NDHIN POLICIES COMBINED

Table of Contents

INTRODUCTION

This document sets forth the policies and procedures governing the North Dakota Health Information Network (NDHIN). Standard policies and procedures have been developed to ensure the privacy and security of Individuals' Protected Health Information (PHI) while facilitating the sharing of health information to provide better quality health care.

NDHIN History

The North Dakota sixty-first legislative assembly [2009-2010] created the Health Information Technology (HIT) Office in the Department of Information Technology and created the Health Information Technology Advisory Committee (HITAC).

The HIT Office, upon recommendations of HITAC, is responsible to implement a statewide interoperable health information infrastructure that is consistent with emerging national standards; promote the adoption and use of electronic health records and other health information technologies; promote interoperability of health information systems for the purpose of improving health care quality, patient safety, and the overall efficiency of health care and public health; apply for federal funds that may be available to assist the state and health care providers in implementing and improving health information technology; establish a health information technology loan program to provide loans to health care providers for the purpose of purchasing and upgrading certified electronic health record technology, training personnel in the use of such technology, and improving the secure electronic exchange of health information.

The HITAC collaborates with and makes recommendations to the HIT office.

NDHIN Purpose

The mission of the NDHIN is to advance the adoption and use of technology to exchange health information and improve healthcare quality, patient safety and overall efficiency of healthcare and public health services of North Dakota.

Governance

The HITAC appoints a Director, and the Director, in collaboration with HITAC shall administer the NDHIN.

The North Dakota HIT Office has engaged Orion Health to provide a technology solution to facilitate the operation of the NDHIN network.

The NDHIN shall grant the use of the network to qualifying Participants and their Authorized Users. Each Participant shall execute a written agreement with the NDHIN prior to being granted access to the Network and after verification of its identity. Authorized Users shall be identified by Participants and shall execute a user agreement prior to being granted access to NDHIN.

The Health Information Technology (HIT) Director possesses the authority to suspend or terminate a Participant's or Authorized User's participation as deemed necessary.

Policies and Procedures

The HIT Director, in collaboration with the HITAC, establishes policies and procedures for the NDHIN. Policies may only be revised by the Director in collaboration with HITAC. NDHIN shall notify all Participants of any changes to the policies and procedures at least thirty (30) days prior to the implementation of the change. If changes require modifications to the Participant's system or may otherwise materially affect the Participant's operations or obligations under the Participation Agreement, NDHIN shall notify the Participant at least ninety (90) days prior to implementation of the change. However, if the change is required in order for the NDHIN and/or Participants to comply with applicable laws or regulations, the NDHIN may implement the change within a shorter period of time as the NDHIN reasonably determines is appropriate under the circumstances; provided that the NDHIN shall provide the Participants with as much notice of any such change as reasonably possible.

Definitions

For the purposes of the North Dakota Health Information Network (NDHIN) policies, the following terms shall have the meaning ascribed to them below. All defined terms are capitalized throughout the policies.

Terms used, but not otherwise defined in NDHIN policies, shall have the same meaning as those terms in 45 C.F.R. §§ 160.103, 164.304 and 164.501.

Applicable Law

Applicable Laws include the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Acts and Regulations, Health Information Technology for Economic and Clinical Health Act (HITECH), Federal and State Laws and Regulations, and Administrative Rules applicable to Individually Identifiable Health Information.

Administrative Authorized User

Administrative Authorized User means individuals who have been authorized by the NDHIN to perform services necessary for operating and maintaining the NDHIN.

Authorized User

Authorized Users are individuals who have been authorized by a Participant to participate in the HIE and may include, but are not limited to, health care providers, employees, contractors, agents, or business associates of a participant.

Breach

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Rules which compromises the security or privacy of the PHI.

Break the Glass

Break the Glass means the ability of an authorized user, who does not have an established relationship with a patient, to access a patient's PHI for treatment of the Individual in the performance of the authorized user's duties.

Business Associate

Business Associate has the meaning set forth in 45 C.F.R. 160.103 and generally means an individual or organization that creates, receives, maintains, or transmits PHI on behalf of a covered entity.

Health Information Technology Advisory Committee (HITAC)

HITAC means the North Dakota Health Information Technology Advisory Committee established by Statute, N.D.C.C. § 54-59-25.

Health Information Technology Office (HIT)

The Health Information Technology Office is established in the North Dakota Information Technology Department (ITD) by Statute, N.D.C.C. § 54-59-26, to implement and administer a health information exchange.

HIPAA Rule

HIPAA Rule or HIPAA means the Health Insurance Portability and Accountability Act of 1996. Specifically including the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic PHI (45 C.F.R. Parts 160 and 164) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009 and as any further amendments, modification, or renumbering which occurs or takes effect during the term of the policies.

Health Information Technology for Economic and Clinical Health Act (HITECH)

HITECH means the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act, Pub. L. No. 111-5.

Individual

An Individual means a person who is the subject of PHI and has the same meaning as the term "Individual" in 45 C.F.R. § 164.501 and shall include a

person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

Individually Identifiable Health Information

Individually Identifiable Health Information means a subset of health information, including demographic information collected from an Individual, that is created or received by a health care provider or plan, employer, or healthcare clearinghouse, and relates to the past, present or future physical or mental health or condition or condition or payment for healthcare and that identifies or can be used to identify the Individual.

Medical Emergency

A Medical Emergency means a medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) such that the absence of immediate medical attention could reasonably be expected to result in:

(1) placing the health of the individual (or, with respect to a pregnant woman, the health of the woman or her unborn child) in serious jeopardy, serious impairment to bodily functions, or

(2) serious dysfunction of any bodily organ or part.

This definition of a Medical Emergency Condition is found in the federal Emergency Medical Treatment and Active Labor Act (EMTALA) at 42 C.F.R. 489.24(b).

A Health Care Provider who reasonable believes in the Provider's professional judgement that a patient presents a Medical Emergency may Break the Glass.

North Dakota Health Information Network
(NDHIN)

The NDHIN is a system to electronically exchange health care information between Participants. The North Dakota Information Technology Department (ITD) is required by statute, N.D.C.C. § 54-59-26(b) to implement and administer a health information exchange that utilizes information infrastructure and systems in a secure and cost-effective manner to facilitate the collection, storage, and transmission of health information.

Participant

A Participant means an organization, health care provider or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with the NDHIN.

