

Communication Sciences and Disorders, Speech-Language-Hearing Clinic

Policies and Procedures

**Title: Responding to Breaches of Protected Health Information (PHI)**

**Policy #10**

**POLICY STATEMENT**

It is the purpose of this Breach Notification policy to provide guidance when an unauthorized or impermissible acquisition, access, use, or disclosure of unsecured protected health information occurs. This policy sets forth the Northern Arizona University Breach Notification requirements in accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act and its related regulation, “Breach Notification for

Unsecured Protected Health Information.”

**DETAILED POLICY STATEMENT**

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act in conjunction with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA), and their related regulations promulgated by the U.S. Department of Health and Human Services mandate that any form of individually identifiable health information be safeguarded appropriately so as to remain private and secure. When there is unauthorized acquisition, access, use, or disclosure of protected health information that has not been

secured through technology or methodology specified by the Secretary for the U.S. Department of Health and Human Services (“HHS”), Northern Arizona University is required to address breach notification requirements. As defined within the Breach of Unsecured Protected Health Information Regulation, “unsecured protected health information” means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary for HHS in guidance issued under the HITECH Act. The Breach of Unsecured Protected Health Information Regulation became effective September 23, 2009.

**APPLICABILITY**

Northern Arizona University workforce members of covered components as defined in the Hybrid Entity.

**POLICY AUTHORITY**

Northern Arizona University HIPAA Privacy Officer

**REFERENCES**

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Health Information Technology for Economic and Clinical Health (HITECH) Act, ARRA Title XIII,

Subtitle D

U.S. Department of Health and Human Services Breach Notification for Unsecured Protected

Health Information Regulation, 45 CFR §164.400 et seq.

Title: Responding to Breaches of Protected Health Information (PHI)

Owner: Privacy Officer

Page 2 of 6

**IMPLEMENTATION PROCEDURES**

**A. Breach of Unsecured Protected Health Information:** A Breach of Protected Health Information (“PHI”) occurs when there is unauthorized acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule, unless an exception or a “low probability of compromise” determination is made.

**B. Discovery of Breach:** A Breach of Protected Health Information or potential Breach of Protected Health Information shall be treated as discovered by NAU as of the first day the breach is known to the NAU staff or faculty member or by exercising reasonable diligence would have been known to the NAU member. This includes breaches by Business Associates of NAU.

1. NAU 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 Business Associate of NAU.

2. Following discovery of a potential breach, NAU shall begin an investigation.

**C. Breaches and Notification:** NAU is committed to the prevention of Breaches with respect to PHI. Suspected breaches of unsecured PHI will be reviewed and assessed by the HIPAA Privacy Officer and/or Security Officer and other appropriate NAU workforce (including, for example, the Office of University Counsel, IT Security, and Human

Resources). The results of the assessment will be used to determine the actions to be taken in response to the actual or suspected Breach. The **Breach Notification Tree** beginning of Page 5 of this policy will be utilized to assess the breach.

1. **Internal Notification**: (for Assessment and Response): Any NAU workforce member who becomes aware of a suspected or actual Breach must immediately notify his or her supervisor who must notify the HIPAA Privacy Officer.

2. **Breach by Business Associate**: In the event that a Business Associate becomes aware of a potential Breach, the Business Associate immediately must notify the office and official of NAU with whom the Business Associate contracted to perform the contracted service. The contacted NAU official must then immediately notify the HIPAA

Privacy Officer.

**3. External Notification**:

a. **Required Notification to Affected Individuals**: In the case of a Breach of Unsecured PHI that is discovered by NAU, and which Breach is determined by NAU to be a reportable Breach, NAU shall notify each individual whose Unsecured PHI has been or reasonably believed to have been acquired, accessed, used, or disclosed as a result of the Breach. The Privacy Officer shall be responsible for drafting the notification letter to each of the individuals identified as having been affected by a Breach, and all information related to the Breach necessary for drafting the notifications shall be made available to the Privacy Officer. Without unreasonable delay, but in no case later than 60 calendar days after discovery of the Breach, NAU, through the appropriate office, shall take the

following actions:

