



Participation Guide

[External HIE Participant Privacy, Security and Compliance Policy](#)

[Participant Compliance with Law and Policy Procedure](#)

[Notice of Privacy Practices Procedure](#)

[Opt-Out Information Procedure](#)

[Access To and Use and Disclosure of Information Procedure](#)

[Information Subject to Special Protection Procedure](#)

[Minimum Necessary Procedure](#)

[Participant Workforce, Agents and Contractors Procedure](#)

[Amendment and Storage of Data Procedure](#)

[Requests for Restrictions Procedure](#)

[Mitigation Procedure](#)

[Investigations; Incident Response System Procedure](#)

[Authorized User Controls Procedure](#)

[Sanctions Procedure](#)

4.200 External HIE Participant Privacy, Security and Compliance Policy

Policy Summary

To meet the requirements of HIPAA and State law, healthConnect Alaska has adopted this policy: (1) to govern the use and disclosure of PHI in the Health Information Exchange (HIE); and (2) to further describe the appropriate uses of Direct Secure Messaging. This document establishes, in accordance with applicable law, healthConnect Alaska's policy for ethical and compliant behavior in regard to the privacy and security of Protected Health Information (PHI), Personal Information, and other records protected by applicable state and federal confidentiality laws and contained in the HIE. The policy is divided into Privacy, Security and Breach Notification elements, each of which are further carried out by the procedures found at 4.201 et seq.

Purpose

This policy reflects healthConnect Alaska's commitment to appropriately use and physically protect protected health information (PHI).

Scope/Applicability

The following procedures apply to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and appropriate use of other data exchange services being made available to Participants in healthConnect Alaska, such as Direct Secure Messaging (the HIE and other services are collectively referred to as the "System"). If there is any conflict between this Policy and the Participation Agreement, the Participation Agreement shall control. The procedures found at 4.201 et seq. will specify if they pertain solely to HIE, Direct Secure Messaging or both activities. Here is a table indicating the applicability of the procedures to HIE and DSM, as well as the corresponding provision of the Participation Agreement, if any:

Procedure	Sections Applicable to HIE	Sections Applicable to DSM	Corresponding Participation Agreement (PA) or HIE/DSM Addendum (HD) Section(s)
4.201 Participant Compliance with Law and Policy	All	All	PA II.B.2 PA II.H.1 HD IV.A
4.202 Notice of Privacy Practices	All	None	HD VI.G

4.203 Opt-Out Information Procedure	All	None	HD VI.G
4.204 Access to and Use and Disclosure of Information	All	1, 2, 4, 5, 6, 8, 10	HD III HD IV.B
4.205 Information Subject to Special Protection Procedure	All	None	HD IV.D
4.206 Minimum Necessary	1, 2, 4-7	1, 3-7	
4.207 Participant Workforce, Agents and Contractors	All	All	HD IV.C
4.208 Amendment and Storage of Data	All	3-4	HD V.G
4.209 Requests for Restrictions	All	All	
4.210 Mitigation	All	All	
4.211 Investigations; Incident Response System	All	All	PA II.B.3 HD VI.E
4.212 Authorized User Controls	All	All	HD V.D
4.213 Sanctions	All	All	

Regulatory Category, Type, Legal Regulatory Reference

45 CFR §164 (Security Rule, Breach Notification Rule & Privacy Rule); AS 18.23.300 et seq.; 7 AAC 166.010 et seq.

Policy Authority/Enforcement

HealtheConnect Alaska’s Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of the Participant Privacy, Security and Compliance Policy and related Procedures.

Related Policies & Procedures

- Security Rule - Internal Security Policies and Procedures found at 2.100 through 2.408
- Breach Notification Rule - 2.600 Breach Notification Policy; 2.601 Breach Notification Procedure
- Privacy Rule - Internal Privacy Policies and Procedures found at 3.100 through 3.101
- Privacy, Security, Breach Notification and General Compliance for HIE Participants - External HIE Privacy, Security and Compliance Procedures found at 4.201 through 4.213

Renewal/Review

This policy is to be reviewed annually to determine if the policy complies with current Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security regulations and to ensure that it incorporates all recent developments in healthConnect Alaska policies, procedures, activities, equipment and technology. In the event that significant related legal, regulatory or organizational changes occur, the policy will be reviewed and updated as needed.

Policy

I. Privacy Policy.

A. The guiding healthConnect Alaska privacy principles are applied by healthConnect Alaska through its internal Privacy and Security Policies, as well as its Privacy and Security Plan. These principles are as follows, and should be applied by Participants in their use of healthConnect Alaska information systems, including HIE and DSM :

1. Openness and Transparency.
2. Purpose Specification and Minimization.
3. Disclosure Limitation.
4. Access and Use Limitation.
5. Individual Participation and Control.
6. Data Integrity and Quality.
7. Security Safeguards and Controls.
8. Accountability and Oversight.
9. Remedies.
10. Reliance on Covered Entity Rules and Enforcement.

B. Qualifying Uses of Information. HealthConnect Alaska and Participants have placed the burden on the requesting Participant to utilize PHI from another Participant's records only for a qualifying use by the requesting Participant. A qualifying use is one that meets the terms of the Participation Agreement and applicable State and Federal law.

C. Mitigation of Inadvertent Disclosures of PHI

Participants must report any improper use or disclosure of PHI utilizing healthConnect Alaska information systems of which they become aware to in accordance with the procedures enacted under this Policy. The Participant shall work with healthConnect Alaska to determine the reasonable and appropriate steps that can be taken which may mitigate any resulting harm.

D. Sanctions for Violations of PHI Privacy

All Participants shall enact a policy for imposing sanctions for using or disclosing PHI in violation of this Policy and the underlying Procedures, in accordance with Procedure 4.213, "Sanctions".

E. Documentation

Participants shall maintain copies of HIPAA compliance documents relevant to their participation in healthConnect Alaska for a period of at least six (6) years from the date the documents were created or were last in effect, whichever is later.