Participation Agreement

Participation Agreement means the Agreement between the State of North Dakota (Information Technology Department) and a Participant which authorizes the Participant to have access to NDHIN.

Patient Data

Patient Data means information that is requested, disclosed, stored, made available, or sent by a Participant through NDHIN. This includes, but is not limited to, PHI, Individually Identifiable Health Information, de-identified data (health information that does not identify an individual as defined in C.F.R. § 164.514(a)) and Limited Data Sets (PHI that excludes certain identifier information as defined in 45 C.F.R. § 164.514(e)).

Protected Health Information and Electronic Protected Health Information (PHI)

Protected Health Information means Individually Identifiable Health Information (e.g., any oral or recorded information relating to the past, present, or future physical or mental health of an Individual; the provision of health care to the Individual; or the payment for health care) that is maintained by any medium and transmitted by electronic media or in any other form or medium.

Electronic protected health information (ePHI) refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPPA) security regulations and is produced, saved, transferred or received in an electronic form.

Security Rule

The Security Rule means the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Part 160 and Part 164, Subparts A and C as may be amended from time to time.

State

State means the State of North Dakota.

Unsecured Protected Health Information (PHI)

Unsecured PHI means PHI in any form, including electronic, paper or verbal, that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in 45 C.F.R. § 164.402.

Vendor

Vendor means Orion Health, selected by the Health Information Advisory Committee, to build and provide an electronic health information exchange system for North Dakota.

INDIVIDUAL PARTICIPATION

Policy Statement: All health care information of Individuals shared through to the North Dakota Health Information Network (NDHIN) will be available for access by participating health care providers through the NDHIN unless an Individual opts out of participation.

Definition of Individual
For purposes of this policy, an Individual shall mean a person who is the subject of Protected Health Information (PHI), and shall have the same meaning as the term "Individual" as defined in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

Definition of Participant
A Participant means an organization, health care practitioner or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with the NDHIN.

NDHIN Information
At the point of care, an Individual or Individual's representative must be provided with written information in plain language about the NDHIN. The material shall describe the benefits of participation, risks of participation, how and where to obtain additional information, contact information, and a description as to how the Individual's health information will be used.

Individuals must be informed that they have the right to opt out of participation and a right to change a prior election and must be provided information on how to exercise those options, at no cost to the Individual. If an Individual later changes a prior election, the Participant receiving the new election shall maintain that documentation and shall notify the NDHIN of the change.

Effect of Opt Out
If an Individual opts out of participation in the NDHIN, that Individual's information will not be able to be searched for through the NDHIN in the future. However, a treating health care provider will still be able to select the NDHIN as a way to receive that individual's lab results, radiology reports, and other data sent directly to any treating health care provider that the provider may have previously received by fax, mail, or other electronic communications. Even if an Individual opts out of participation, limited information may be disclosed through NDHIN if subject to mandatory public health reporting and child immunization information. Minimal identifying information about the Individual will also be maintained in master patient index.

An Individual may opt out of participation with an exception providing permission to access health information in the case of a Medical Emergency or if a disclosure is required by law.

Provision of Coverage or Care
A Participant may not withhold coverage or care from an Individual on the basis of that Individual's choice to opt out of participation in NDHIN.

Reliance
If an Individual's health information is available through the NDHIN a Participant may assume the Individual has not opted-out of participation.

Minors
A minor, who may under North Dakota law consent for certain treatment without parental consent, may restrict access to information relating to treatments that a minor may obtain without parental consent. In North Dakota a minor age 14 and over may consent to treatment for sexually transmitted diseases, alcohol and drug abuse, pregnancy testing, and certain prenatal care.

A person who has authority to consent to the provision of health care to a minor is authorized to act as a personal representative.

When a minor reaches the age of majority or is emancipated, access or exercise of control of the minor's health information by a parent or legal guardian will cease. When a minor reaches the age of 18 the minor has the right to participate or opt out of participation in the NDHIN.

If a parent opted out of participation in the NDHIN on behalf of the minor that election will remain in effect following the minor's reaching the age of majority until the Individual makes a change to a prior election.

SECURITY

Policy Statement: The North Dakota Health Information Network (NDHIN), Vendor, and each Participant shall be responsible for maintaining a secure environment that supports access to, use of, and the continued development of the NDHIN.

Safeguards

NDHIN, Vendor, and each Participant shall use appropriate safeguards to prevent the impermissible access, use or disclosure of Protected Health Information (PHI) other than as permitted by the NDHIN policies, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI through NDHIN. Appropriate safeguards for NDHIN, Vendor, and Participant shall be those identified in the HIPAA Rules and other applicable federal and state standards and requirements, regardless of whether NDHIN, Vendor, and Participant is subject to HIPAA Rules. The NDHIN, Vendor, and each Participant shall be responsible for requiring each of their Business Associates and Subcontractors to agree to comply with this Security Policy.

NDHIN Administrative Authorized Users and Participant Authorized Users will be granted access to the NDHIN. All authorizing access will use the principle of "Least Privilege", that is, granting access to the minimal amount of resources required for the function that the user performs. A list of Authorized Users is maintained in the NDHIN Clinical Portal. As required in the NDHIN Participant and Authorized User Authentication Policy, Participants shall notify NDHIN within twenty-four hours, of termination of an Authorized User's employment or affiliation with the Participant. NDHIN will on a semi-annual basis audit Participant's list of Authorized Users with Participants to verify the list's accuracy.

Administrative Authorized User

Definition: Administrative Authorized User means individuals who have been authorized by the NDHIN to perform services necessary for operating and maintaining the NDHIN.

NDHIN Administrative Authorized Users shall comply with ITD's Annual Disclosure Awareness and Training and ITD's Annual Acknowledgement of Secrecy Provision.

Authorized User

Definition: Authorized Users are individuals who have been authorized by a Participant to participate in the NDHIN and may include, but are not limited to, health care providers, employees, contractors, agents, or business associates of a participant.

Reporting Security Incidents

Reporting to Participants

NDHIN will report to a Participant any successful impermissible access, use, disclosure, modification, or destruction of Participant's electronic PHI or interference with system operations in an information system containing

Participant's electronic PHI of which NDHIN becomes aware, within five (5) business days of NDHIN's learning of the event. When feasible, NDHIN will also report to a Participant the aggregate number of unsuccessful attempts of impermissible access, use, disclosure, modification, or destruction of electronic PHI or interfere with system operations in an information system containing electronic PHI of which NDHIN becomes aware, provided that these reports will be provided only as frequently as the parties mutually agree.

