;

d. The time period that the release of authorization remains in effect (generally not to exceed a year); and

e. Proactive Home Care will receive a statement that authorization may be revoked at any time by the individual in advance of the exchange of information.

Exceptions to use of a release of information:

a. Disclosure may be made if required or permitted by law;

b. Disclosure is authorized as a valid exception to the law;

c. A valid court or subpoena is required for mental health or developmental disabilities records;

d. A valid court order and subpoena is required for alcohol or drug abuse records;

e. In the case of an emergency treatment situation as determined by the individual’s physician, the chief clinical officer can release Protected Health Information to the treating physician or psychologist.

1. References Uses and Disclosures:

Proactive Home Care Services, Inc. will not use or disclose Protected Health Information (PHI), except permitted or required by law.

1. Proactive Home Care Services, Inc. will disclose Protected Health Information

 (PHI):

a. In accordance with Proactive’s “Authorization of Disclosure of Protected Health Information

1. Proactive Home Care Services, Inc. will use or disclose Protected Health Information (PHI) as permitted by law and consistent with HIPAA Privacy Rule and Security Compliance Rule of Georgia and DBHDD:
2. Notice of Privacy Practices – A notice of the uses and disclosures of Protected Health Information (PHI) that may be made by Proactive Home Care, and of the individual’s rights and Proactive Home Care’s duties regarding the individual’s Protected Health Information.
3. Authorization for Disclosure of Protected Health Information – A written authorization from an individual before using or disclosing Protected Health Information (PHI) for any purpose not otherwise permitted by law.
4. Release of Information – The release, transfer, or provision of access to an individual’s information outside the entity holding the information.
5. **Discharge Summary:**

A. When Proactive Home Care anticipates a discharge, the individual will have a discharge summary that includes:

a. A recapitulation of the individual’s stay;

b. A final summary of the individual’s status to include the discharge that is available for release to authorized persons and agencies, with the consent of the individual or legal representative; and

B. The Discharge plan of care will include:

1. Evaluate the extent to which individuals have received, the services and supports defined during transition planning;
2. Identify any additional service(s) or support (s) needed during the transitional period and collaborate with the receiving provider(s) to continue the existing services or new services and supports available.
3. Act to reduce undesirable outcomes after transfer from Proactive Home Care including undesirable behavior
4. **Security of Health Information**
5. Proactive Home Care Services, Inc. will protect PHI from unauthorized access, modification, disclosure, and destruction. Proactive will maintain backups of all data stored on the computer system on a flash drive and/or portable hard drive. Use Policy listed below.
	* 1. Passwords Policy
6. All office personnel that have access to the organizations computer systems will adhere to the password procedure below in order to protect security of the network, protect integrity, and protect the computer systems.
	1. Proactive Home Care’s resources on the network by requiring strong passwords along with protection of these passwords and establishing a minimum time between changes to passwords.
	2. Administration:
7. Administrator passwords will be protected very carefully. Administrator accounts will have the minimum access to perform their function. Administrator accounts will not be shared unless given authorization.
	1. Other office personnel who have any form of computer account requiring a password on Proactive’s network; including but not limited to a domain e-mail account.
8. Password Protection
9. Never write down passwords.
10. Never send personal password through email.
11. Never reveal password over the telephone.
12. Don’t use common words or reverse spelling of words as part of your password.
13. Don’t use names of people or places as part of your password.
14. Don’t use part of your login name in your password.
15. Be careful about letting someone see you type your password.
16. Password Requirements
17. Minimum length of 8 characters recommended
18. Maximum length of 14 characters
19. Passwords should use three or four of the following four types of characters: lowercase, uppercase, numbers, and special characters such as!@#$ %^&\*(){}[].
20. Reset account lockout after four failed attempts.
21. Enforcement
22. Since password security is critical to the security of Proactive Home Care Services, Inc. Personnel that do not adhere to this policy may be subject to disciplinary action and/ or termination of employment.
23. **Time Frame for Documentation:**
24. Critical Incident Report
25. All Incident Reports have to be turned in within 24 hours of the incident
26. Once the Incident Report has been reviewed by the director, the incident report will be emailed to the regional office.
27. A copy of the Incident Report will be placed into the individual/staff file
28. Documentation
29. Staff will turn in the individual monthly documentation the 15th of each following month (for example June documentation will be turned in on July 15th)
30. If the 15th is on a weekend or holiday, the documentation will then be turned in on the next business day.
31. Medical Records
32. Staff will turn all medical documentation in to the office on the same day the medical report was completed on.
33. If for any reason staff cannot make it to the office, the medical documentation will be turned in on the next business day.