F. Complying with Individual Rights

HIPAA provides patients with individual rights that shall be recognized and enforced by healthConnect Alaska whenever possible, and Participants shall assist patients in exercising these rights in accordance with the procedures enacted hereunder. The following rights shall be recognized in accordance with such procedures:

- A. Access
- B. Amendment
- C. Accounting of Disclosures of PHI
- D. Confidential Communications
- E. Requests for Restrictions on Uses and Disclosures of PHI

II. Security Policy

1. Compliance. HealthConnect Alaska is committed to running the HIE in compliance with all applicable laws, regulations and healthConnect Alaska policies/procedures. HealthConnect Alaska has adopted this policy in part to provide for the security of EPHI in accordance with the federal HIPAA Security Regulations and State law. This policy and the procedures enacted hereunder encompass healthConnect Alaska's general approach to compliance with HIPAA Security Regulations and State law through policy statements and procedures in the following categories:
 - a. Administrative Safeguards,
 - b. Physical Safeguards, and
 - c. Technical Safeguards.
2. Administrative Safeguards. The security management process is designed to prevent, detect, contain, and correct security violations relative to healthConnect Alaska information systems. The execution, development and implementation of remediation programs is the joint responsibility of healthConnect Alaska and the Participants.
 - a. Participants are expected to cooperate fully with any risk assessment being conducted by healthConnect Alaska.
 - b. Audit procedures will be implemented and maintained to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. These reviews will be used to determine if Participants are complying with the requirements of this policy and the related procedures.

- c. Participants will assist in making sure access to healthConnect Alaska information systems is assigned and managed appropriate to the duties and responsibilities of each authorized user, and that authorized users are properly trained on the applicable laws, policies and procedures.
- 3. Physical Safeguards. Physical Safeguards are to be made in order to protect healthConnect Alaska information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion. Procedures will be implemented that limit physical access to electronic information systems and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed. Participants should ensure that similar safeguards are in place to protect access points to healthConnect Alaska information systems owned by or housed with Participants.
- 4. Technical Safeguards. Technical Safeguards shall be maintained by each Participant that protect healthConnect Alaska information systems and control access to assure that such systems are accessed only by those individuals or software programs that have been granted access rights. Participants will implement technical security measures to guard against unauthorized access to or modification of EPHI that is being transmitted to or from healthConnect Alaska information systems.

III. Breach Notification Policy. HealthConnect Alaska has implemented internal policies and procedures to address breaches, including breach notification and mitigation measures. Participants are expected to assist with the breach notification process as it applies to their organization, and to follow related procedures enacted under this policy.

4.200 External HIE Privacy, Security and Compliance Policy		
APPROVED BY: healthConnect Alaska Board	ADOPTED:	02/20/2013 v1
	REVISED:	05/31/2013 v2
	REVISED:	06/18/2014 v3
	REVIEWED:	03/08/2015 v3
	REVIEWED:	03/16/2016 v3
	REVIEWED:	07/19/2017 v3
Name change from AeHN to healthConnect Alaska	REVISED:	09/21/2018 v3.1

4.201 Participant Compliance with Law and Policy Procedure

Procedure Summary

This procedure requires Participants to comply with the laws, regulations and policies that apply to the activities of the HIE.

Purpose

This procedure is to ensure that all Participants are using the HIE and other data exchange services in an appropriate and lawful manner, which will help to build trust in the System and among other Participants.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This applies to all Participants, both HIE and DSM.

Regulatory Category, Type, Legal Regulatory Reference

All State and Federal laws pertaining to privacy and security of health information, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and AS 18.23.300 et seq.

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 4.200 External HIE Privacy, Security and Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Laws. Each Participant must, at all times, comply with all federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of protected health information and establishing certain individual privacy rights. Each Participant must use reasonable efforts to stay up-to-date of any changes or updates to and interpretations of such laws and regulations to ensure compliance.
- II. External HIE Privacy, Security and Compliance Policy. Each Participant shall, at all times, comply with the healthConnect Alaska External HIE Privacy, Security and Compliance Policy and related procedures found at 4.200 et seq. (the policy and procedures are referred to collectively in this procedure as the "External HIE Privacy, Security and Compliance Policy"). The External HIE Privacy, Security and Compliance Policy may be changed and updated from time to time upon reasonable written notice to Participants.
- III. Amendment. Amendment to the policy shall be effective when adopted by the healthConnect Alaska Board of Directors, ordinarily following input by the healthConnect Alaska Privacy, Security and Compliance Workgroup and any other relevant workgroups. Amendment to the procedures shall be effective when adopted by the healthConnect Alaska Executive Director, following input by relevant workgroups. healthConnect Alaska shall notify Participants of all rule changes and shall post the most current version of the External HIE Privacy, Security and Compliance Policy on its website.
- IV. Compliance. Each Participant is responsible for ensuring it has, and is in compliance with, the applicable portions of the most recent version of the External HIE Privacy, Security and Compliance Policy.
- V. Participant's Internal Policies. Each Participant is responsible for establishing internal policies that are necessary to comply with applicable laws and the applicable portions of the External HIE Privacy, Security and Compliance Policy. If a Participant is accessing the HIE, as stated in the Participant Agreement, healthConnect Alaska may request a copy of the Participant's policies for its review and reference.
- VI. Participant Criteria. Each Participant shall itself be a HIPAA "covered entity", "business associate" or otherwise subject to HIPAA and its contractually assumed obligations under its Participant Agreement. Each Participant must agree to be a data provider in order to become a data user and full Participant, if the Participant is reasonably capable of providing data. This ensures maximum participation and available information.
- VII. User Criteria. Authorized users are individuals who have been granted access authority. Each authorized user derives his or her permission to access and use the System from a Participant pursuant to 4.212 Authorized User Controls Procedure. Therefore each authorized user must maintain a current relationship to a Participant in order to use the System. Authorized users must be: (i) Participants (for example, an individual physician) or workforce of a Participant, (ii) an

individual Business Association (BA) or workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or workforce of such contractor or subcontractor. The Participants acknowledge the need to revise Rules and certain other technical and administrative features to conform to HIPAA, HITECH, AS 18.23.300 and regulations to be promulgated thereunder. These changes will be made as necessary.