Reporting to Information Technology Department (ITD)
NDHIN will immediately notify ITD Service Desk at 701.328.4470 of any reportable security incident.

For purposes of this policy, security "incident" means the act of violating a security policy, which includes unwanted disruption or denial of service, the unauthorized access to a system or its data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction. While certain adverse events, (e.g. floods, fires, electrical outages, excessive heat, etc.) can cause system crashes, they are not considered incidents.

NDHIN recognizes there will be a number of unsuccessful attempts to access the network, that is, remote access attempts without authorization. The number of unauthorized remote access attempts have a demonstrable effect on incident handling capability. Therefore, an "unsuccessful security event" is defined as one that does not result in unauthorized access, use, disclosure, modification, or destruction of electronic PHI or does not result in interference with an information system. No further notice of any such unsuccessful security event will be required.

Malicious Software
NDHIN, Vendor, and each Participant shall ensure that it employs security controls that meet applicable industry or Federal standards so that the information being transmitted and any method of transmitting any such information will not introduce any malware or other program designed to disrupt the proper operation of a system, the network or any part of the network, or any hardware or software used by the NDHIN. Malicious software includes any software which, upon the occurrence of a certain event, the passage of time, or the taking of (or failure to take) any action, will cause a system or the network or any part of a system or network or any hardware, software or data used by a NDHIN, Vendor, and each Participant in connection with a system or network, to be impermissibly accessed, used, disclosed, destroyed, damaged, or otherwise made inoperable.

In the absence of applicable industry standards, NDHIN, Vendor, and each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.

Encryption
The NDHIN's vendor system shall employ Federal Information Processing Standards (FIPS) 140-2 compliant cryptography and cryptographic modules.

Policy Review: This policy will be reviewed on an annual basis.

PARTICIPANT AND AUTHORIZED USER AUTHENTICATION

Policy Statement: To protect an Individual's health information from unauthorized use, the North Dakota Health Information Network (NDHIN) shall verify the identity of Participants and their Authorized Users before access to the NDHIN is granted. Health information available through NDHIN may be accessed only by Authorized Users who have a legitimate need to access the information.

Authentication

Authentication is the process of verifying that an Authorized User who is seeking to access information through the NDHIN is the individual who the Authorized User claims to be.

Participant Authentication

The Health Information Technology (HIT) office shall review, evaluate and act upon requests submitted by organizations that want to become a Participant in the NDHIN.

Each Participant involved in NDHIN must demonstrate that it is a legitimate business by completing an application and provide the requested information and must assure that it participates in the types of health care transactions required of a Covered Entity or its Business Associate.

The Health Information Technology (HIT) Director, or designee, in collaboration with the Vendor shall determine whether an entity meets technical and operational requirements and passes the readiness assessment.

Participant identity shall be authenticated and unique user names and passwords shall be assigned by NDHIN to Authorized Users identified by Participant.

Each Participant shall designate its responsible contact person who shall be initially responsible on behalf of the Participant for compliance with these policies and to receive notice on behalf of the Participant.

The HIT Director, or designee, and each Participant shall execute a written and signed Participation Agreement prior to the Network access.

Participants shall, within five (5) working days, notify NDHIN if there is a material change in status such as a change in ownership. If the Participant ceases to engage in health care transactions, it shall notify NDHIN at least 30 days before the change.

Participants shall notify NDHIN within twenty-four hours, of termination of an Authorized User's employment or affiliation with the Participant.

Authorized Users Authentication
Participants shall designate the Authorized Users within their organizations who will be authorized to access information through the NDHIN. Participants shall develop and implement policies to assure proper identification of each Authorized User.

Authorized Users shall be required to execute a user agreement prior to network access.

Authorized Users must maintain a current relationship with a Participant to access the NDHIN.

Access of health information shall be based on the Authorized User's job function and relationship to the patient. Categories of Authorized Users shall be established, at a minimum, as the following:

1. Provider with access to clinical information and Break the Glass authority.
2. Provider with access to clinical information but no Break the Glass authority.
3. Non-provider with access to clinical information.
4. Non-provider with access to non-clinical information.

NDHIN Administrative Authorized Users shall be based on the job functions. Categories of NDHIN Administrative Authorized Users shall be established, at a minimum, as the following:

1. Administrative Authorized User with access to non-clinical information.
2. Administrative Authorized User with access to clinical information to resolve technical issues or input advance directives received from third parties.
3. Administrative Authorized user with access to clinical information for audit purposes.

Passwords
Each Authorized User shall be assigned a unique user name and password by the NDHIN.

Passwords shall meet the password strength requirements set forth in the ND Information Technology Access Control Policy.

Each Authorized User will be assigned an initial password that is required to be changed at the next use. Authorized Users shall be required to change their passwords at least every 60 calendar days and shall be prohibited from reusing passwords.

Authorized Users are prohibited from sharing their user names and passwords with others and from using the user names and passwords of others.

NDHIN shall encrypt user authentication data stored in the Network.

Failed Access Attempts
The NDHIN shall enforce a limit of consecutive failed access attempts by an Authorized User. Upon the 5th failed attempt, NDHIN shall disable the Authorized User's access to the NDHIN. The Authorized User may reestablish access using appropriate identification and authentication procedures established by the Participant.

Periods of Inactivity
The NDHIN will have an automatic log-off and will terminate an electronic session after 30 minutes of inactivity. A Participant may establish a shorter automatic log-off and termination period for an electronic session on its network or for any device or class of devices used by its Authorized Users to access the Participant's network.

Training
Participants shall provide training for all of its Authorized Users consistent with the Participant's and NDHIN policies including privacy and security requirements.

Participant Policies/Remote Access
Each Participant shall establish and enforce policies and procedures regarding Authorized User access to Patient Data (including Remote Access), the conditions that must be met and documentation that must be obtained prior to allowing an Authorized User access to Patient Data.

Policies shall include procedures for taking disciplinary actions for its Authorized Users or members of its workforce in the event of a breach or non-compliance with the policies.

The Participant may suspend, limit, or revoke the access authority of an Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's policies or the NDHIN policies. The Participant shall inform the HIT office immediately, and in any case within twenty-four hours, of any revocation or suspension.

NDHIN Authentication
NDHIN shall authenticate users accessing the NDHIN at each attempt the user accesses the Network.

