n00220

Privacy & Confidentiality of Member/Participant Information and Records

Values

Accountability ● Integrity ● Service Excellence ● Innovation ● Collaboration

Abstract Purpose:

State and federal law requires Network Health and its subsidiaries and controlled affiliates (hereafter, Network Health) to ensure that anyone who handles Protected Health Information (PHI) maintains its confidentiality. PHI includes medical records, claims, benefits and other administrative data that are personally identifiable. Use of aggregated data in which an individual's personal information is not identifiable to a statistically significant degree is not subject to privacy restrictions.

Policy Detail:

State and federal law requires a Managed Care Organization (MCO) to ensure that anyone who handles oral, written and/or electronic PHI maintains its confidentiality. PHI includes medical records, claims, benefits and other administrative data that are personally identifiable.

Maintaining confidentiality encompasses how PHI is collected, maintained and used. This accountability extends to the entities with which information is shared. Compliance with the policies is demonstrated through audits, employees, employer groups/plan sponsors, agents, broker and consultant confidentiality agreements, Business Associate Agreements/addendums and external reviews. The "minimum necessary standard" applies when PHI is collected, maintained and used.

Procedure Detail:

I. Members/Participants have certain rights to their PHI
   A. Member/Participant Consents
      1. A member/participant has the opportunity to determine the appropriate uses of his or her PHI. The member/participant must authorize, in writing, the release or refusal to release any and all information unless required or exempt by law.
      2. Consents must describe the PHI to be used or disclosed, state the name of whom is authorized to make the use or disclosure (in our case Network Health), identify the person(s) to whom the use or disclosure may be made, a description of the purpose of the use or disclosure, an expiration date or event and it must be signed and dated.
   B. Routine Consent:

1. The member/participant application signed by the employee at the time of enrollment covers future, known or routine needs for uses of PHI. It does not provide for release of information beyond the uses specified on the application.
    a. Examples: Uses specified on an enrollment form may include utilization review, coordination of benefits or reimbursement with other health or insurance programs.

C. Special Consents:
1. Network Health affords its members/participants the right to consent specifically to requests for PHI in the following instances, unless otherwise authorized by state and federal law:
    a. Treatment pertaining to mental illness, developmental disability, alcoholism, drug abuse or HIV infections
    b. Treatment received from non-contracted practitioners/providers
    c. Workers compensation or auto insurance claims

D. Authorized Consents:
1. For cases in which Network Health is required to obtain informed consent for treatment or special consent for the release of and access to PHI from members/participants who lack the ability to give consent, the following persons can be authorized by the member/participant;
    a. Guardian or legal custodian of a minor member/participant.
    b. Guardian of a member/participant adjudged incompetent.
    c. Personal Representative of a member/participant (as defined below).

E. If there is no Executor of Estate and no spouse survives a deceased member/participant, an adult member of the deceased member's/participant's immediate family may qualify. A court appointed temporary guardian of PHI may also qualify to sign consent for the release of information. In cases involving court decrees or appointments, Network Health must utilize court documents to determine the validity of the consent.

II. Access to health plan information and PHI

A. The following entities may request access to member/participant PHI at Network Health: members/participants, employees, employer groups/plan sponsors, agents, brokers, practitioners, providers, third parties such as vendors or consultants, non-contracted practitioners and/or providers, oversight organizations and researchers.
1. Member/Participant: The member/participant has the right to contact Network Health to obtain access to his or her PHI for review, comment and/or correction of any errors. Members/participants should also be directed to the originating source of the health information to correct errors.
2. Employees: The member's/participant's privacy is protected internally within Network Health's administrative functions by:
    a. Identifying employees who have access to oral, written and/or electronic PHI;
    b. Restricting automated system access to only those employees whose job description requires access;
    c. Requiring all new employees, during orientation, and all existing employees annually to read and understand the confidentiality polices, as well as provisions for corrective actions if employees inappropriately use or disclose oral, written, and/or electronic PHI. Employees must not share and/or receive member or

participant PHI using personal applications or services, including text messaging, personal email systems, personal cloud storage solutions (such as Dropbox, Google Drive, OneDrive). Employees may only share and/or receive PHI that is related to their job responsibilities and must use only Network Health approved devices or systems. Any employee who uses non-approved devices to share and/or receive member or participant PHI may be subject to discipline, up to and including termination.

d. Examples of inappropriate use or disclosure include, but are not limited to:
    i. Employees discussing member/participant information in public areas such as copy rooms, hallways, break rooms, elevators or restrooms;
    ii. An employee discussing confidential member/participant information outside the facility;
    iii. An employee leaving a copy with member/participant PHI unattended in a public area;
    iv. An employee leaving a computer unattended in an accessible area with PHI unsecured;
    v. An employee accessing and reviewing a member/participant record out of concern or curiosity;
    vi. An employee reviewing member/participant PHI to use information in a personal relationship;
        1. Corrective actions are based on individual circumstances and include but are not limited to coaching, oral warning, written warning, final written warning, termination, or if applicable, reporting to the appropriate professional licensing board

e. Requiring all employees and non-employee committee members/participants to sign either Network Health's Confidential Healthcare Information Agreement.

f. Requiring all employees to place documents containing PHI and all other business confidential documents in the locked recycling containers located throughout the building. Employees also have the option of using the designated bin labeled "Confidential - Authorized Personnel Only" located by each employee's desk for the temporary disposal of PHI and other documents containing confidential business information. However, employees are required to empty the contents of their bin into the locked recycling containers at the end of each workday to ensure the documents are disposed of properly.

g. Ensuring that data contained within reports meets the "minimum necessary standard". The data contained within a report must be de-identified when possible (i.e., does not contain member/participant names or any member/participant information that is not needed)

3. Business Associates:
    a. Network Health ensures that the use and disclosure of PHI is consistent with the requirements of the Privacy Rule. Network Health prohibits sharing member/participant PHI with any

employer/plan sponsor, agent, broker and/or third parties such as vendors or consultants without a signed and dated Business Associate Agreement/Addendum.