- VIII. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.
- IX. Participant Agreement Controls. If anything in these Rules shall conflict with the Participant Agreement (either HIE or DSM), the terms of the Participant Agreement shall control.
- X. Use of System Equipment, Programs and Information. Participants shall not use any equipment, programs or information associated with the System, whether supplied by healthConnect Alaska, a Participant or a third-party, to interfere in any way with the operation of the System.

4.201 PARTICIPANT COMPLIANCE WITH LAW AND POLICY PROCEDURE		
APPROVED BY: healthConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healthConnect Alaska	REVISED:	11/26/2018 V2.1

4.202 Notice of Privacy Practices Procedure

Procedure Summary

This procedure provides guidance to Participants regarding necessary changes to their Notice of Privacy Practices to indicate that they are now participating in the healthConnect Alaska HIE.

Purpose

This procedure is intended to provide individuals with the reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information and to ensure that individuals are aware when their provider participates in the HIE, so they may exercise their rights under HIPAA with regard to the information provided.

Scope/Applicability

The following rules apply to Participants who are accessing the HIE, and covers the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE").

Regulatory Category, Type, Legal Regulatory Reference

"an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information"

45 CFR §164.520

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 2.100 Consumer Opt-Out Election Policy
- 4.200 External HIE Privacy, Security and Compliance Policy
- 4.203 Individual Control of Information Available Through HIE Procedure

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Revision to Participant Notice of Privacy Practices. Each Participant shall revise its notice of privacy practices (the "Notice") to describe the uses and disclosures of protected health information contemplated through the Participant's participation in the healtheConnect Alaska HIE, if such a use and disclosure is not already addressed in the Notice.
- II. Content. The Notice must meet the content requirements set forth under the HIPAA Privacy Rule and comply with applicable laws and regulations. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through the healtheConnect Alaska HIE. healtheConnect Alaska provides the following sample language for Participants who elect to amend their Notice: "We may make your protected health information available electronically through an electronic health information exchange to other health care providers and health plans that request your information for their treatment and payment purposes. Participation in an electronic health information exchange also lets us see their information about you for our treatment and payment and healthcare operation purposes. You are permitted to request and review documentation regarding who has accessed your information through the electronic health information exchange. Your provider will have information on how to make this request, or you may find the information at www.healthconnectak.org." Participants may elect more stringent language, but may not commit healtheConnect Alaska to any additional obligations or liabilities through the Notice. healtheConnect Alaska reserves the right to review the language developed and request changes through a mutual collaboration of the parties, as necessary.
- III. Dissemination and Individual Awareness. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgment of receipt by the individual. Those policies and procedures shall comply with applicable laws and regulations. The Notice is part of a larger effort by Participants to make individuals aware of their options for participating in the healtheConnect Alaska HIE. More information about this is available in 4.203 Opt-Out Information Procedure.
- IV. Participant Choice. Participants may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice, so long as any expanded detail does not misstate the safeguards supporting the healtheConnect Alaska HIE. 45 C.F.R. § 164.520(b). See 45 C.F.R. § 164.520(c)(2)(ii).

4.202 NOTICE OF PRIVACY PRACTICES PROCEDURE

APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healtheConnect Alaska	REVISED:	11/26/2018 V2.1

4.203 Opt-Out Information Procedure

Procedure Summary

This procedure provides the guidelines for an individual to opt-out, either completely or partially from the healthConnect Alaska HIE.

Purpose

This procedure is intended to provide individuals with the reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information, and to opt-out of the HIE as permitted under Alaska law.

Scope/Applicability

The following procedure applies to Participants who are accessing the HIE, and the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE").

The opt-out procedure does not apply to Direct Secure Messaging (DSM).

Regulatory Category, Type, Legal Regulatory Reference

AS 18.23.310

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 2.100 Consumer Opt-Out Election Policy
- 2.101 Consumer Opt-Out Election Procedure
- 4.200 External HIE Privacy, Security & Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Definitions

Opt-in – All patients are initially considered opt-in under Alaska law. If an individual has previously opted-out and chooses to opt-in to the healthConnect Alaska HIE, their protected health

information will be available through the HIE from the date upon which the opt-in is processed. Information about the individual created by a provider prior to the opt-in will not be available through healthConnect Alaska.

Opt-out - If an individual chooses to opt-out of the healthConnect Alaska HIE, protected health information will not be shared or visible through the HIE, with the exception of limited demographic information necessary to make sure that no health information is added to the healthConnect Alaska HIE in the future. Limited information that is required to be reported by healthcare providers under the law will continue to be directly transmitted to the required recipient in accordance with mandatory reporting laws.

Partial Opt-out - If an individual chooses partial opt-out, protected health information is stored in an encrypted file and will only be accessed in an emergency, such as an emergency room visit. The emergency doctor will be given a decryption key to view the data and will be required to answer a question about why the record is being accessed. This information is stored with the health record and the individual can request the information regarding access by contacting healthConnect Alaska.