AUDITS

Policy Statement: The North Dakota Health Information Network (NDHIN) shall conduct audits of health information accessed and used by Authorized Users to identify inappropriate access, verify compliance with access controls to assure confidentiality, verify appropriate use of Individually Identifiable Health Information, and assure compliance with HIPAA Rules and NDHIN policies.

NDHIN Audits

The NDHIN shall periodically audit user authentication logs. Unusual findings must be investigated and resolved in a timely manner.

The NDHIN shall audit Break the Glass on a monthly basis, scan for anomalies, and audit, at a minimum, 10 authorized users access and review findings with Participants.

The NDHIN shall conduct periodic audits of Participant usage of NDHIN and upon request, shall provide the Participant with audit reports.

The NDHIN may perform other Participant and Authorized User audits as it determines necessary.

Unauthorized access, use, or disclosure must be addressed by the Health Information Technology (HIT) Director, or designee, by taking immediate and appropriate corrective measures including the NDHIN Enforcement policy.

ENFORCEMENT

Policy Statement: The Health Information Technology (HIT) Director has the authority to suspend or terminate the participation in the North Dakota Health Information Network (NDHIN) of any Participant or Authorized User.

Emergency Suspension

If the Vendor discovers a breach or suspicious transactions and considers it necessary to take immediate action, it may suspend access to the NDHIN immediately. The Vendor shall notify the NDHIN of the action, reason for its action, and collaborate with the HIT Director to address the situation.

Authorized User Suspension or Termination

Upon the HIT Director, or designee completing a preliminary investigation and the HIT Director determining that there is a substantial likelihood that an Authorized User's acts or omissions create an immediate threat or will cause irreparable harm to another party, including, but not limited to, a Participant, an Authorized User, the NDHIN, Vendor, or an Individual whose health information is exchanged through the NDHIN; the HIT Director, or designee may suspend, to the extent necessary to address the threat, the Authorized User's NDHIN access.

A Participant may suspend, limit, or revoke the access authority of its Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's privacy policies, the NDHIN policies, or the terms of the user agreement, if it is determined by the Participant to be necessary to protect the privacy of Individuals or the security of the system. The Participant must immediately notify the HIT Director, or designee, of any action limiting access of an Authorized User.

The Participant responsible for the Authorized User shall take necessary steps to resolve the problems. Once resolved, the Participant shall notify the HIT Director, or designee, and may request reinstatement of the Authorized User's access.

The Participant must immediately notify the HIT Director, or designee, of any change to an Authorized User's job responsibilities or a change of employment status or staff privileges, including every change in an Authorized User's access whether it opens, expands, restricts, or terminates the Authorized User's access to the NDHIN.

Participant Suspension Process

The HIT Director, or designee, shall immediately but within twelve hours of suspending a Participant's access provide notice of the suspension to all Participants and provide a written summary of the reasons for the suspension to the suspended Participant. The Participant shall use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within three business days or, if such a submission is not reasonably feasible within three business days, then at the earliest practicable time.

Within five business days after submission of the Participants plan of correction, the HIT Director, in collaboration with Vendor shall review and either accept or reject the plan of correction. If the plan of correction is accepted, the HIT Director will, upon completion of the plan of correction, reinstate the Participant's access and provide notice to all Participants of the reinstatement. If the plan of correction is rejected, the Participant's suspension will continue, during which time the HIT Director, Vendor, and the Participant shall work in good faith to develop a plan of correction that is acceptable to all. If agreement cannot be reached, either party may appeal the dispute to the Health Information Technology Advisory Committee (HITAC).

Appeal Process
A Participant may appeal, in writing, the HIT Director's decision to suspend or terminate its participation in the NDHIN to the HITAC. The Committee shall review the written material from the Participant, Vendor, HIT Director, or any affected party. The Committee may hold a meeting with the parties to gather additional information. The Committee shall issue a final determination, in writing, and the decision shall be provided to all Participants.

Termination of Participation Agreement
Upon any termination of the Participation Agreement the terminated party shall cease to be a Participant and neither it nor its Authorized Users shall have any rights to use the NDHIN (unless the Authorized Users have an independent right to access the NDHIN through another Participant).

Disposition of Health Information upon Termination
At the time of termination, another Participant that received health information, may, at its election, retain the information in accordance with its document and data retention policies and procedures, applicable law, and the terms and conditions of the Participation Agreement and these policies.

The NDHIN shall retain an audit trail for a terminated Participant for at least six years.

Upon termination the NDHIN may no longer access or transmit any health information to and from the terminated Participant.

Except as retained by other Participants, Vendor must delete or destroy any health information of the terminated Participant and certify the destruction to the Director and Participants.

Governing Law
In the event of a dispute between or among the parties to the NDHIN, the laws of the State of North Dakota will govern. Any action to enforce a Participation Agreement or participation in the NDHIN must be adjudicated exclusively in the state District Court of Burleigh County, North Dakota.

Participant Policies/Remote Access
Each Participant shall establish and enforce policies and procedures regarding Authorized User access to Patient Data (including Remote Access), the conditions that must be met and documentation that must be obtained prior to allowing an Authorized User access to Patient Data.

Policies shall include procedures for taking disciplinary actions for its Authorized Users or members of its workforce in the event of a breach or non-compliance with the NDHIN policies.

The Participant may suspend, limit, or revoke the access authority of an Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's policies or the NDHIN policies. The Participant shall inform the HIT office immediately, and in any case within twenty-four hours, of any revocation or suspension of access to the NDHIN.

BREACH

Policy Statement: The impermissible use or disclosure of an Individual's Protected Health Information (PHI) will be reported and Participants shall comply with the notification requirements of 45 C.F.R. Part 164, Subpart D.

Definition of Breach

'Breach' means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Rules which compromises the security or privacy of the PHI.

The impermissible acquisition, access, use, or disclosure PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved in the incident, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed or disclosed (re-disclosed); and
4. The extent to which the risk to the PHI has been mitigated.

EXCEPTIONS. 'Breach' does not include:

- Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate.
- Inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.
- Good faith by the covered entity or business associate that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Reporting

Participants shall notify the North Dakota Health Information Technology (HIT) Office of any breach of unsecured PHI in the most expedient time possible and without unreasonable delay but no later than five (5) days following discovery.