Title: Responding to Breaches of Protected Health Information (PHI)

Owner: Privacy Officer

Page 3 of 6

(i) **Notice to Affected Individuals**: Notify affected individuals (or next of kin if deceased) in writing by first class mail at the last known address of the affected individual (or by electronic communication if so indicated by the individual is the preferred method of communication) of the following information:

a) A brief description of the Breach, including the date of the Breach and the date of discovery;

b) A description of the types of PHI that were involved in the Breach;

c) Steps that individuals should take to protect themselves from potential harm resulting from the Breach;

d) A brief description of NAU’s remedial measures in response to the Breach, including investigations, mitigation of losses and protection against further Breaches; and

e) Contact information for NAU, or its designated agent, including, as appropriate, a toll-free telephone number, e-mail address, website, or postal address where individuals can obtain additional information and make requests.

(ii) **Substitute Form of Notice**: If there is insufficient or no up-to-date contact information precluding direct written communication to an individual, then a substitute form of notice shall be provided. If there is insufficient or out-of-date contact information for ten (10) or more individuals, NAU shall provide a toll-free telephone number where

individuals can learn if they have been affected by the Breach by:

a) Posting a notice of the Breach on the NAU website as specified by the U.S. Department of Health and Human Services; or

b) Placing a notice in major print or broadcast media in geographic areas where the affected individuals are likely to reside.

b. **Emergency Notice:** If the Privacy Officer or the Office of University Counsel deems that a Breach notification is urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other means is permitted, as appropriate, in addition to written notice.

c. **Required Notification to Media**: Notice of a Breach shall be provided to prominent media outlets serving the state if the unsecured PHI of more than 500 residents of such state has been or is reasonably believed to have been acquired, accessed, used or disclosed as a result of a Breach.

d. **Required Notification to the Secretary of the U.S. Department of Health and Human Services (HHS):** Notice shall be provided to the Secretary of HHS of aBreach of unsecured PHI for which Notice to an affected individual has been or willbe provided.

(i) If the Breach involves the data of 500 or more individuals, the Privacy Officer shall notify the Secretary of HHS in the manner as specified at www.hhs.gov at the same time notice is made to the individuals.

(ii) Breaches that involve the data of fewer than 500 individuals will be maintained in a log and the Breach information submitted annually to the Secretary, no later than 60 days after the end of the calendar year.

(iii) If a Breach involves “secure” PHI, no notification to HHS is required.

e. **Law Enforcement Delay**: Notice to affected individuals shall be delayed if law enforcement informs NAU that disclosure of a Breach would impede a criminal investigation or jeopardize national security.

(i) A request for delayed notification must be made in writing or documented contemporaneously by NAU in writing, including the name of the law enforcement officer making the request and the officer’s agency engaged in the investigation.

(ii) The required notice shall be provided without unreasonable delay after the law enforcement agency communicates to NAU the law enforcement agency’s determination that notice will no longer impede

the investigation or jeopardize national or homeland security.

**D. Documentation:** Documentation of a Breach incident shall be maintained for at least six (6) years after a Breach incident has been closed and any required notification sent.

Title: Responding to Breaches of Protected Health Information (PHI)

Owner: Privacy Officer

Page 4 of 6

**E. Sanctions**: NAU shall have in place and apply appropriate sanctions for failure to comply with privacy policies and procedures.

**F. Retaliation/Waiver**: NAU may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. NAU may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

**DEFINITIONS**

**1. Breach:** A “breach” means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA which compromises the security or privacy of the protected health information.

a. **“Access” and “Acquisition”** to information is based on their plain meanings.

b. **“Unauthorized”** is an impermissible use or disclosure of protected health information under the HIPAA Privacy Rule.

**2.** The term **“Breach” does not include**:

a. Any unintentional acquisition, access, or use of protected health information by an employee or individual acting with authorization if:

(i) such acquisition, access, 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 NAU or Business Associate; and

(ii) such information is not further acquired, accessed, used, or disclosed by any person;

or

b. any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by NAU or Business Associate to another similarly situated individual at the same facility; and

c. any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

**3. Business Associate:** A Business Associate is a party with whom NAU enters into a contract in order to perform a service that NAU otherwise would perform for itself. Pursuant to HIPAA, the contract is called a “Business Associate Agreement” (BAA). The Business Associate “steps into the shoes” of NAU with regard to the responsibility to protect PHI, including responsibility to report a Breach to the NAU HIPAA Privacy Officer.

