Title:	Breach Incident Response and Notification Procedure	Page 1 of 6

Department:	Organization-Wide Procedure	Procedure #EC-011
Reference Policy:	Privacy & Security Breaches and Other Violations Policy	Reference Policy #01-2027
Approved By:	Consortium Executive Team	Effective Date: 8/17/2018
Policy Owner:	Privacy Officer	Last Reviewed: 2/16/2023

1. Purpose:

To ensure incidents of impermissible or unauthorized access, acquisition, use, or disclosure of patient protected health information (PHI) are reported, investigated, and assessed as possible breaches, and that all required notices for breaches of unsecured PHI are provided in accordance with applicable law, including the Health Insurance Portability and Accountability Act (HIPAA)'s Breach Notification Rule, 45 CFR §164 Subpart D.

2. Scope:

This procedure applies to the Privacy Officer and any other members of the workforce with responsibilities related to review of or response to a breach of PHI.

3. Definitions:

3.1. For purposes of this procedure, these terms have the following definitions.

3.1.1. Affected Individual: an individual whose unsecured PHI has been, or is reasonably believed by ANTHC to have been, accessed, acquired, used, or disclosed as a result of such breach.

4. Procedure:

4.1. Discovery of a Breach. Following a report or other discovery of a potential breach incident, the Privacy Officer is responsible for ensuring appropriate response. A breach has been discovered by Alaska Native Tribal Health Consortium (ANTHC):

4.1.1. on the first day on which the breach is known to have occurred or should have been known to have occurred by any member of the workforce, aside from the member who committed the breach; or

4.1.2. upon notice by a business associate of a breach.

4.2. Investigation**.** The Privacy Officer is responsible for investigating, or assigning investigation of, incidents of acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule potentially compromising the security or privacy of the PHI.

4.3. Risk Analysis. Where an incident is substantiated, the Privacy Officer must conduct a risk analysis of the incident using the *ANTHC Breach Risk Assessment Tool* (Attachment A) or other comparable analysis.

4.3.1. Presumption of Breach. The incident is presumed to be a breach unless a risk analysis demonstrates low probability the PHI has been compromised based on an assessment of the following factors:

4.3.1.1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

4.3.1.2. the unauthorized person who used the PHI or to whom the disclosure was made;

4.3.1.3. whether the PHI was actually acquired or viewed; and

4.3.1.4. the extent to which the risk to the PHI has been mitigated.

4.3.2. Follow Up Action. The risk analysis must identify required notifications, corrective actions (including sanction of members of the workforce), and mitigation steps.

4.4. Individual Notification Letters. Where required, the Privacy Officer or designee will provide written notice to Affected Individuals.

4.4.1. Content of Notification. Breach notification letters to Affected Individuals will be in plain language and include the following information, to the extent possible:

4.4.1.1. a brief description of what happened, including the date of the breach and the date of discovery of the breach;

4.4.1.2. a description of the types of unsecured PHI involved in the breach, including:

4.4.1.2.1 clinical (diagnosis/conditions; lab results; medication; or other clinical information)

4.4.1.2.2 demographic (address/ZIP code; date of birth; driver's license number; name; social security number; or other demographic information);

4.4.1.2.3 financial (claims information; credit card/bank account numbers; or other financial information); and

4.4.1.2.4 any other types of PHI.

4.4.1.3. steps the Affected Individual should take to protect themselves from potential harm resulting from the breach;

4.4.1.4. a brief description of what ANTHC is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches, including whether ANTHC has taken or will take any of the following types of action:

4.4.1.4.1 adopt encryption technologies;

4.4.1.4.2 change passwords/strengthened password requirements;

4.4.1.4.3 increase a new/updated Security Rule Risk Management Plan;

4.4.1.4.4 implement new technical safeguards;

4.4.1.4.5 implement periodic technical and nontechnical evaluations;

4.4.1.4.6 improve physical security;

4.4.1.4.7 perform a new/updated Security Rule Risk Analysis;

4.4.1.4.8 provide business associates with additional HIPAA training;

4.4.1.4.9 provide individuals with free credit monitoring;

4.4.1.4.10 revise Business Associate Agreements;

4.4.1.4.11 revise policies and procedures;

4.4.1.4.12 sanction workforce members involved;

4.4.1.4.13 take steps to mitigate harm and train or retrain workforce members; or

4.4.1.4.14 any other actions which may have been or may be taken in response to a breach; and

4.4.1.5. a description of how to ask ANTHC questions or learn additional information, including contact information with a toll-free telephone number, an email address, website, or a postal address.

4.4.2. Timing of Notification**.** Breach notification to Affected Individuals will be provided without unreasonable delay and no later than 60 days after discovery of the breach by ANTHC.

4.4.3. Method of Notification**.** Breach notifications to Affected Individuals will be sent by first-class mail to the address on file, with notification provided in multiple mailings, if necessary. Electronic mail (e-mail) may be used to provide notification if requested by the Affected Individual. Special notification requirements for certain types of affected individuals or in certain situations are set forth in the subsections below.