North Dakota Health Information Network (NDHIN) will report to a Participant any use or disclosure of the Participant's PHI that is not permitted. In addition, NDHIN will report to the Participant, following discovery and without unreasonable delay, but in no event later than five (5) days following discovery, any "breach" of "Unsecured PHI" as these terms are defined by the HIPAA Rules. NDHIN shall cooperate with the Participant in investigating a breach and in meeting the Participant's obligations under the Breach Notification Rule and any other state or federal privacy or security breach notification laws.

Any such report must include the following information, if known at the time of the report:

1. the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by NDHIN to have been, accessed, acquired, or disclosed during the breach, including their contact information if available to NDHIN;
2. a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
3. a description of the types of Unsecured PHI involved in the breach (such as name, Social Security number, date of birth, home address, or account number);
4. the identify of any person who received the non-permitted PHI;
5. any steps Individuals should take to protect themselves from potential harm resulting from the breach;
6. a brief description of what NDHIN is doing or has done to investigate the breach, mitigate losses to Individuals and the Participant, and protect against any further breaches;
7. contact procedures for Individuals to ask questions or learn additional information about the breach, which must include a toll-free telephone number and an e-mail, website, or postal address at NDHIN; and
8. identification of the names and respective titles of those who conducted the investigation on the part of NDHIN, be delivered on NDHIN's official letterhead, signed by an officer or director of NDHIN or other responsible person and contain appropriate contact information should the Participant need further clarification regarding the content of the report.

If NDHIN reports to Individuals directly, NDHIN also shall prepare a draft notice, and allow Participant(s) to provide input on and review the draft notice prior to it being sent; or conduct its own reporting, if so desired. If the required information is not known at the time of the initial report to a Participant or Participants, NDHIN will follow up with an additional report or reports when the information becomes known.

Reporting If More than One Participant Involved

If there is a breach of Unsecured PHI involving more than one Participant, NDHIN will conduct the reporting on behalf of those Participants, so as to avoid duplicative reporting so long as Participant has reviewed and approved the draft notice. However, a Participant may conduct its own reporting if so desired.

NDHIN will make any required reports without unreasonable delay after approval of the content by Participant, if required, and in no event later than sixty (60) days after NDHIN learns of the breach. However, NDHIN may delay reporting if a law enforcement official determines that reporting will impede a criminal investigation or cause damage to national security, in which case reporting may be delayed in the same manner as provided under 45 C.F.R. § 164.528(a)(2).

NDHIN will include the following information in the report to Individuals:

1. a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. a description of the types of Unsecured PHI involved in the breach (such as name, Social Security number, date of birth, home address, or account number);
3. a brief description of what NDHIN is doing or has done to investigate the breach, mitigate losses to Individuals, and protect against any further breaches;
4. steps Individuals should take to protect themselves from potential harm resulting from the breach; and
5. contact procedures for Individuals to ask questions or learn additional information about the breach, which shall include a toll-free telephone number and an e-mail, website, or postal address at NDHIN. If the report mentions a Participant, the Participant has the right to approve the content of the report in advance, which approval the Participant may not unreasonably withhold.

Reporting to Individuals
NDHIN must provide the report to Individuals in writing, by first class mail, sent to the last known address of the Individual (or to the next of kin or personal representative if the Individual is deceased). If an Individual has specified a preference for electronic mail in communications with NDHIN, then NDHIN must use electronic mail. In any case in which there is insufficient or out-of-date information to provide the written notice required, NDHIN must include a conspicuous posting on its website that includes a toll-free phone number so that affected Individuals may learn whether or not their Unsecured PHI may have been included in the breach.

Reporting to Information Technology Department (ITD)
NDHIN will immediately notify ITD Service Desk at (701) 328-4470 of any breach of Unsecured PHI.

Reporting to the Media
If NDHIN believes that the breach of Unsecured PHI involved more than 500 Individuals residing within a State, NDHIN also must provide notice to prominent media outlets serving that State. The media announcement must include a toll-free phone number so that Individuals may learn whether or not their Unsecured PHI may have been included in the breach.

Reporting to HHS
If NDHIN believes that the breach of Unsecured PHI involved 500 or more Individuals, NDHIN must also immediately notify the Secretary of the U.S. Department of Health and Human Services (HHS), and must indicate in its notice to HHS that the report is made on behalf of Participants in the NDHIN to avoid duplicative reporting.

For breaches affecting fewer than 500 individuals, NDHIN will maintain a log of all such breaches occurring during the year and annually submit such log to the Secretary.

Responsibility of Vendor
If Vendor discovers a breach or suspicious transaction and considers it necessary to take immediate action, it may suspend the Authorized User's access to the NDHIN immediately. Vendor shall notify the NDHIN of the action, reason for its action, and collaborate with the HIT Director, or designee, to address the incident.

NDHIN Response to a Breach
The NDHIN may conduct an investigation of the breach, determine the extent of the breach, determine corrective actions, and may apply sanctions, as considered necessary. Participants shall cooperate in any investigation conducted by the NDHIN, state, or federal government authorities.

The NDHIN shall document its findings and any actions taken in response to an investigation. A copy shall be provided to the Participant.

Sanctions
The HIT Director may apply sanctions to Participants and their Authorized Users in the event of a breach. Sanctions may include restricting, suspending, or terminating a Participant or an Authorized User's access to the NDHIN pursuant to the Enforcement Policy, requiring Participants or Authorized Users to undergo additional training, requiring the Participant to develop a remediation plan, terminating a Participant's Agreement, or other remedies as the Director may reasonably deem necessary.

Each Participant, Vendor, or NDHIN shall be respectively liable for any monetary penalties imposed as a result of a state or federal investigation and shall implement identified corrective actions at its expense.

Participant Policies
Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable or required by law, the harmful effects that are known to the Participant of a known or suspected breach of access, use or disclosure of PHI.

Participants shall make this policy applicable to their business associates and their contractors and subcontractors.