Procedure

- I. Choice Whether to Have Information Included in the healthConnect Alaska HIE. All individuals will have the opportunity to opt out of participating in healthConnect Alaska. A request to opt out will be treated as a request for restrictions on use and disclosure of protected health information. Participants agree to approve such requests, subject to qualifications and limitations as described below or in these policies.
 - A. Individuals shall be afforded the opportunity to exercise this choice at the time of any service at a Participant that is a health care provider, or thereafter through a uniform "opt-out" process.
 - B. healthConnect Alaska will, from time to time, furnish Participants that are health care providers with a sample informational brochure about the healthConnect Alaska HIE for use in explaining the meaning and effect of participation or opting out. Participants may customize the informational brochure as they deem appropriate to fit their circumstances, so long as healthConnect Alaska does not incur any additional obligations or liabilities as a result. Modified brochures should contain a link to the healthConnect Alaska website where healthConnect Alaska will provide an explanation of the meaning and effect of participation or opting out and a tool for opting out or revoking a prior opt-out election. The healthConnect Alaska website will include information about the current participating entities, and the types and format of information that participants can obtain through the HIE.
 - C. Participants may provide opt-out information through the Participant's Notice of Privacy Practice, brochure, or other mechanism as appropriate to the Participant workflow. Notification should include:
 - a. An explanation of the healthConnect Alaska HIE-wide scope of an opt-out or partial opt-out decision, the risks to the individual's data privacy and security if the individual participates including a list of the ways in which information may be used, the effect and benefits of participation, and the effect and disadvantages of opting out.

- b. Information that the Participant (and other Participants) will not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her included in the healthConnect Alaska HIE.
- D. Participants shall furnish information regarding the HIE and the opt-in/out options to individuals at the initiation of an episode of care, as determined by the Participant. Participants shall also provide for each individual the opportunity to opt-out or ask questions. Each Participant will have one or more persons designated to answer questions about the healthConnect Alaska HIE or about opting out or revoking a prior opt-out election.
- E. Participants may also direct individuals to the healthConnect Alaska website and to healthConnect Alaska, where the individual can ask additional questions and obtain additional information about participation in healthConnect Alaska and opt-out options. The healthConnect Alaska website will have opt-out and opt-in forms available in the form attached hereto as Appendix A and Appendix B. healthConnect Alaska as a business associate of the Participants is authorized to provide information and answer individual questions about healthConnect Alaska and the opt-out alternatives on behalf of Participants.
- F. Participants that provide only limited information through the healthConnect Alaska HIE and have limited or no face-to-face contact with individuals shall provide the following information in their patient documentation as they determine necessary: a description of the healthConnect Alaska HIE, an explanation of the right to opt out, a link to the healthConnect Alaska website and a phone number individuals can use to obtain additional information about healthConnect Alaska HIE, insurer access, and the right to opt out. However, all Participants will provide this information if they are the primary provider for an individual. Additionally, all Participants will be listed on the healthConnect Alaska website, regardless of the amount of contact with individuals.
- G. An individual's election to opt out of participation in the healthConnect Alaska HIE shall be communicated to healthConnect Alaska in the manner provided by healthConnect Alaska in 2.101 Consumer Opt-Out Procedure and be in effect once so communicated and processed.
- I. Change to Prior Election. An individual may opt out or revoke a prior election to opt out at a later date. The brochures provided by Participants and information on the healthConnect Alaska website should inform the individual that withdrawing a prior opt-out election will result in information that was previously unavailable through the healthConnect Alaska HIE becoming available to all Participants using the healthConnect Alaska HIE.
- II. Effect of Choice. An individual who completely opts out of the healthConnect Alaska HIE opts out as to all of his or her records made available through the healthConnect Alaska HIE, not just with respect to a particular Participant or episode of care. The effect is system-wide. An individual who opts out of the healthConnect Alaska HIE for regular treatment, but allows access for emergency purposes will have information remain in the healthConnect Alaska HIE, but access is only allowed after certain emergent circumstances

are presented. An individual's election to opt out, whether made at the time of service or subsequently, will have prospective effect only and will not impact access, use and disclosure occurring before the decision is received and communicated through the healthConnect Alaska HIE.

- III. Limited Effect of Opt-Out. A decision to opt out only affects the availability of the individual's protected health information through the healthConnect Alaska HIE. Each Participant's policies continue to govern access, use and disclosure in all other contexts and via all other media.
- IV. Documentation. Each Participant should maintain documentation that information about the healthConnect Alaska HIE and about the ability to opt out of the healthConnect Alaska HIE has been provided to the Participant.
- V. Participant's Choice. Participants shall develop and implement the necessary processes to allow an individual to choose not to have information about him or her included in the healthConnect Alaska HIE. The uniform processes described in this procedure are not exclusive, and Participants may adopt additional, not inconsistent, mechanisms.
- VI. Provision of Coverage or Care. A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice to opt out.
- VII. Reliance. Participants will be entitled to assume that if an individual has not opted-out the individual's protected health information may be available through the healthConnect Alaska HIE.

4.203 OPT-OUT INFORMATION PROCEDURE		
APPROVED BY: healthConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healthConnect Alaska	REVISED:	11/26/2018 V2.1

Appendix A – Opt Out Form

Health Information Exchange Patient Opt-Out Form

You may Opt-In or Opt-Out of health information exchange at any time. Whichever you choose, your selection is confidential. In certain cases such as the reporting of infectious diseases to public health officials, your choice is overridden by law. Whatever your choice, in no circumstances is data provided to anyone other than your provider or your insurer as allowed by law. This is the same reporting that currently occurs with your paper health information by fax or mail. Electronic transfer allows your data to be transferred securely and provides you with an audit of where your data has been sent which paper transfers cannot guarantee.

For more information about the security and benefits of health information exchange see the [healthConnect Alaska](http://www.healthconnectak.org) website at www.healthconnectak.org.

