Title:	Privacy & Security Breaches and Other Violations Policy	Page 1 of 5

Department:	Organization-Wide Policy	Policy #01-2027
Approved By:	Board of Directors	Effective Date: 4/24/2015
Policy Owner:	Information Systems Security Officer (ISSO) and Privacy Officer	Last Reviewed: 2/16/2023

1. Purpose:

1.1. To comply with Alaska Native Tribal Health Consortium (ANTHC)' s privacy and security policies and procedures, and to clarify the responsibilities of workforce members under ANTHC's direct control for monitoring, reporting, and addressing:

1.1.1. breaches;

1.1.2. other unauthorized uses or disclosures of Protected Health Information (PHI); and

1.1.3. other violations or actions that fail to comply with applicable law, policy, procedure, standard, guidance, or instruction regarding such information.

2. Scope:

This policy applies to all organizational units designated under ANTHC's Health Insurance Privacy and Accountability Act of 1996 (HIPAA) and Privacy Policy and members of their workforce under ANTHC's direct control.

3. Definitions:

3.1. Breach: the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the HIPAA Privacy Standards that compromises the security or privacy of the PHI. Breach excludes:

3.1.1. an unintentional acquisition, access, or use by a workforce member under direct control or a business associate if it was made in good faith and within the scope of authority, and the acquisition, access, or use does not result in any other impermissible use or disclosure;

3.1.2. an inadvertent use or disclosure of unsecured PHI by an authorized workforce member under direct control or business associate to another authorized recipient within ANTHC, the business associate, or any organized health care arrangement to which ANTHC belongs;

3.1.3. a disclosure where ANTHC or its business associate has a good faith belief that the unauthorized recipient cannot retain the information; or

3.1.4. an impermissible access, acquisition, use, or disclosure where there is a low probability following the completion of a HIPAA compliant risk assessment that the unsecured PHI has been compromised.

3.2. Members Under Direct Control: employees, volunteers, trainees, and other persons who report directly to ANTHC rather than a contractor when performing work on or for ANTHC, whether or not they are paid for by ANTHC.

3.3. Unsecured Protected Health Information (PHI): PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through use of technology or methodology.

3.4. All other terms of art used under this policy, such as PHI, personal information, use, disclosure, confidentiality, integrity, security, and privacy will be defined as defined under HIPAA, Health Information Technology for Economic and Clinical Health (HITECH), the Privacy Act, and other applicable law.

4. Policy:

4.1. ANTHC's Commitment to Privacy and Security. Maintaining the privacy and security of sensitive information, especially PHI, is critically important to ANTHC. In adherence with this commitment, ANTHC expects all workforce members under direct control to comply with the policies and procedures it establishes, as well as all applicable security and privacy laws, statutes, and regulations, including HIPAA, HITECH, and applicable provisions of the Privacy Act of 1974, and their implementing regulations.

4.1.1. This policy is intended to supplement, and not supplant, other more restrictive or prohibitive requirements that may apply, including those identified in Alaska Native Medical Center (ANMC) policies and procedures. Under direct control, members should meet the most stringent requirements and standards applicable to their activities, unless otherwise specifically directed by ANTHC's Information Systems Security Officer (ISSO) or Privacy Officer.

4.2. ANTHC's Duty to Assess and Correct. ANTHC will investigate and take corrective action for all alleged violations of this policy. Corrective action against workforce members under direct control will be taken in compliance with ANTHC human resources policies or, as applicable, a governing contract and will reflect whether the breach or violation resulted from careless, reckless, or intentional behavior; if there is a prior pattern or practice of noncompliance with HIPAA or other ethics and compliance standards; and other relevant factors.

4.3. ANTHC'S Duty of Breach Notification. When there is a substantiated breach of unsecured PHI as defined by and in accordance with applicable law, ANTHC will notify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, used, or disclosed in a manner that violates applicable law. If required by applicable law, ANTHC will also provide further notice to the United States Department of Health and Human Services and the media.

4.4. Roles and Responsibilities.

4.4.1. Managers and supervisors are responsible for:

4.4.1.1. ensuring that they and each of their direct reports receive adequate training in applicable privacy, security, and breach notification requirements, including ANTHC policies, procedures, standards, guidance, and instructions;

4.4.1.2. review the activities of their staff and support compliance with the privacy, security, and breach notification standards of ANTHC, including that of ANMC;

4.4.1.3. reporting issues that recur or are prevalent to the ISSO and/or Privacy Officer; and

4.4.1.4. working cooperatively with the ISSO, Privacy Officer, and others to prevent, detect, and address breaches, violations, and other concerns involving information privacy and security.

4.4.2. Workforce members under the direct control of ANTHC are responsible for:

4.4.2.1. learning and complying with applicable privacy and security requirements and standards and using good privacy

and security practices as they relate to their job responsibilities, especially with respect to the rules of behavior concerning PHI and electronic Protected Health Information (ePHI), through education and training offered by ANTHC;

4.4.2.2. reviewing their own activities and assisting their co-workers in their own efforts;

4.4.2.3. detecting, tracking, and reporting potential privacy and security breaches to their supervisor, the ISSO, and/or the Privacy Officer;

4.4.2.4. working cooperatively with the ISSO, Privacy Officer, and others to address breaches, any other unauthorized uses or disclosures of PHI, or a violation of patient rights provided under ANMC's Notice of Privacy Practices; and

4.4.2.5. seeking clarification and assistance if they do not understand what is expected of them, if standards or requirements appear to conflict, or if compliance with identified standards and requirements seems unduly burdensome.

4.4.3. The ISSO and Privacy Officer are responsible for:

4.4.3.1. developing, in cooperation with ANTHC leadership, policies, procedures, standards, guidelines, and instructions necessary to implement this policy;

4.4.3.2. educating managers, supervisors, and other workforce members under direct control on applicable requirements and standards and good practices;

4.4.3.3. coordinating with each other and other appropriate individuals to investigate and respond to potential breaches and other violations, including the development of corrective action plans; and

4.4.3.4. taking other necessary steps to implement this policy.

4.5. Exceptions/Violations/Enforcement. The President/CEO has authority to delegate exceptions to this policy to the ISSO, Privacy Officer, or other identified members of the workforce.