

NORTHCARE NETWORK

POLICY TITLE: Breach Notification and Management	CATEGORY: Compliance & Privacy	
EFFECTIVE DATE: 8/13/14	BOARD APPROVAL DATE: 4/13/16	
REVIEW DATE: 10/23/23	REVISION(S) TO POLICY STATEMENT: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	OTHER REVISION(S): <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
RESPONSIBLE PARTY: Compliance & Privacy Officer	CEO APPROVAL DATE: 11/7/23 Megan Rooney, CEO	

APPLIES TO

NorthCare Network Personnel
Network Providers
Business Associates

POLICY

NorthCare Network, a HIPAA Covered Entity (CE), and other Covered Entities and all Business Associates (BA) must provide notification following the discovery of a breach of unsecured protected health information. (45 CFR §§ 164.400-414).

PURPOSE

To ensure compliance with regulatory standards regarding breaches of privacy and breach notification requirements.

DEFINITIONS

1. ***Breach*** means an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information.

There are three exceptions to the definition of “breach” which are:

- (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of NorthCare Network or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted.
- (ii) Any inadvertent disclosure by an employee who is authorized to access protected health information to a business associate, or another employee authorized to access protected health information and the information received because of such disclosure is not further used or disclosed in a manner not permitted.
- (iii) A disclosure of protected health information where NorthCare Network or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. **Unsecured protected health information** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals using a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 (HITECH Act) on the HHS Web site.
3. **Workforce** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for NorthCare Network or a business associate, is under the direct control of NorthCare Network or a business associate, whether they are paid by NorthCare Network or a business associate.

REFERENCES

45 CFR § 164 Privacy of Individually Identifiable Health Information
45 CFR § 164.400-414 Breach Notification Rule
Public Law 111-5 Health Information Technology for Economic and Clinical Health Act (HITECH Act)
Public Act 452 of 2004, Identity Theft Protection Act
NorthCare Information Security Policy
NorthCare Security Incident Response Procedure

HISTORY

REVISION DATE: N/A, 3/16/16, 6/30/16, 1/19/18, 11/26/18, 9/29/19, 4/22/21, 1/13/22, 10/19/22, 10/23/23

REVIEW DATE: N/A, 5/22/15, 3/16/16, 6/30/16, 4/19/17, 1/19/18, 11/26/18, 6/23/20, 4/22/21, 1/13/22, 10/19/22, 10/25/23

CEO APPROVAL DATE: 7/15/14, 6/2/15, 4/4/16, 7/5/16, 5/2/17, 2/27/18, 12/4/18, 10/10/19, 7/6/20, 5/4/21, 2/1/22, 11/1/22, 11/7/23

BOARD APPROVAL DATE: 8/13/14, 4/13/16

PROCEDURES

I. Administrative Requirements and Burden of Proof

- A. An impermissible use or disclosure of protected health information (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 protected health information has been compromised based on a risk assessment of at least the following factors:
 1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
 2. The unauthorized person who used the protected health information or to whom the disclosure was made.
 3. Whether the PHI was acquired or viewed; and
 4. The extent to which the risk to the PHI has been mitigated.
- B. Policies, Training and Enforcement
Covered Entities must have in place written policies and procedures regarding privacy of PHI and breach notification.
- C. Training
Covered Entities' personnel must be trained on the policies and procedures with respect to protected health information, privacy and security practices, and

breach notification as necessary and appropriate for personnel to perform their duties.

D. Refraining from Intimidating or Retaliatory Acts

Covered Entities may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this procedure or any Privacy Practices, including the filing of a complaint under this section.

E. Waiver of Rights

NorthCare Network will not require individuals to waive their rights under federal privacy laws as a condition of the provision of treatment, payment, enrollment, or eligibility for benefits.

II. Reporting and Documentation Requirements

Personnel who believe there has been a breach of protected health information shall notify NorthCare Network's Privacy Officer immediately.