To Opt-Out, please select ONE of the following:

- I WISH to partially **OPT OUT** of healthConnect Alaska, allowing providers to access my health information only in the event of a medical emergency.
- I WISH to completely **OPT OUT** of healthConnect Alaska. I understand that by making this selection, **NONE** of my healthcare providers will be able to access my health information maintained at healthConnect Alaska, even in a medical emergency;

I hereby acknowledge and agree as follows. I understand that:

1. My providers **will continue to have access** to my information, but only in the electronic medical record that was created for me by my provider; my provider will not be able to access another record from a different provider I have seen.
2. Any information that is disclosed before I submit this Alaska HIE Opt-Out form cannot be taken back and will remain with my provider if he/she accessed such information before this Opt-Out went into effect.
3. My Primary Provider will receive a copy of my Opt-Out choice from healthConnect Alaska.
4. Once this Opt-Out goes into effect, I can change my decision **only by** submitting an Opt-In form to healthConnect Alaska.
5. This request, and any future request to Opt-In, can take up to 3 business days after receipt to take effect.
6. If the information on this form changes, I must notify both healthConnect Alaska and my primary care provider. If I provide information to a provider that does not match this form, that information may not be opted-out of the health information exchange.

If I have questions regarding Opt-In and Opt-Out, I understand I can contact healthConnect Alaska directly at 866-966-9030, ext 1.

Please Type or Print Clearly. *Denotes required fields. Forms cannot be processed without the required information.

*Patient Name (Last):	* (First):	(MI):	
Previous Names or Nicknames:	*Patient Date of Birth (mm/dd/yyyy):	*Primary Telephone Number: () -	
Email:	*Sex (M/F):	Secondary Telephone Number: () -	
*Address (Mailing):	* (City):	* (State):	* (Zip):
*Primary Provider Name:	Facility:	Medical Record Number (MRN):	

*Signature of Patient

*Date Signed

*Signature of Facility Staff Member
(please complete Facility and MRN)

Notary: (Form must be notarized if not witnessed by provider, clinic or hospital)

STATE OF _____

The foregoing signature was acknowledged before me this ____ day of _____ as an authorized, free and voluntary act. IN WITNESS WHEREOF, I have hereunto set my hand and seal.

By: _____)

Notary Public for: _____)ss

My Commission Expires: _____)

ite 203,
K 99537

2/03/2016 v5

Appendix B – Opt In Form



Health Information Exchange
Patient Opt-In Form

I previously submitted a request to **Opt-Out** of the healtheConnect Alaska system and am now requesting my health information be made electronically accessible to authorized health care providers.

I understand that any health information about me prior to processing of this **Opt-In** notice will not be accessible to me or any provider.

For more information about the security and benefits of the HIE, please see the healtheConnect Alaska website at www.healthconnectak.org.

A separate form must be filled out for each family member requesting to **Opt-In** if **Opt-Out** was previously selected.

If this form is signed by someone other than the person named below, the person signing the form hereby certifies that he/she is acting as:

(CHECK ONE) Parent Legal Guardian Other (Specify Relationship) _____ for the person named below.

Contact information for individual completing this form if other than patient (please print clearly)*

*I have had an opportunity to ask and receive answers to all my questions about **Opt-In** participation.*

Please Type or Print Clearly. * Denotes required fields.

*Patient Name (Last):	* (First):	(MI):	
Previous Names or Nicknames:	*Patient Date of Birth (mm/dd/yyyy):	*Primary Telephone Number: () -	
Email:	*Sex (M/F):	Secondary Telephone Number: () -	
*Address (Mailing):	* (City):	* (State):	* (Zip):
*Primary Provider Name:	Facility:	Medical Record Number (MRN):	

Signature of Patient

Date Signed

Notary: (Form must be notarized if not submitted via provider, clinic or hospital.)	
STATE OF _____; _____ JUDICIAL DISTRICT or _____ COUNTY	
The foregoing signature was acknowledged before me this _____ day of _____, by _____, the _____ of _____, as the authorized, free and voluntary act of said organization. IN WITNESS WHEREOF, I have hereunto set my hand and seal.	
_____)	
Notary Public for: _____)ss	
My Commission Expires: _____)	

Submit form by: fax to: 866-966-9030; or mail to: healtheConnect Alaska, 4000 Old Seward Hwy Suite 203, Anchorage, AK 99503

4.204 Access to and Use and Disclosure of Information Procedure

Procedure Summary

This procedure requires Participants to access, use and disclose protected health information only in the manner permitted by law, under the appropriate Participant Agreement, and subject to any restrictions to which they have agreed upon with individual patients.

Purpose

This procedure is to ensure that protected health information is only collected, used and/or disclosed to the extent necessary to accomplish a specified purpose and not to discriminate inappropriately.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This procedure generally applies to all Participants, both HIE and DSM, with specific references to each system if a provision applies only to one activity.

Regulatory Category, Type, Legal Regulatory Reference

Privacy Rule, 45 CFR §164.500 et seq.

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 2.212 Access Authorization Procedure
- 2.213 Access Establishment and Modification Procedure
- 2.401 Access Control Procedure
- 2.600 Breach Notification Policy
- 2.601 Breach Notification Procedure
- 4.200 External HIE Privacy, Security and Compliance Policy
- 4.210 Mitigation Procedure

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Compliance with Law – All Users. Participants shall access, use and disclose protected health information through healtheConnect Alaska only in a manner consistent with all applicable federal, state, and local laws and regulations and not for any unlawful or discriminatory purpose. Under AS 18.23.300, this is limited to treatment and billing purposes only.
- II. Documentation and Reliance – All Users. If applicable law requires that certain documentation exist or that other conditions be met prior to disclosing protected health information for a particular purpose (such as consent to release substance abuse information), the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions. Each disclosure of protected health information by a Participant is a representation to every other Participant that all prerequisites under state and federal law for such disclosure by the disclosing Participant have been met. If a Participant is unable to withhold information that requires additional protections, it should not provide any information to the System.
- III. Purposes – HIE Users. A Participant may request and use protected health information through the HIE only for the Participant's treatment and billing purposes or as required by law, and only to the extent necessary and permitted by applicable federal, state, and local laws and regulations and these Rules. A Participant may request and use protected health information through the HIE only if the Participant has or has had or is about to have the requisite relationship to the individual whose protected health information is being accessed and used. The requisite relationships include, but are not limited to, the primary care provider for each patient and other providers in a treatment relationship with the patient. A list of the types of persons who can qualify to have the requisite relationship will be contained on the healtheConnect Alaska website. Prohibitions – HIE Users. Information may not be requested from the HIE for marketing or marketing related purposes. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request or access information through the HIE.
- IV. Participant Rules – All Users. Each Participant shall reference and maintain compliance with its own internal policies and procedures regarding disclosures of protected health information, including the conditions that shall be met and documentation that must be obtained, if any, prior to making such disclosures. In the event that Participant's internal policies and procedures conflict with External HIE Privacy, Security and Compliance

Policy and related procedures, or the relevant Participant Agreement, the provision that provides for greater privacy and security of protected health information shall govern.

