NORTHCARE NETWORK

POLICY TITLE: Information Security Policy	**CATEGORY:** Information Management	
EFFECTIVE DATE: 11/4/09	**BOARD APPROVAL DATE:** 11/4/09	
REVIEWED DATE: 5/24/24	**REVISION(S) TO POLICY STATEMENT:** ☐ **Yes** ☒ **No**	**OTHER REVISION(S):** ☐ **Yes** ☒ **No**
RESPONSIBLE PARTY: Chief Information Officer	**CEO APPROVAL DATE:** 6/11/24 Megan Rooney, CEO	

APPLIES TO

NorthCare Network Personnel
Network Providers

POLICY

NorthCare Network personnel and Network providers are required to maintain the confidentiality, integrity and availability of electronic protected health information (ePHI) through technical and non-technical mitigation techniques required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), Michigan Mental Health Code and 42 CFR Part 2.

PURPOSE

This policy outlines expectations to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act, Michigan Mental Health Code, 42 CFR Part 2 and any subsequent revisions.

DEFINITIONS

1. ***Computing equipment*** – refers to computers, laptops, tablets, smart phones or any other device capable of accessing ePHI.

2. ***Physical Safeguards*** – are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

3. ***Security Incident*** – the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

4. ***Protected Health Information (PHI)*** - Any information that identifies an individual and relates to at least one of the following:

    - The individual's past, present or future health care.
    - The provision of health care to the individual.
    - The past, present or future payment for health care.

5. ***Electronic Protected Health Care Information*** - Any protected health information (PHI) which is stored, accessed, transmitted or received electronically.

6. ***Business Associate*** – A person or entity that creates, receives, maintains, or transmits protected health information on behalf of, or provides services to, a Covered Entity.

7. ***Member CMHSPs*** – The five Upper Michigan Community Mental Health Service Providers; Copper Country Mental Health, Gogebic Community Mental Health, Hiawatha Behavioral Health, Northpointe Behavioral Health, Pathways Community Mental Health

8. ***Network Providers*** - refers to all providers employed or under contract with NorthCare Network

9. ***Covered Entities*** – Health plans, health care clearinghouses, or health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

10. ***Electronic Health Systems*** – NorthCare Network sanctioned, supported and recognized systems for creating, storing or transmitting electronic protected health information. NorthCare Network Electronic Health Systems include, but are not limited to: ELMER, CAFAS, Supports Intensity Scale (SIS), iCarol, Michigan Health Information Network (MiHIN) and Upper Peninsula Health Information Exchange (UPHIE).

REFERENCES

- HIPAA SECURITY - CODE OF FEDERAL REGULATIONS, 45 CFR 164
- HITECH ACT – PUBLIC LAW 111-5, DIVISION A, TITLE XIII, SUBPART D
- HIPAA OMNIBUS RULE – FEDERAL REGISTER, 78 FR 17
- MICHIGAN MENTAL HEALTH CODE
- 42 CFR PART 2
- MDHHS PREPAID INPATIENT HEALTH PLAN (PIHP) CONTRACT SCHEDULE A – STATEMENT OF WORK, SECTION Q.PART 4.
- MDHHS PREPAID INPATIENT HEALTH PLAN (PIHP) CONTRACT SCHEDULE B – HIPAA BUSINESS ASSOCIATE AGREEMENT

HISTORY

REVIEW DATE: 12/8/10, 1/13/11, 1/11/12, 1/11/12, 4/3/13, 4/2/14, 5/27/15, 3/30/16, 1/16/17, 11/14/17, 1/19/18, 11/25/18, 9/19/19, 7/26/20, 9/20/20, 7/25/21, 6/30/22, 6/22/23, 5/24/24
REVISION DATE: 4/3/13, 4/2/14, 3/30/16, 1/16/17, 11/14/17, 1/19/18, 9/20/20, 6/22/23
CEO APPROVAL DATE: 4/3/13, 4/2/14, 6/2/15, 4/1/16, 2/7/17, 12/11/17, 2/12/18, 12/4/18, 10/10/19, 8/4/20, 10/6/20, 8/3/21, 7/12/22, 6/22/23, 6/11/24
BOARD APPROVAL DATE: 11/4/09

PROCEDURES

NorthCare Network shall maintain the following standards:

A. Adhere to all applicable security and notification provisions of the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) legislation.

B. Access to Electronic Health Systems is permitted only from NorthCare Network managed equipment, Member CMHSP managed equipment or Business Associate managed equipment. No personal equipment shall be used to gain access to Electronic Health Systems.

C. Covered Entities within the NorthCare Network will conduct an assessment of information security capability for potential Business Associates prior to signing a Business Associate Agreement. If a potential Business Associate does not meet minimum security requirements, access to information systems shall not be granted.

D. Establish Business Associate Agreements with independent contractor based on the clinical or administrative functions required. Business Associate Agreements shall contain regionally approved HIPAA, HITECH and other compliance requirements.

E. Covered Entities within the NorthCare Network are required to provide adequate security and functionality training to Business Associates prior granting access to Electronic Health Systems.

F. NorthCare Network and Member CMHSPs shall participate in the design and management of shared telecommunications networks. The NorthCare Network Chief Information Officer and Member CMHSP Information Technology Department staff shall develop a comprehensive telecommunication network management plan to assist in identifying and rectifying network problems which may impact the availability of regional information systems.

G. NorthCare Network Chief Information Officer shall report security incidents with potential impact to applicable Network Providers.

H. Network Providers are required to report security incidents involving MDHHS and PIHP data to NorthCare's Security Officer, in writing, immediately upon learning of the incident

I. Security incidents involving MDHHS data must be reported by NorthCare Network in writing to the MDHHS Privacy and Security e-mail box (MDHHSPrivacySecurity@michigan.gov) immediately and no later than 24 hours from the time NorthCare becomes aware of the incident. The standard DCH-1422 HIPAA-Data Incident Report form is to be used for this purpose.