EMPLOYEE CONFIDENTIALITY AGREEMENT

MEMBERS' RIGHTS

Individuals receiving healthcare services through Peoples Health Network (PHN) have entrusted the staff and have been given the assurance that all information about them is held in strict confidence in accordance with legal requirements. Any information about a member's condition, care, or treatment must not be discussed with anyone, either at or away from the PHN office, except with those who are in "need to know" situations, or as permitted by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Carelessness or thoughtlessness leading to the release of this information is not only unethical and possibly illegal, but could be referred to the Human Resources Department or CEO for immediate disciplinary action.

Any breach of a member's right to confidentiality of legally protected health information by an employee of PHN subjects that employee to disciplinary action, up to and including possible immediate termination. For purposes of this agreement, the word "employee" includes not just employees of PHN, but also any temporary workers, including staffing agency personnel, interns, volunteers, and contract labor workers who may be working in any PHN department.

MEMBERS' PROTECTED HEALTH INFORMATION (PHI)

The Health Insurance Portability and Accountability Act of 1996 established the Privacy Rule which protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information" or "PHI."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

This identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers such as:

- Names
- Addresses
- Dates, such as birth dates, or dates of service
- Telephone, fax numbers, and email addresses
- Any number that can be used to track a member
- Medical device numbers used by the member
- Pictures of the member

- Any other information that can be used to identify the member

All computer system PHI must be secured by:

- Setting screen saver passwords. The duration time should be set to ten minutes.
- Minimizing open documents that contain PHI on your computer screen when not in use.
- Locking computer screens when stepping away from desks.
- Electronic PHI removed from an office facility needs to be reasonably secured. Reasonably securing electronic PHI includes, but is not limited to, encrypting all electronic files or preventing access to such files with a password locking mechanism.

All printed documents with PHI must be secured by:

- Printing out only the documents containing PHI that are absolutely necessary to perform your job.
- Putting away all documents containing PHI at the end of the day. Such documents need to be secured inside a closed drawer or file cabinet. A locking drawer or cabinet is preferred if available.
- Never leaving documents containing PHI in unattended offices or conference rooms.
- Placing all documents containing PHI that are no longer needed in a designated, secure company shred bin by the close of each business day.
- Placing all printed documents containing PHI that are to be sent to other departments in an Inter-Department Delivery envelope and properly identifying the receiving and sending parties on the envelope.
- Carrying all documents containing PHI in a closed briefcase, folder, or audit bag if such documents are removed from the office. Any documents containing PHI that are removed from the office must be kept secured at all times and be returned to the office for proper disposal.
- In the event documents containing PHI are lost, misplaced, or compromised in any way, please notify management immediately.

COMPUTER PASSWORDS and ACCESS

Passwords

- All passwords must be kept confidential.
- Do not share your passwords with other users. These passwords should be treated the same way you would treat your PIN number for your ATM card.
- If you have given out your password, or suspect that someone might know it, please contact the IT Help Desk.
- Passwords should not be left on a sticky note attached to your monitor or anywhere else on your desk. If you must write your password down, please put it in a secure location.
- Passwords must meet complexity requirements:
    - Minimum of 8 characters
    - Consist of at least 3 of the following 4 character sets:
        - Lower case alpha characters (e.g. a, b, c, d)
        - Upper case alpha characters (e.g. A, B, C, D)
        - Numbers (e.g. 1, 2, 3, 4)
        - Special or punctuation characters (e.g. !, @, #, ?, %)
- Passwords must be changed every 90 days (3 Months).

Access

- When using computer remote access, minimize windows on your computer screen to prevent others from viewing PHI.
- Computer access is limited by your actual job duties. Should your duties change, your access may be changed accordingly.
- Computer access is terminated immediately upon an employee's resignation or termination.
- Remember, if someone accesses PHN information systems using your password, you, not the person who is masquerading as you, are responsible for all that is done.
- Remember, your computer should be powered off or restarted at the end of your work shift to ensure that updates and security patches are installed and implemented.

EMAILS and FAXES

All PHN correspondence transmitted by email or facsimile must contain the appropriate confidentiality statement. In the event that an email contains PHI, the word "Confidential" must be typed in the email subject line to ensure encryption.

CONFIDENTIAL AND PROPRIETARY BUSINESS INFORMATION

PHN maintains a policy that all confidential and/or proprietary business information, including but not limited to strategic plans, marketing plans, financial prospects and results of operations, and other similar information that we use to compete in the marketplace, is confidential and may not be shared or discussed with anyone other than those employees and business associates who have a "need to know" and/or with whom PHN has an approved confidentiality and nondisclosure agreement. Violation of this policy may lead to disciplinary action, up to and including immediate termination.