- V. Subsequent Use and Disclosure – All Users. A Participant that has accessed information through the System and merged the information into its own record shall treat the merged information as part of its own record and thereafter use and disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own record. A Participant shall not access protected health information through the HIE for the purpose of disclosing that information to third parties, other than for the Participant's qualifying treatment and billing purposes.
- VI. Accounting of Disclosures – All Users. Each Participant shall be responsible to account only for its own disclosures. All requests for an accounting of disclosures received by healthConnect Alaska will be forwarded back to the Participants to address for their respective patients, except that healthConnect Alaska may produce an audit log as described further below.
- VII. Audit Logs – HIE Users. healthConnect Alaska shall develop an audit log capability to document which Participants posted and accessed the information about an individual through the HIE and when such information was posted and accessed.
- VIII. Authentication – All Users. healthConnect Alaska shall follow a uniform authentication requirement for verifying and authenticating the identity and authority of each authorized user and Participant consistent with the National Institute of Standards and Technology Special Publication 800-63 Version 1.0.2. Assurance Level 2 and **2.212 Access Authorization Procedure, 2.213 Access Establishment and Modification Procedure** and **2.401 Access Control Procedure**. healthConnect Alaska will act as the Credentials Service Provider (CSP) in all instances but may delegate CSP responsibilities to participants with system administrators. All Participants are responsible to act as Registration Authorities (RA). Participants shall be entitled to rely on healthConnect Alaska's user access and authorization safeguards and may be assured an authorized user making a request for protected health information on behalf of another Participant is authorized to do so. Participants shall be responsible for their own authorized users and ensuring that their own authorized users are appropriately authorized and accessing information. NIST Requirements for Level 2 Assurance are included in the table at the end of this procedure.
- IX. Access – HIE Users. Each Participant should have a formal process through which it permits individuals to view information about them that has been posted by the Participant to the HIE. For HIPAA Covered Entities, this is currently required by law. Individuals may also contact healthConnect Alaska or check www.healthconnectak.org for ways in which they can access their personal information on the HIE.

- X. Application to BAs and Contractors – All Users. Participants shall make this rule applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

	In- Person	Remote
Basis for Issuing Credentials	Possession of a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport)	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.
RA Actions	<p>Inspects photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then:</p> <p>a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or;</p> <p>b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.</p>	<p>Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. Address confirmation and notification:</p> <p>a) Sends notice to an address of record confirmed in the records check or;</p> <p>b) Issues credentials in a manner that confirms the address of record supplied by the applicant; or</p> <p>c) Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.</p>

4.204 ACCESS TO AND USE AND DISCLOSURE OF INFORMATION PROCEDURE		
APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healtheConnect Alaska	REVISED:	11/12/2018 V2.1

4.205 Information Subject to Special Protection Procedure

Procedure Summary

This procedure requires Participants to only disclose information that can legally be exchanged and is not subject to additional protections under the law. In addition, it explains to Participants the types of information that may be excluded from the records they receive through the System.

Purpose

This procedure is intended to make Participants aware of the restrictions of the system with regard to certain categories of information, and to ensure that Participants restrict the information they provide in accordance with any protections accorded that information under the law.

Scope/Applicability

The following rules apply to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 4.200 External HIE Privacy, Security and Compliance Policy
- 4.204 Access to and Use and Disclosure of Information Procedure

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and other applicable Federal and State law. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Special Protection. The System and these policies are geared to the HIPAA level of privacy, in addition to AS 18.23.300 et seq. Some health information may be subject to special protection under additional federal, state, and/or local laws and regulations. Other health information may be deemed so sensitive that a Participant has made special provisions to safeguard the information, even if not legally required to do so.

Sensitive information falls under two categories: (1) mental health and HIV, which will be separated and require additional security, but not be excluded from the HIE and (2) 42 CFR Part 2, which will be excluded from the HIE, but can still be provided through DSM if the Participant has the proper authorization in place for disclosure. Each Participant shall be responsible to identify what information is legally subject to special protection under applicable law and what information (if any) is subject to special protection under that Participant's policies, prior to disclosing any information through the HIE. Participants should not make protected health information requiring special protection available to the HIE. Each Participant is responsible for complying with laws and regulations and its own policies in regard to identifying and providing special treatment for information needing special protection. healthConnect Alaska has worked with the HIE system provider to filter certain sensitive codes and diagnoses, but this filter cannot be relied upon by Participants to remove all sensitive information. A list of the codes and diagnoses filtered by the HIE system provider is available on the healthConnect Alaska website.

II. Information Not Furnished. For System data to be useful, the Participant using it must know if it is complete or whether certain information would be withheld due to more stringent state and federal law or Participant policies.

A. Accordingly, Participants accessing and using another Participant's information obtained through the System may act with the understanding that the information made available may not include any of the following:

1. Alcohol and substance abuse treatment program records subject to 42 CFR Part 2;
2. Records of emergency protective custody proceedings;
3. HIV testing information;
4. Certain records of minors if under state law only the minor's consent to treatment is needed, the minor has consented to the care, but the minor is not the party electing not to opt out. In Alaska, this may include, but is not limited to the following records:
 - a. Records of STD testing and treatment (including HIV testing);
 - b. Diagnosis and treatment of suspected abuse by a parent, guardian or personal representative; and
 - c. Provision of birth control and other reproductive treatment.
5. Records of mental health treatment centers.

