NORTH Dakota Be Legendary.™

Health Information Network
INFORMATION TECHNOLOGY

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.

Revised: 11-2016
12-2020

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.