A. Upon receipt of a breach or suspected breach of PHI, NorthCare Network will:

1. Record the date that the suspected breach was known or should have been known, to the organization.
2. Determine if an actual breach occurred; and
3. If a breach occurred:
 - i. Record the date the breach occurred.
 - ii. To the extent practicable, mitigate the cause of the breach.
 - iii. Provide notice, as required by federal law, to the individual affected by the breach outlined below.
 - iv. Provide notice, as required by federal law to the Department of Health and Human Services, as outlined below; and
 - v. Conduct post-breach evaluation and remediation.
4. Ensure all required notifications have been provided or that the use or disclosure of unsecured PHI did not constitute a breach.
5. With respect to an impermissible use or disclosure, NorthCare will maintain documentation that all required notifications were made, or alternatively, documentation to demonstrate that notification was not required, such as: (1) the risk assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

III. Breach Notification Requirements

A breach shall be treated as discovered as of the first day on which such breach is known by the CE/BA, or, by exercising reasonable diligence would have been known to the CE/BA. CE/BA shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent.

Following the discovery of a breach of unsecured protected health information, CE shall notify everyone whose unsecured protected health information has been, or is

believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

A. Individual Notice

CE shall notify affected individuals in written form by first class mail to their last known address. Notice must be provided without unreasonable delay and in no case later than sixty calendar days after discovery of a breach. Notification may be provided in one or more mailings as information is available. If the individual is deceased written notification by first class mail will be sent to the personal representative of the individual, if known.

1. The notice shall include:

- a) A brief description, in plain language, of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- b) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
- c) Any steps individuals should take to protect themselves from potential harm resulting from the breach.
- d) A brief description of what the CE is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- e) Contact information for individuals to ask questions or learn additional information, including a toll-free number and email address.

B. Substitute Notice – **Insufficient or Out-of-Date Contact Information**

1. If CE has insufficient or out-of-date contact information for **fewer than ten** individuals, CE may provide substitute notice by an alternative form of written notice, by telephone, or other means.
2. If CE has insufficient or out-of-date information for **ten or more** individuals, CE must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individual likely resides. A toll-free phone number that remains active for at least 90 days must be included.
3. These notices must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, the same information as noted in A.1 above.

C. Additional Notice in Urgent Situations

If CE deems a breach to be a potential for imminent misuse of unsecured PHI, CE may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice.

D. Notification to the Media

For a breach of unsecured protected health information involving more than five hundred residents of a State or area, CE shall notify prominent media outlets serving the State or area. Media notification shall be provided without unreasonable delay and in no case later than sixty calendar days after discovery of a breach. Media notification shall include the same information required for the individual notice.

- E. **Notification to the Secretary of Health and Human Services**
In addition to notifying affected individuals and the media (where appropriate), CEs must notify the Secretary of breaches of unsecured PHI. Notification is made electronically at the HHS web site on the breach report form provided. If a breach affects five hundred or more individuals, CE must notify the Secretary without reasonable delay and in no case later than 60 days following the discovery of a breach. If, however, a breach affects fewer than five hundred individuals, CE may notify the Secretary of such breaches on an annual basis, no later than 60 days after the end of the calendar year in which the breaches are discovered.
- F. **Notification to a Covered Entity**
If NorthCare Network is a Business Associate of another Covered Entity, NorthCare Network will notify the covered entity immediately following the discovery of a potential breach of the covered entity's protected health information. The Covered Entity will file necessary notification to individuals, Secretary of HHS, and the media, as applicable, unless stated otherwise in the Business Associate Agreement.
- G. **Law Enforcement Delay**
If a law enforcement official states that a notification, notice, or posting required under this procedure would impede a criminal investigation or cause damage to national security, CE or a BA shall:
- a) delay such notification, notice, or posting for the time period specified by the official, if the statement is in writing and specifies the time for which a delay is required, or
 - b) document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, if the statement is made orally; or unless a written statement as described in paragraph (a) of this section is submitted during that time.

IV. Notification by a Business Associate to NorthCare Network as the Covered Entity

A Business Associate shall notify NorthCare Network immediately following the discovery of a breach of unsecured protected health information as outlined in this policy. NorthCare Network, as the CE, is responsible for breach notification to the individual, Secretary of Health and Human Services, and the media, as required, unless delegated to the Business Associate and stated in the Business Associate Agreement.

V. When is Breach Notification Not Required?

Required notifications are only required if the breach involved unsecured protected health information. Encryption and destruction are technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. Covered entities and business associates that secure information as specified by this guidance are not required to provide notifications following the breach of such information.