4. The Agreements acknowledge that PHI must be safeguarded and agrees to the following:
    a. To not use or disclose PHI other than as permitted by Network Health documents or required by law
    b. Ensure that agents and subcontractors of the Business Associate agree to the same restrictions and conditions as Network Health requires of the Business Associate regarding PHI;
    c. Prohibit the use of PHI by the Business Associate for employment or other benefit related decision;
    d. Notify Network Health of any use or disclosure of PHI that is inconsistent with the uses and disclosures established in the plan documents;
    e. Allow individuals access to PHI, including access to amend PHI;
    f. Make necessary information available to Network Health in order to provide individuals with accountings of disclosure;
    g. Procedures for return, destruction and restrictions of further use of PHI by Business Associate;
    h. Include provisions for actions if Business Associate inappropriately uses or discloses PHI.
    i. Network Health also ensures that PHI shared with employer group/plan sponsor, if implicitly or explicitly identifiable, requires a specific consent by the member/participant. Explicit information is clearly identifiable with member/participant names. Implicit information does not include specific member/participant names but includes information that may be used to identify a member/participant.
5. Practitioners/Providers/Other Third Parties:
    a. Network Health ensures that contractual agreements with third parties that provide clinical and administrative services incorporate confidentiality requirements into the agreement.
6. Non-contracted Practitioners/Providers:
    a. Network Health will verify how the information will be used and obtain from the practitioner/provider a signed agreement that indicates their compliance with specific confidentiality policies governing the use of information shared by Network Health.
7. Oversight Organizations:
    a. Network Health ensures that accrediting bodies, state and federal agencies include in their contracts, terms that describe their responsibility to maintain the confidentiality of any PHI that they receive. To the extent possible, these organizations should minimize their access to PHI. Aggregated and or de-identified data should be used whenever feasible.
8. Researchers:
    a. Network Health ensures that the intended research has appropriate reviews for and contains necessary controls to protect the confidentiality of the member/participant.

B. Use of aggregated data in which an individual's PHI is not identifiable to a statistically significant degree is not subject to privacy restrictions.

III. Use and protection of PHI for quality measurement.

A. Network Health minimizes the identifiably of the data used for quality measurement and protects the information from inappropriate disclosure.
B. All Network Health employees reviewing PHI off site will sign a confidentiality agreement as requested and protect the information from being viewed by unauthorized personnel.
C. This policy is reviewed by Network Health's compliance officer or their designee, for compliance with state and federal regulations and is approved by the Privacy and Compliance Committee. This policy will be reviewed annually, and revised as needed.

Definitions:

Individually Identifiable Health Information: As defined by 45 C.F.R. 160.103, Information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    a. That identifies the individual; or
    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information: Means individually identifiable health information, as defined by 45 C.F.R. 160.103:

1. Except as provided in paragraph (2) of this definition, that is:
    a. Transmitted by electronic media;
    b. Maintained in electronic media; or
    c. Transmitted or maintained in any other form or medium.
2. Protected health information excludes individually identifiable health information:
    a. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
    b. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
    c. In employment records held by a covered entity in its role as employer; and
    d. Regarding a person who has been deceased for more than 50 years.

Personal Representative: as defined by 42 C.F.R. 441.735, the individual's legal guardian or other person who is authorized under State law to represent the individual for the purpose of making decisions related to the person's care or well-being.

Related Policies:

n00230 – Notice of Privacy Practices
n00280 – Business Information Protection

Origination Date: 05/10/2001	**Approval Date:** 11/13/2023	**Next Review Date:** 11/13/2024
Regulatory Body: Other	**Approving Committee:** Privacy & Compliance Committee	**Policy Entity:** NHAS, NHIC, NHP
Policy Owner: Angela Keenan	**Department of Ownership:** Compliance	**Revision Number:** 6

Revision Reason:
02/15/2018 – Annual review – minor grammatical changes
08/15/2018 – Change in business practices
10/15/2018 – Updates to definitions for consistency; changed associate to employee
08/30/2019 – Updates to employee use of personal applications or services to share/receive PHI
08/05/2020 – Annual Review. No changes.
10/22/2021 - Pushed through as consent to ensure redlines can be captured. Original renewal date and approval date stand.
11/8/2021: Minor grammar changes made. Formatting of policy corrected.
10/28/2022: Removal of NCQA language no longer applicable. Approved at Privacy and Compliance Committee 12/12/2022.
10/06/2023: Updates to reflect current state of processes and references to Network Health. Removed related document as we do use it. Added definition.
11/13/2023 – Approved at Privacy and Compliance Committee