4.4.3.1. Minors. If an Affected Individual is a minor, breach notification will be provided to the minor's parent or legal guardian.

4.4.3.2. Deceased. If an Affected Individual is deceased, breach notification will be provided to the personal representative of the estate or, if no personal representative is known, to the next-of-kin of the Affected Individual.

4.4.3.3. Substitute Notice. If ANTHC cannot provide written notice because it has insufficient or out-of-date contact information for an Affected Individual, then ANTHC must provide substitute notice.

4.4.3.3.1 For fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.

4.4.3.3.2 For 10 or more individuals, substitute notice will be in the form of either:

4.4.3.3.2.1. a conspicuous posting for a period of 90 days on the ANTHC home page, or conspicuous notice in major print; or

4.4.3.3.2.2. broadcast media in geographic areas where the affected individuals likely reside; and

4.4.3.3.2.3. will include a toll-free phone number that remains active for at least 90 days where an Affected Individual can learn if his or her unsecured PHI may be included in the breach.

4.4.3.4. Urgent Situations. In cases deemed by ANTHC to require urgent notice because of possible imminent misuse of unsecured PHI, ANTHC may provide information to Affected Individuals by telephone or other means in addition to the required written notice.

4.5. Notification to the Media. For a breach of unsecured PHI involving more than 500 individuals, ANTHC will notify prominent media outlets serving the state without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. Such notice will include the same type of content as Affected Individual's notice.

4.6. Notification to the Secretary. Where a notice to an Affected Individual is required, ANTHC will also provide notice to the Secretary of Health and Human Services (HHS) in the manner specified on the HHS Web site, and as follows:

4.6.1. For breaches involving 500 or more individuals, ANTHC will provide notification to the Secretary at the time of notice to Affected Individuals; and

4.6.2. For breaches involving less than 500 individuals, ANTHC will maintain a breach log and will provide notification to the Secretary before March 1 of each year for breaches discovered during the preceding calendar year.

4.7. Tribal Health Organization Notification. ANTHC will notify any tribal health organization which is a participating organization in the Shared Domain of any breach within the Cerner electronic health record affecting the tribal health organization in accordance with the Shared Domain Rules of Behavior, which provides that where a breach of unsecured PHI (under HIPAA) or a breach of the security of the system (under Alaska law) may have occurred involving Technology and Services, the EHR, and/or the Shared Domain impacts multiple Participating Organizations. Each affected Participating Organization and ANTHC shall cooperate and coordinate with each other in providing any notifications of a breach of unsecured PHI or breach of the security of the system to Individuals, the media, and HHS so appropriate notification is provided and duplicative notifications are not issued.

4.8. Law Enforcement Delay. If a law enforcement official notifies ANTHC a breach notification, notice, or posting would impede a criminal investigation or damage national security, ANTHC will delay such notification, notice, or posting for the time period specified by the official in writing. If the statement is made orally, ANTHC will document the statement and the identity of the official and will delay the notification, notice, or posting temporarily (no longer than 30 days from the date of the oral statement unless subsequently directed otherwise in writing.)

4.9. Documentation. The Privacy Officer will document notice and the risk analysis in the Ethics and Compliance Services record keeping system.

Attachments:

1) ANTHC Breach Risk Assessment Tool

ANTHC Breach Risk Assessment Tool

All alleged incidents of impermissible use or disclosure of PHI must be investigated. Where an incident is substantiated, this ANTHC Breach Risk Assessment Tool is used to determine if the incident constitutes a breach under the HIPAA Breach Notification Rule, 45 CFR § 164.400-414.

Incident Description

ComplyTrack/Quantros Reference Numbers: ###

Date of Discovery of the Incident: Date.

Involved Person(s):
Name, Job Title, Department

Description of Incident of Impermissible Use or Disclosure of PHI (including dates):
Provide a detailed explanation of the incident, including any.

What type of PHI was involved?
Describe type of identifiers, number of records, etc.

Was the PHI unsecured? Yes/No
If, "yes" then continue to next question.
If, "no", then breach notification is not required. Document how the PHI was rendered unusable, unreadable, indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary.

Was the impermissible use or disclosure limited to a workforce member of a covered entity whose access or use was unintentional? Yes/No
If, "no" then continue to next question.
If, "yes", then breach notification is not required. Document the basis for this answer.

Risk Assessment Questions

A substantiated incident is presumed to be a breach, unless ANTHC demonstrates a low probability that the PHI has been compromised based on the following factors:

a. **Does the nature and extent of the PHI involved support a low probability of compromise?** [Yes No], based on the following considerations:
   - The types of identifiers involved [included] [did not include] direct identifiers. The likelihood of re-identification of the patient based on the types of identifiers involved and in the context of the incident as a whole is [high, medium, low].
   - The likelihood that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests is [high, medium, low].