Responsibility to the Sequoia Project
In addition to any other requirements, if NDHIN joins the Sequoia Project, the public-private partnership that operationally supports the nationwide eHealth Exchange, Participant agrees to comply with the provisions in Section 15.04 of the Restatement I of the Data Use and Reciprocal Support Agreement (FINAL May 3, 2011) ("DURSA") that require the Participant:

1. To comply with all Applicable Law;
2. To reasonably cooperate with NDHIN regarding issues related to the DURSA;
3. To Request, retrieve and send data only for a Permitted Purpose as defined in the DURSA (which is more restrictive than HIPAA);

4. To use data received from NDHIN or another Sequoia Project Participant in accordance with the terms and conditions of the DURSA;
5. To refrain from disclosing to any other person any passwords or other security measures issued to the Participant or to an Authorized User of the Participant by the NDHIN; and
6. To as soon as reasonably practicable, but no later than:

    a. one (1) hour after discovering information that leads a NDHIN Participant to reasonably believe that a Breach related to Transacting Message Content pursuant to the DURSA may have occurred, alert NDHIN to the suspected breach; and

    b. twenty-four (24) hours after determining that a Breach related to Transacting Message Content pursuant to the DURSA has occurred, provide a Notification of any such Breach to NDHIN;

In other words, if a breach (or suspected breach) occurs **WHILE** the Participant is sending, requesting, receiving, or accessing an electronic transmission of health information through the DURSA, the breach must be reported as required by this subsection. BUT IF the breach was from the Participant's EHR or electronic records system and did not occur **while** (i.e., at the same time) the Participant or the Participant's Authorized user was using the DURSA (even though the information is ePHI received or accessed through the DURSA), the breach is considered to be **not directly related to the DURSA** and should not be reported under this subsection. (Although the Participant may be required to report the breach under other NDHIN and HIPAA Notification rules).

As used in Subsection (6.), "Transacting Message Content pursuant to the DURSA" means sending, requesting, receiving, asserting, responding to, submitting, routing, subscribing to, or publishing information contained within an electronic transmission of health information transacted by an NDHIN Participant using the DURSA Specifications, including any information contained in an electronic transmission, or accompanying any such transmission such as Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonymized (partially de-identified) data, metadata, Digital Credentials, and schema.

The Notification of a DURSA breach should include sufficient information for NDHIN to understand the nature of the Breach.

1. For instance, the Notification could include, to the extent available at the time of the 24-hour Notification, the following information:

    a. One or two sentence description of the breach
    b. Description of the roles of the people involved in the breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)

c. The type of Message Content breached

d. Participants likely impacted by the breach

e. Number of individuals or records impacted or estimated to be impacted by the breach

f. Actions taken by the Participant to mitigate the breach

g. Current Status of the breach (whether under investigation or resolved)

h. Corrective action taken and steps planned to be taken to prevent a similar breach.

2. The Participant shall supplement the information contained in the Notification as it becomes available and cooperate with other Participants and NDHIN in investigating and taking corrective action in response to the breach.

The requirements do not apply to any acquisition, access, disclosure or use of information contained in or available through the Sequoia Project if the acquisition, access, disclosure or use:

1. Is not directly related to Transacting Message Content through the DURSA; or

2. Is an unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of the NDHIN or Participant if—

   a. the acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the NDHIN or Participant and

   b. the Message Content is not further acquired, accessed, disclosed or used by that employee or individual.

The requirements are addition to and do not supersede a Participant's obligations, if any, under relevant security incident, breach notification, or confidentiality provisions of the Participation Agreement, the Participant's Business Associate Agreement with NDHIN, the HIPAA Rules, or other applicable law.

USES AND DISCLOSURES OF HEALTH INFORMATION

Policy Statement: Individual Health information may be accessed only by Authorized Users through the North Dakota Health Information Network (NDHIN) for only the purposes consistent with this policy.

Compliance with Law

All disclosures and uses of health information through the NDHIN must be consistent with all Applicable Laws and the NDHIN policies, and may not be used for any unlawful or discriminatory purpose. If applicable law requires that certain documentation exist (such as an authorization) or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting Participant shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of the documentation and conditions at the request of the disclosing Participant.

Participant Permitted Purposes

A Participant may request and may disclose individual health information through the NDHIN only for purposes of treatment, payment, health care operations, to comply with public health reporting requirements, and as required by law.

Each Participant shall provide or request Individually Identifiable Health Information through the NDHIN only to the extent necessary for the permitted purpose.

Any other use of Individually Identifiable Health Information data is prohibited.

NDHIN Permitted Purposes

NDHIN may use and disclose Protected Health Information (PHI) for the following purposes:

1. for the proper management and administration of the Business Associate, in accordance with 45 C.F.R. § 164.504(e)(4);
2. subject to the Participation Agreement, NDHIN policies and procedures, and 45 C.F.R. §§ 164.504(e)(2)(i) and 164.504(e)(2)(i)(B), provide data aggregation services related to the health care operations of the covered entities with which NDHIN has a Participation Agreement;
3. manage authorized requests for, and disclosures of, PHI among Participants in the network;
4. create and maintain a master patient index;
5. provide a record locater or patient matching service;
6. standardize data formats;
7. implement business rules to assist in the automation of data exchange;
8. facilitate the identification and correction of errors in health information records; and
9. subject to the Participation Agreement and the NDHIN policies and procedures, aggregate data on behalf of multiple covered entities.

Prohibitions
Except as permitted by the HIPAA Rules, Patient Data may not be used by a Participant or NDHIN for marketing, marketing related purposes, or sales without the authorization of the Individual or the Individual's designee to whom the information pertains.

Information Subject to Special Protection
Certain health information may be subject to special protection under federal, state, or local laws and regulations (e.g., substance abuse). Each Participant shall identify any information that is subject to special protection under applicable law prior to disclosing any information through the NDHIN. Each Participant is responsible for complying with all applicable laws and regulations.

Minimum Necessary
Participants shall establish and enforce policies that permit disclosure and use of only the minimum amount of information reasonably necessary to achieve a particular purpose.

An Authorized User may access health information through the NDHIN only to the extent they need the information in connection with their job function or duties.

This minimum necessary policy does not apply to the disclosure of PHI to health care providers for treatment.

Treatment and Insurance Denial Prohibition
A health care practitioner may not deny a patient health care treatment and a health insurer may not deny a patient a health insurance benefit based solely on the provider's or patient's decision not to participate in the NDHIN.

Participant Policies
Each Participant shall have in place and shall comply with its own internal policies and procedures regarding the disclosure of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making any such disclosure.

ACCOUNTING FOR DISCLOSURE AND USE

Policy Statement: An Individual has the right to request an accounting of disclosures as defined by the HIPAA Rules.

Participant Requirements
Each Participant shall comply with the HIPAA Rules and is responsible to meet its obligations to provide Individuals with an accounting of disclosures and uses of individual health information through an electronic health record.

NDHIN Requirements
North Dakota Health Information Network (NDHIN) shall maintain an audit log documenting which Participants and Authorized Users accessed or disclosed health information about an Individual through the NDHIN and when that information was accessed.