B. This list is suggestive only. Other records may be added to the list. Data recipients are not entitled to rely on records being inclusive of the above listed records.

III. Application to Business Associates and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs through

the terms of their business associate agreements, if those BAs will be accessing the System.

4.205 INFORMATION SUBJECT TO SPECIAL PROTECTION PROCEDURE		
APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healtheConnect Alaska	REVISED:	11/26/2018 V2.1

4.206 Minimum Necessary Procedure

Procedure Summary

This procedure described the restrictions on information requests and the application of the minimum necessary rule with regard to the HIE. Participants are asked to request the minimum necessary information for their intended use.

Purpose

This procedure ensures that the information used and disclosed through the HIE is provided in accordance with HIPAA and that requesting parties only access the minimum amount of information needed for treatment of a patient.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This procedure generally applies to all Participants, both HIE and DSM, with specific references to each system if a provision applies only to one activity.

Regulatory Category, Type, Legal Regulatory Reference

"When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

45 CFR §164.502(b)

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 4.200 External HIE Privacy, Security and Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and other applicable Federal and State law. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Requests – All Users. Each Participant shall request only the minimum amount of health information through the System as is necessary for the intended purpose of the request. However, for some requests made of the HIE, a standard set of information will be received in return for a limited request, due to the technical limitations of the System. When this occurs, Participant will not be deemed to be in violation of this procedure.
- II. Disclosures – HIE Users. A Participant is entitled to rely on the scope of a requesting Participant's request for information as being consistent with the requesting Participant's minimum necessary policy and needs.
- III. Disclosures – DSM Users. A DSM Participant should follow their internal policies and procedures regarding minimum necessary and verification of requests for information to determine if a Participant's request for information through DSM is consistent with HIPAA minimum necessary. This may include verification of whether a treatment relationship exists or is anticipated, verification of the need for the information or independent verification of any other circumstances related to the request. DSM is secure messaging only, and requests received or sent through DSM should be treated as any other request for protected health information.
- IV. Workforce, BAs and Contractors – All Users. Each Participant shall adopt and apply policies to limit access to the System to members of its workforce who qualify as authorized users. Such access shall be made available only to the extent needed by such authorized users to perform their job functions or duties for the Participant.
- V. Entire Medical Record – All Users. A Participant shall not use, disclose, or request an individual's entire medical record unless necessary and justified to accomplish the specific purpose of the use, disclosure, or request.
- VI. Application to Providers and Treatment Purposes – All Users. While this minimum necessary policy is not required by HIPAA for providers accessing, using and disclosing health information for treatment purposes, they are encouraged to follow it when consistent with treatment needs.
- VII. Application to BAs and Contractors – All Users. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs through the terms of their business associate agreements, if those BAs will be provided access to the System.

4.206 MINIMUM NECESSARY PROCEDURE		
APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healtheConnect Alaska	REVISED:	11/26/2018 V2.1

4.207 Participant Workforce, Agents and Contractors Procedure

Procedure Summary

This procedure requires Participants to inform its workforce, agents, contractors and business associates regarding the requirements of Participation and their obligation to comply with the laws, regulations and policies that apply to the activities of the System.

Purpose

This procedure is to ensure that all Participants are using the HIE and other data exchange services in an appropriate and lawful manner, which will help to build trust in the System and among other Participants.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This applies to all Participants, both HIE and DSM.

Regulatory Category, Type, Legal Regulatory Reference

All State and Federal laws pertaining to privacy and security of health information.

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 4.200 External HIE Privacy, Security and Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Participant Responsibility. Each Participant is responsible to establish and enforce policies designed to comply with its responsibilities as a covered entity or business associate under HIPAA and a Participant in the System, and to train and supervise its authorized users on those responsibilities, to the extent applicable to their job responsibilities. Training shall include, but not be limited to, the requirements of these Rules, the Participant Agreement, and applicable law governing the confidentiality, privacy and security of protected health information, such as HIPAA and AS 18.23.300. All such training will be conducted at the sole cost of Participant, prior to any access to the System by authorized users.
- II. healthConnect Alaska Responsibility. healthConnect Alaska will provide general training to Participants regarding the use of the System, which will include information about how HIPAA and AS 18.23.300 apply to the System and Participants' responsibilities to adhere to HIPAA, AS 18.23.300 and other laws and regulations, but this training is not intended to substitute for general training regarding privacy, security and compliance with laws. This training will be provided as part of the onboarding process to key Participant staff members, who will be expected to provide the training to additional users at Participant's organization.
- III. Authorized Users. All authorized users, whether members of a Participant's workforce or member of the workforce of a BA or contractor, shall execute an individual user agreement and acknowledge familiarity with and acceptance of the terms and conditions on which their access authority is granted. This shall include familiarity with applicable privacy and security policies of the Participant, BA, or contractor, as applicable. Participants shall determine to what extent members of their workforce or the workforce of BAs and contractor require additional training on account of the Participant's obligations under their Participant Agreement and these policies, and arrange for and document such training. healthConnect Alaska shall reserve authority in the Participant Agreement to suspend, limit or revoke access authority for any authorized user or Participant for violation of Participant and/or healthConnect Alaska privacy and security policies.
- IV. Access to System. Each Participant shall allow access to the System only by those authorized users who have a legitimate and appropriate need to use the System and/or release or obtain information through the System. No workforce member, agent, or contractor shall have access to the System except as an authorized user on behalf of a Participant and subject to the Participation Agreement, State and Federal laws, Participant's privacy and security policies and procedures, and the terms of the individual's user agreement.
- V. Discipline for Non-Compliance. Each Participant shall have disciplinary policies to hold authorized users, BAs and contractors accountable for following the Participant's policies and procedures and for ensuring that they do not use, disclose, or request health information except as permitted by these Rules. Examples of disciplinary measures include, but are not be limited to, verbal and written warnings, demotion, and termination and may provide for retraining in certain circumstances. Participants and users may also be subject to additional sanctions in accordance with 4.213 Sanctions Procedure.

