

NORTHCARE NETWORK

POLICY TITLE: Privacy and Notice of Privacy Practices Policy	CATEGORY: Compliance	
EFFECTIVE DATE: 11/4/09	BOARD APPROVAL DATE: 2/12/20	
REVIEWED DATE: 8/26/24	REVISION(S) TO POLICY STATEMENT: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	OTHER REVISION(S): <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
RESPONSIBLE PARTY: Compliance & Privacy Officer	CEO APPROVAL DATE: 9/3/24 Megan Rooney, CEO	

APPLIES TO:

NorthCare Network Personnel
Network Providers

POLICY

Personnel and Network Providers shall preserve the confidentiality and privacy of Protected Health Information (PHI) and Individually Identifiable Health Information (IIHI) (hereinafter collectively referred to as PHI). Personnel and Network Providers may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. PHI may be used or disclosed for treatment, payment and coordination of care in accordance with HIPAA, the Michigan Mental Health Code and P.A. 559 or 42 C.F.R. Part 2 and NorthCare Network policy; when it is authorized by the recipient (or guardian if applicable); or when it is mandatory under state or federal laws such as to adult or child protective services. NorthCare Network does not engage in the use of PHI for the purposes of research, marketing, or fundraising. Furthermore, NorthCare Network will not sell PHI. Network Providers shall adhere to and/or have written policies and procedures that comply with HIPAA, 42 CFR Part 2, the Michigan Mental Health Code, P.A. 559, and NorthCare Network policy.

PURPOSE

To assure the confidentiality and privacy of PHI in accordance with applicable Federal and state laws.

DEFINITIONS

1. **Disclosure** - means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
2. **Individually Identifiable Health Information (IIHI)** – is information that is a subset of health information, including demographic information collected from an individual and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 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 that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
3. **Personnel** – means employees, contracted individuals, board members, interns, students, and volunteers.

4. **Protected Health Information (PHI)** – any information, whether oral or recorded in any form or medium, that is created or received by a “Covered Entity” (or a Business Associate of a Covered Entity), and relates to the past, present, or future physical or mental health or condition of any 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.

REFERENCES

- HIPAA Privacy Standards – Health Insurance Portability and Accountability Act of 1996, 45 CFR Parts 160 and Subparts A and E of Part 164
- HIPAA Security Standards - Health Insurance Portability and Accountability Act of 1996, 45 CFR Part 160 and Subparts A and C of Part 164
- HITECH – Health Information Technology for Economic and Clinical Health Act
- 42 CFR, Part 2
- Michigan Mental Health Code, PA 258
- Public Act 559 of 2016
- MCL 330.1748, 1748a, and 1750, 258 PA 1974
- Department of Community Mental Health Administrative Rules, R 330.7051.
- Administrative Rules for Substance Abuse Programs in Michigan
- Accreditation Standards, as applicable
- NorthCare Network Breach Notification Policy
- NorthCare Network Enrollee Rights Policy
- NorthCare Network Security Policy
- NorthCare Network Consent to Share Information Policy
- NorthCare Network Coordination and Integrated Care and Treatment Policy
- NorthCare Network Social Security Number Privacy Policy
- NorthCare Network Customer Service Handbook
- NorthCare Network Notice of Privacy Practices

HISTORY

Privacy of PHI Policy combined.

REVISION DATE: 11/4/09, 5/22/13, 6/5/13, 4/2/14, 3/3/15, 10/19/16, 5/1/18, 3/25/19, 2/4/20, 11/17/20, 7/14/22, 6/2/23, 8/26/24

REVIEW DATE: 1/13/11, 1/4/12, 6/5/13, 4/2/14, 3/3/15, 1/27/16, 10/19/16, 8/9/17, 5/1/18, 3/25/19, 2/4/20, 11/17/20, 9/23/21, 7/14/22, 6/2/23, 8/26/24

CEO APPROVAL DATE: 2/15/11, 1/11/12, 6/5/13, 4/2/14, 3/3/15, 2/9/16, 11/1/16, 9/12/17, 5/10/18, 4/1/19, 2/4/20, 12/1/20, 10/5/21, 8/2/22, 6/5/23, 9/3/24

BOARD APPROVAL DATE: 11/4/09, 6/5/13, 2/12/20

PROCEDURES

- A. Personnel will be required to sign a statement attesting that they understand their responsibility to preserve confidentiality of all PHI and any other information and communication involving individuals served.
- B. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. All individuals needing access to the designated medical record and/or PHI must do so only in the course of assigned duties and responsibilities. These include reasons for payment, treatment, coordination of care

activities, reporting, claims/encounters, and auditing. All individuals must follow the standards of minimum necessary and need to know for all access to use or disclosure of protected health information.

C. Minimum necessary does not apply to:

- 1) Disclosures to or requests by a health care provider for treatment. **NOTE:** It is recommended to verify exactly what the provider is asking for before sending an “entire” record.
- 2) Uses or disclosures made to the individual.
- 3) Uses or disclosures made pursuant to an authorization under 45 CFR 164.508.
- 4) Disclosures made to the Secretary regarding compliance and investigations under 45 CFR Part 160.
- 5) Uses or disclosures that are required by law, as described by 45 CFR 164.512(a); and from a business associate that is a subcontractor.
- 6) Uses or disclosures that are required for compliance with applicable requirements of 45 CFR.

D. Individuals are required to maintain privacy and confidentiality of all PHI obtained while conducting assigned duties and responsibilities. The requirement to maintain privacy and confidentiality of this information also extends beyond the term of one’s employment/appointment.

E. Personnel are required to contact the CEO and/or the Privacy Officer when responding to court orders, subpoenas, and search or arrest warrants and in the event, Personnel have questions regarding the use or disclosure of PHI.

F. Accounting of Disclosures – Individuals have a right to receive an accounting of disclosures of PHI made by the PIHP/Network Provider in the six (6) years prior to the date on which the accounting is requested, with some exceptions. [45 CFR 164.528] NorthCare’s process is to log all disclosures made on the disclosure log to ensure all required disclosures are included.

G. Notice of Privacy Practices

1. The PIHP must:

- a) Include all rights afforded to the individual under 45 CFR 164 – HIPAA Security and Privacy law.
- b) Provide notice to individuals at time of enrollment and upon substantial changes to the notice.
- c) Remind enrollees of the availability of its Notice or Privacy Practices, as well as how to obtain a copy, no less frequently than once every 3 years.

2. Covered health care providers with a direct treatment relationship with a consumer must:

- a) give the notice to every individual no later than the date of first service delivery,
- b) make a good faith effort to obtain written acknowledgments from those individuals that they have received the provider’s notice the first time the notice is given to the consumer,
- c) post their entire notice in a clear and prominent location at the physical site where they provide services,
- d) updated notices are given to everyone at the first visit after the update and posted in a prominent location at the service site and on their website if they have one.