NORTH Dakota Be Legendary.™

Health Information Network

INFORMATION TECHNOLOGY

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 CFR 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 of 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 Network (NDHIN) 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.

Revised: 11-2016
12-2020

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, NDHIN has participated in the Sequoia Project, the public-private partnership that operationally supports the nationwide eHealth Exchange for a number of years, In doing so NDHIN agreed 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.