PROBERCO PRIVACY POLICY

Personnel Policy	**Location: Employee Handbook**
Effective Date: 04/14/03	**Revised: 02/19/08, 12/07/22**

It is the policy of the Corporation to maintain and protect the privacy of the Protected Health Information (PHI) of program participants and to give program participants specific rights with respect to their PHI. Under HIPAA, PHI is considered any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity. This is interpreted rather broadly and includes any part of a program participant's medical record or payment history.

This Privacy Policy shall be overseen by the Privacy Official, who shall report on privacy issues to the Executive Director. The Privacy Official shall have authority and responsibility for implementation and operation of the policy.

Procedures:

Identifiers that make health information PHI:

- Names
- Dates, except year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e., retinal scan, fingerprints)
- Any unique identifying number or code

One or more of these identifiers turns health information into PHI, and PHI HIPAA Privacy Rule restrictions will then apply which limit uses and disclosures of the information.

Collection and Receipt of Protected Health Information

1. When collecting or discussing PHI, employees will comply with the following privacy guidelines, along with any additional procedures established from time to time:

   - PHI should not be discussed in any open area.
   - Documents containing PHI should be kept in locked files and should not be left in any open area or area where the general public has access.
   - Documents containing PHI should be de-identified wherever possible.
   - Documents containing PHI should be shredded when they are no longer needed.

2. PHI will be discussed and shared with an employee only to the extent that the employee has a need to know the PHI as part of the performance of his or her job duties.

Access to Protected Health Information by Program Participants

1. Program participants have the right to supervised access to their own PHI that has been collected and is maintained by the Corporation.

2. A management employee will provide the file in the format requested by the program participant, unless it is not readily producible in that format.

3. Employees may provide the program participant with a summary of the PHI or an explanation of the PHI, if the program participant requests such a summary or explanation.

Amendment of Protected Health Information

1. The Corporation will allow program participants to request amendment of their PHI that is documented and/or maintained by the Corporation which they believe to be incorrect or incomplete. PHI that was not created by the Corporation or that is accurate and complete, as determined by the Privacy Official, is not subject to amendment.

2. A request for amendment of PHI must be made in writing to the Privacy Official. The request must be made by the program participant or the program participant's personal representative, including a parent (for a minor) or guardian. The request must reference the information for which amendment is requested and the reason for the requested amendment.

3. Within 60 days after receipt of the request for amendment, the Privacy Official will either accept or deny the amendment request. The Privacy Official will make this determination.

4. If the amendment request is accepted, the Privacy Official will notify the program participant/representative and make a reasonable effort to notify business associates or other persons who have received the incorrect PHI about the program participant from the Corporation.

5. If the amendment request is denied, the Privacy Official will notify the program participant/ representative of the basis for the denial. The program participant/ representative has the

right to submit a written statement of disagreement or to request that the amendment and the denial be included in any future disclosures.

Uses and Disclosures of Protected Health Information

1. The Corporation will use and disclose the PHI they create, collect, and/or maintain for *"valid recipients"* responsible for the following: *provision of services; training; quality assessment; health management or wellness program development or implementation; licensing; development or improvement of payment methods; referral for services; to obtain emergency medical treatment; incident reporting; or as required by law.*

2. In addition, all PHI collected by the Corporation will be disclosed to the following *"valid recipients"* or in the following situations: (1) to the program participant; (2) the program participant's parent or legal guardian; (3) to an insurance company or a business associate of the Corporation; (4) to the program participant's representative, agent, or any other person with a signed authorization from the program participant; (5) in response to legal process; or (6) to help settle a claim dispute for benefits under a medical benefit plan or insurance policy.

3. PHI will be disclosed to a *valid recipient* as described above through the telephone, only after the identity and authority of the person who is on the other end of the call is verified.

4. PHI will be sent to a *valid recipient* by facsimile or email only if the employee who is sending the information can determine that the intended recipient will be the receiver. All fax cover sheets and email utilized by employees will contain a standard confidentiality statement. To the extent reasonably possible, PHI that is requested or disclosed by the Corporation will be received or distributed after it has been de-identified. The Privacy Official will oversee the de-identification process. Where it is not possible or practical to de-identify PHI that is disclosed, employees will disclose only the minimum necessary information. The Privacy Official will help, upon request, to determine that the minimum necessary information is disclosed.