**4. Disclosure:** Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of PHI outside of the entity holding the information.

**5. Individual**: The person who is the subject of the PHI.

**6. Protected Health Information (“PHI”):** Protected Health Information (PHI) is information created by a health care provider, health plan, or health care clearinghouse that identifies an individual or provides a reasonable basis to believe the information can be used to identify the individual and that relates to:

a. the past, present, or future physical or mental health or condition of an individual;

b. the provision of health care to an individual;

c. the past, present, or future payment for the provision of health care to an individual; and

d. that is transmitted or maintained in any form or medium, including electronic information.

Title: Responding to Breaches of Protected Health Information (PHI)

Owner: Privacy Officer

Page 5 of 6

**7. Reasonable Diligence:** Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

**8. Unsecured Protected Health Information:** As defined within the Breach of Unsecured Protected Health Information Regulation, unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary for the U.S. Department of Health and Human Services in guidance issued under the HITECH Act.

**9. Workforce Member:** Consistent with HIPAA and for purposes of this policy, “workforce member” means employees, volunteers, students, trainees, and other persons whose conduct, in the performance of work for NAU or a Business Associate of NAU, is under the direct control of NAU or the Business Associate, whether or not they are paid by the NAU or the Business Associate.

a. A person is acting under the authority of NAU if he or she is acting on its behalf.

b. A person may include a Business Associate or an employee of a Business Associate

**Breach Notification Tree:**

Not reportable if:

\*Secured or destroyed

\*Used within an entity, and

- unintentional, in good faith, with no further use or disclosure

- inadvertent and within job scope, with no further use or disclosure

\*Information cannot be retained

\*Not reportable if a “low probability of compromise” of data. Based on a risk assessment including:

-what was the info (and is its release “adverse to the individual”)

-to whom was it disclosed

- was it actually acquired or viewed

-the extent of mitigation

**Step 1**

Was there acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule?

**Step 2**

Was the information secured according to HHS guidance, or destroyed?

**Step 3**

Was the potential breach internal to your organization, AND unintentional, in good faith, with no further use, or inadvertent and within job scope?

**Step 4**

Is there no way the breached information can be retained?

Title: Responding to Breaches of Protected Health Information (PHI)

Owner: Privacy Officer

Page 6 of 6

**Step 5**

If step 5 is reached, there is a breach, and the probability of compromise is the last evaluation. If there is a low probability of compromise, it is not reportable and is the end of the process.

**Perform Breach Notification Risk Assessment**

Not reportable if there is a “low probability of compromise” of the data, based on a risk assessment including at least:

\*what was the information and how well identified was it (and is its release “adverse to the individual”)

\*to whom it was disclosed and was it actually viewed

\*the extent of mitigation

**Factor 1**

Evaluate the nature and extent of the PHI involved including the types of identifiers and the likelihood of re-identification. Consider:

-Financial and clinical sensitivity of the information

-Are direct or indirect identifiers included

-Can the information be linked for re-identification

-Does the person receiving the PHI have the ability to re-identify

**Factor 2**

Evaluate the nature of the unauthorized person who used the PHI or to whom the disclosure was made. Consider:

-Does the person have obligations to protect the privacy and security of the PHI

-Is the identity of the unauthorized person known

-What is the likelihood that the information would be used by an unauthorized recipient to adversely affect individuals for personal gain.

**Factor 3**

Evaluate whether the PHI involved was actually acquired or viewed. Consider:

-Was there opportunity to acquire or view the PHI

-Was the potential breach discovered and prevented before PHI was viewed or acquired.

-What information are you relying upon.

**Factor 4**

Evaluate the extent to which the risk to the PHI has been mitigated. Consider:

-Were satisfactory assurances obtained that PHI will not be further used or disclosed

-Are the satisfactory assurances written.

**Document Decision:**