Upon Participant's written request for an accounting, or an Individual's written request for an accounting of disclosure of their own health information, NDHIN shall provide an accounting of disclosures of health information to the Participant, or directly to the Individual if requested by the Individual, within ten (10) days of the request.

NDHIN will not charge a fee for the first request for an accounting within a calendar year but may charge a reasonable and cost-based fee for providing an additional accounting within the same calendar year. If a fee will be required, NDHIN shall inform the Participant, or the Individual, if the account is sent directly to the Individual, at the time of the request.

NOTICE OF PRIVACY AND DATA PRACTICES
NORTH DAKOTA HEALTH INFORMATION NETWORK (NDHIN)

"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

Purpose of NDHIN and who has access to health information
NDHIN is a system created to securely allow your health information to be shared electronically with all of your health care providers that participate in the NDHIN.

NDHIN established systems and procedures that seek to assure your information is consistently and accurately matched to you.

Information is encrypted when sent through NDHIN, which means it cannot be read by unauthorized persons even if received or accessed by an unauthorized person.

Your health information may be used, consistent with state and federal law, for the following purposes:

- **Treatment Purposes:** Each treating physician will be able to access another treating physician's electronic records to better treat you.
- **Payment Purposes:** Information may be sent to health care payers for payment of treatment you receive.
- **Public Health Purposes:** Information may also be sent to the Health Department if required by law, such as immunization information for children.

A health care provider and other entities, such as insurance payers, may participate in the NDHIN after completing an agreement and assuring compliance with all laws pertaining to confidentiality of health information and with NDHIN policies. Their employees are restricted as to what information they may have access to depending on their need for the information. For example, the receptionist is only allowed to see your demographic information such as your name, address, the name of your insurance company. A physician or other health care professionals, such as nurses, may be able to view most of your health information if necessary for your treatment.

NDHIN Protects Health Information
NDHIN complies with patient privacy rights in accordance with state law and the Privacy and Security Regulations enacted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

If substance abuse and addiction treatment information is protected by federal law, it is not available to any other health care provider unless you have given written consent for them to access the information or in the case of a medical emergency.

Opt-Out
You have the right to opt out of participation in the NDHIN. Opt out means your written decision that your Protected Health Information (PHI) cannot be searched for through the NDHIN by a health care provider except as required by law or as authorized by you in the case of an emergency.

Even if you opt out, a health care provider may elect to receive through the NDHIN your lab results, radiology reports, and other data sent directly to them that the provider may have previously received by fax, mail, or other electronic communications from a laboratory, radiology facility, etc. providing services to that provider.

Care and Benefits
A health care provider, health insurer or government health plan may not withhold coverage or care nor may a health insurer deny a health insurance benefit based solely on your choice to opt out of the NDHIN.

Requesting Restrictions on Certain Uses and Disclosures
You have the right to object to, and ask for restrictions on, how your health information is used or to whom the information is disclosed.

You have the right to restrict disclosures of your health information to health plans for products or services paid for in full out of pocket.

Sale of Protected Health Information
Your health information may not be sold without your consent and NDHIN will not sell your health information to any third party.

Marketing and Fundraising
NDHIN must have your written authorization before sending marketing communications to you. You have the right to opt out of receiving future fundraising communications.

Requesting Amendments to Health Information
You have the right to request an amendment of incorrect Individually Identifiable Health Information available through the NDHIN.

Receiving an Accounting of Disclosures of Health Information
You have the right to request an accounting of disclosures as defined by the Health Insurance Portability Accountability Act Privacy Rules.

Access, Inspection and Copying of Health Information
You or your designee have the right to request an electronic copy of your Individually Identifiable Health Information that is available through the NDHIN. The NDHIN may provide the health information directly to you or may require health care providers participating in the NDHIN to provide access or an electronic copy to you.

Notification of a Breach
You have the right to be notified, pursuant to Title 45, Code of Federal Regulations, part 164, subpart D, of a breach that affects your Individually Identifiable Health Information.

Complaints
You have the right to file a complaint as defined in the NDHIN policies and procedures. The complaint must be in writing and may be filed with a Participant or directly with the NDHIN.

Availability of NDHIN's Notice of Data Practices
You have the right to receive the notice of privacy and data practices in a timely manner. Upon request, you may at any time receive a paper copy of the notice, even if you earlier agreed to receive the notice electronically.

Summary of Rights

- Right to receive Notice of Privacy and Data Practices.
- Right to opt-out.
- Right to care and benefits.
- Right to request restrictions on certain uses and disclosures of PHI.
- Right to amend PHI.
- Right to receive an accounting of disclosures of PHI.
- Right to access, inspect and copy PHI.
- Right to request restrictions on marketing and fundraising.
- Right to receive notification of a breach.
- Right to file a complaint.

CONTACT INFORMATION
For additional information, copies of forms, copy of this notice or if you have questions, please contact NDHIN at:

Phone: (701) 328-1983 or toll free (855) 761-0534.
Website: www.ndhin.org
Address: 4201 Normandy Street
Bismarck, ND 58503-1324

AMENDMENT OF DATA

Policy Statement: Individuals may request an amendment of their Protected Health Information ("PHI").

Definitions
"Amendment" as used in this Policy means the correction of previously recorded Protected Health Information or other information maintained in a designated record set, but does not include changes in vital signs, laboratory reports, or other health information created during a new encounter with a provider or other covered entity.

"Authorized Users" are individuals who have been authorized by a Participant to participate in the Health Information Exchange and may include, but are not limited to, health care providers, employees, contractors, agents, or business associates of a participant.

"Individual" means a person who is the subject of Protected Health Information (PHI) and has the same meaning as the term "Individual" in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

"Participant" means an organization, health care provider or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with the NDHIN.

Accepting Requests for Amendments
If an Individual requests an amendment to the individual's Protected Health Information or other information that is created by the NDHIN, the NDHIN shall respond to the request as required by 45 C.F.R. 164.526.

If an Individual requests an amendment to the individual's Protected Health Information, NDHIN, as permitted by 45 C.F.R. 164.526, may deny an individual's request for an amendment, if NDHIN determines that the Protected Health Information or record that is the subject of the request was not created by the NDHIN, unless an exception set forth in 45 C.F.R. 164.526 applies.

If the information subject to a request for an amendment was created by a Participant, the NDHIN shall forward the request to that Participant, and inform the individual requesting the amendment that the request was transferred to that Participant.

Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information.

Informing other Participants
If the Participant that created the information accepts the requested amendment, in whole or in part, the covered entity must as required by 45 C.F.R. 164.526(c), make reasonable efforts to

inform and provide the amendment within a reasonable time to: (i) persons identified by the individual as having received Protected Health Information about the individual and needing the amendment; and (ii) persons, including business associates, that the Participant knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on that information to the detriment of the individual.

Application to Business Associates and Contractors

Participants shall make this policy applicable to their Business Associates ("BA") and to the contractors and subcontractors of their BAs as required by the HIPAA Rules.

COMPLAINT PROCESS

Policy Statement: The North Dakota Health Information Network **(**NDHIN) provides a complaint process for any Individual or Participant to register a complaint.

Definitions
"Authorized Users" are individuals who have been authorized by a Participant to participate in the HIE and may include, but are not limited to, health care providers, employees, contractors, agents, or business associates of a Participant.

"Individual" means a person who is the subject of Protected Health Information (PHI) and has the same meaning as the term "Individual" in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

"Participant" means an organization, health care provider or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with the NDHIN.

Who May file a Complaint
An Individual or a person on behalf of an Individual may file a complaint concerning:

- the impermissible use, disclosure or disposal of PHI
- denials of access to Individual PHI
- retaliation against an individual for filing a complaint

A Participant or its Authorized Users, or member of the NDHIN workforce may file a complaint concerning the following issues:

- violation of policies and procedures
- the impermissible use, disclosure or disposal of PHI
- retaliation against an individual for filing a complaint

Complaints relating to a Participant or its Authorized Users
Each Participant shall implement a process for workforce members, agents, contractors and Individuals to report any non-compliance with policies and a process for Individuals whose health information is shared through NDHIN to file a complaint with the Participant about impermissible disclosures and uses of information about them.

The Participant shall investigate the complaint and shall provide a written response to the complainant. The response must include information about how the complainant may forward the complaint to the NDHIN if the complaint concerns NDHIN.

Complaints relating to the NDHIN
The complaint must be in writing and contain the complainant's name and contact information. No personal health information should be included. Verbal complaints will

not be accepted by NDHIN. Anonymous complaints will not be accepted by NDHIN. The form is available at www.ndhin.org or call NDHIN at 701.328.2508. The complaint form may be submitted by mail or electronically.

If the complaint relates to a suspected violation or breach of PHI, the complaint must be filed within 180 days from the date of becoming aware of a suspected violation.

If the complaint relates to NDHIN, NDHIN shall review and investigate the complaint.

A complaint against NDHIN must be submitted to:

North Dakota Health Information Network
c/o Privacy Officer
4201 Normandy Street
Bismarck, ND 58503-1324
Phone: 701.328.2508

Or submitted by email to: ndhin@nd.gov

NDHIN shall acknowledge receipt of the complaint within 2 business days.

NDHIN shall issue a written response to the Individual or Participant within 30 days of receipt of the complaint, unless under extenuating circumstances, NDHIN may extend this deadline and provide the Individual or Participant written notification of the delay.

The response must include information about how the complainant may forward the complaint to the Health Information Technology (HIT) Director.

If the complainant is not satisfied by the NDHIN investigation, findings, and any proposed resolution of the complaint, the complainant may send the complaint to the HIT Director for further review and consideration.

A complaint may be sent to the Health Information Technology Advisory Committee for review if there is a conflict for the HIT Director in reviewing the complaint.

The disposition of a complaint shall be documented by NDHIN.

General
NDHIN will maintain the confidentiality of the Individual who files a complaint.

NDHIN shall not retaliate, discriminate against, intimidate, coerce, or threaten any person who files a complaint.

Documentation concerning a complaint including response and resolution shall be maintained by NDHIN for six (6) years.

NDHIN shall periodically analyze filed complaints to determine if persistent or recurrent problems exist and make recommendations to correct identified problems.

Filing a Complaint with U.S. Department of Health and Human Services
Individuals are encouraged to file a complaint with a Participant or the NDHIN to resolve an issue. However, an Individual or a person on behalf of an Individual may also file a complaint with the Secretary of the U.S. Department of Health and Human Services, Office of Civil Rights, within 180 days from the date of becoming aware of a suspected violation of the Individual's Protected Health Information or privacy rights.

Limitation on the Right of an Individual to Access Their Own PHI

Policy Statement: The North Dakota Health Information Network (NDHIN) shall limit the right of an Individual to access their own PHI or that of a family member.

Individual Access to their own PHI
An individual who is an "authorized user" of a "participant" may not access his or her own protected health information through the clinical portal of the North Dakota health information network.

Individual Access to a family member's PHI
An individual who is an "authorized user" of a "participant" may not access the protected health information of a family member through the clinical portal of the North Dakota health information network unless the user is a health care provider that has a provider-patient relationship with the family member, or is another authorized user who is accessing the protected health information of a family member for treatment of the Individual.

As used in this section, "family member" has the meaning set forth in section 103 of part 160 of title 45 of the Code of Federal Regulations.

> 45 C.F.R. § 160.103
> *Family member* means, with respect to an individual:
>
> > 1. A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
> >
> > 2. Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).
> >
> > (i) First-degree relatives include parents, spouses, siblings, and children.
> > (ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
> > (iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
> > (iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Patient Portal Participation by Minors and Parents of Minors

Policy Statement: The North Dakota Health Information Network (NDHIN) shall limit participation of a patient and patient representative to the patient portal of the North Dakota health information network.

Participation of a Patient

The PHI of an unemancipated minor may not be accessed through the patient portal of the North Dakota health information network.

Participation of a Patient Representative

The personal representative, including the parents, of an unemancipated minor must not be invited to or participate on behalf of the unemancipated minor in the patient portal of the North Dakota health information network.

If a parent wishes to obtain a copy of, or access to, their minor child's health information the parent must make a manual request to NDHIN (or a health care provider) and a Communicate (Direct Secure Message) email with the requested information will be sent to the parent.

Definitions

1. "*Minor*" means an individual under eighteen years of age.
2. "*Unemancipated minor*" means an individual who is under 18 years of age and is under the care or supervision of his or her parents or legal guardian.
3. "*Emancipated minor*" means an individual who is under eighteen years of age but who is regarded in the eyes of the law as being old enough—usually because he or she is married, in the military, financially independent, or otherwise no longer dependent on their parents—to make adult decisions and exercise general control over his or her own life.