5. In any situation where PHI is requested from the Corporation, an employee will verify the identity of the person requesting the information and the authority of the person to have access to PHI (unless the identity and authority is already known).

6. All disclosures of PHI, other than those conducted during payment, treatment, or healthcare operations of the Corporation, will be reported to the Privacy Official. When requested by a program participant, the Privacy Official will prepare an accounting of all disclosures that were not part of the payment, treatment, or healthcare operations of the Corporation or not made at the request of the program participant. The accounting will include all disclosures made by the Corporation that occurred in the past six (6) years (or shorter period as requested by the program participant), but excluding any disclosures made prior to April 14, 2003, and will comply with all applicable laws and regulations. The accounting will be provided within 60 days of the request. No charge will be imposed for the first accounting requested during any 12-month period.

Notice of Privacy Practices

1. ProBerco will also post a copy of the Notice of Privacy Practices prominently on its Web site and at all facilities operated by the Corporation.

2. Every three (3) years from the date of the initial delivery of the Notice (4/14/03), the Privacy Official will be responsible for notifying program participants that the Notice is available and that they can receive a copy of it on request.

3. The Notice of Privacy Practices may change at any time, consistent with prevailing federal and state laws. New notices will be posted, when changed, and will be made available, upon request.

Training

1. The Privacy Official or his or her designee will conduct training for all employees who have or may have access to or may be recipients of PHI. New employees will be required to receive training on the Privacy Policy within three (3) months of the start of their employment, or within three (3) months of the assignment to a position in which they deal with PHI as part of their job requirements.
2. The Privacy Official or his or her designee will conduct training on any material changes made to the Privacy Policy within one (1) month after the changes become effective.

3. Additional training sessions may be conducted by the Privacy Official or his or her designee as needed.

4. Each employee will be required to sign a Confidentiality Statement at the beginning of his or her employment.

Complaints

1. The Privacy Official will review all written complaints, will discuss them with the Executive Director, and/or other employees, as needed, will review relevant documents, and will respond to the program participant who has filed the complaint.

   All complaints will be logged by the Privacy Official. The log will include the complaint and a brief description of the resolution of the complaint.

Recordkeeping

1. The Corporation will retain all documentation related to this Privacy Policy for a minimum of six (6) years from the date the documentation was created or the date that it was last in effect, whichever is later.

2. The following documents will be maintained in the files of the Privacy Official or other secured location:

   - This Privacy Policy
   - Notice of Privacy Practices (all versions)

- All signed authorizations
- PHI Disclosure Log
- Access, Amendment, and Restriction Request Log
- Requests to access, amend, or restrict disclosures of PHI
- Complaint Log, along with copies of any written complaints
- Records of any sanctions imposed on employees
- Employee training manuals and procedures
- Business associate contracts

Annually, the Privacy Official will determine which records, if any, have been held for the minimum period required and should be destroyed.

PHI and Working from Home

1. All hard copy PHI must be maintained in a lockable file cabinet/safe for employees who store hard copy (paper) PHI in their home offices.

2. All employees must ensure that they disconnect from the corporate network when their work is complete.

3. Employees are prohibited from allowing friends and family from using devices that contain PHI.

4. Once hard copy PHI is no longer needed, information must be maintained in a locked area until the employee returns to the office. When returning to the office, PHI should be placed in one of the two United Document locked storage consoles at William Lane (Central Copy Area or Adult Training Office) OR the storage console at the Kutztown Road office.

Sanctions

Employees who fail to comply with this Privacy Policy will be subject to disciplinary action in accordance with the Corrective Disciplinary Action Policy.

Mitigation of Wrongful Disclosures

The Corporation will attempt to mitigate any disclosures of PHI that are in violation of this Privacy Policy by, for example, requesting return of any written PHI improperly disclosed, or by admonishing the recipients of any wrongly disclosed PHI of their obligation not to further disclose the PHI.

Refraining from Intimidating or Retaliatory Acts

Intimidation, threats, coercion, discrimination, or other retaliatory acts against any program participant for exercising his or her rights under this Privacy Policy, for filing a complaint with the DHHS, or for assisting in an investigation of any act made unlawful by the Health Insurance Portability and Accountability Act is forbidden.