- VI. Reporting of Non-Compliance. Each Participant shall have a procedure, and shall encourage all workforce members, BAs and contractors to report any noncompliance with the Participant's policies or the policies applicable to authorized users. Each Participant also shall establish a mechanism for individuals whose health information is included in the System to report any non-compliance with these Rules or concerns about improper disclosures of protected health information.
- VII. Enforcing BAAs and Contractor Agreements. Each Participant shall require in any relationship with a BAs, contractor, or other third party (which may include staff physicians) that will result in such third party becoming an authorized user on behalf of the Participant, or that will result in members of the workforce of such third party becoming an authorized user on behalf of the Participant, that: (i) such third party and any member of its workforce shall be subject to these Rules when accessing, using or disclosing information through the System; (ii) that such third parties and/or authorized users on its workforce may have their access suspended or terminated for violation of these Rules or other terms and conditions of the authorized user agreement; and (iii) that such third party may have its contract with the Participant terminated for violation of these Rules or for failure to enforce these policies among its workforce.

4.207 PARTICIPANT WORKFORCE, AGENTS AND CONTRACTORS PROCEDURE		
APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2012 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healtheConnect Alaska	REVISED:	11/26/2018 V2.1

4.208 Amendment and Storage of Data Procedure

Procedure Summary

This procedure requires Participants to accommodate requests for amendment, when it pertains to data that originated in their records. In addition, it provides notice that Participants should not rely on healthConnect Alaska for backup or storage of the information on the system.

Purpose

This procedure is intended to provide direction to Participants regarding the responsibility and ownership of records for amendment purposes. In addition, it provides guidance to Participants to allow them to arrange for alternative backup of the information gained through the System.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This procedure generally applies to all Participants, both HIE and DSM, with specific references to each system if a provision applies only to one activity.

Regulatory Category, Type, Legal Regulatory Reference

45 CFR §164.526

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 4.200 External HIE Privacy, Security and Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 et seq. and applicable Federal and State law. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Accepting Amendments – HIE Users. Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information. Only the Participant responsible for the record being amended may accept an amendment. If one Participant believes there is an error in the record of another Participant, it shall contact the responsible Participant or healthConnect Alaska to follow up on the error.

- II. Informing Other Participants – HIE Users. A Participant shall update an individual’s record in the HIE using a method established by healthConnect Alaska for such purpose when it has amended an element of the individual’s protected health information that gets transmitted to the HIE. healthConnect Alaska shall cooperate in identifying other Participants who have accessed the information in its pre-amendment form, to the extent reasonably possible. Participants shall also notify healthConnect Alaska of data errors reported to it by patients or providers that cannot be lawfully amended through the automated transmission of an update or amendment from the Participant’s electronic system.

- III. Application to BAs and Contractors – All Users. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs through the terms of their business associate agreements, if the BA will have access to the System.

- IV. Data Backup – All Users. Participants shall not hold healthConnect Alaska responsible for protecting and backing up the source data used in connection with or furnished for processing by the System, unless expressly agreed upon pursuant to the Participant Agreement. healthConnect Alaska will perform backups as required to comply with HIPAA and its obligations to Participants, but Participants should not rely upon this backup for its own data. Participants can contact healthConnect Alaska to obtain more information about how to properly backup their own records.

4.208 AMENDMENT AND STORAGE OF DATA PROCEDURE		
APPROVED BY: healthConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/04/2015 V2
	REVIEWED:	03/16/2016 V2
Name change from AeHN to healthConnect Alaska	REVIEWED:	07/19/2017 V2
	REVISED:	11/26/2018 V2.1

4.209 Requests for Restrictions Procedure

Procedure Summary

This procedure provides guidance for Participants regarding restrictions requested by individuals on the use and disclosure of their records.

Purpose

This procedure is intended to clarify the roles of the Participants with regard to request for restrictions.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This procedure generally applies to all Participants, both HIE and DSM, with specific references to each system if a provision applies only to one activity.

Regulatory Category, Type, Legal Regulatory Reference

45 CFR §164.522

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 4.200 External HIE Privacy, Security and Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300, and other applicable Federal and State law. In the event that significant related legal, regulatory and technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Recipient Responsibility. A Participant, when accessing data as a data recipient, shall not be expected to know of or comply with a restriction on use or disclosure agreed to by a Participant that provides data unless such restriction on use or disclosure is transmitted with the data. This procedure is applicable to requests from an individual for restrictions, as opposed to restrictions imposed by law, which are addressed in 4.205 Information Subject to Special Protection Procedure.

- II. Data Provider Responsibility. If a Participant agrees to an individual's request for restrictions, as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions. This shall include not making the individual's information available to the System, including opting the individual out of the System, if required by the restriction. Participants should advise individuals that opting out only affects access, use and disclosure of their protected health information through the System. Participants should also advise individuals whether the restriction will apply to use of DSM. When evaluating a request for a restriction, the Participant shall consider the implications that agreeing to the restriction would have on the accuracy, integrity and availability of information through the System and on their ability to participate in the System.

4.209 REQUESTS FOR RESTRICTIONS PROCEDURE		
APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/03/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healtheConnect Alaska	REVISED:	11/26/2018 V2.1

4.210 Mitigation Procedure

Procedure Summary

This procedure requires Participants to mitigate the effects of any breach and assist healthConnect Alaska with its mitigation efforts.

Purpose

This procedure is to ensure breaches are properly mitigated, in accordance with breach notification and other requirements of the Security Rule.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This applies to all Participants, both HIE and DSM.

Regulatory Category, Type, Legal Regulatory Reference

45 CFR §164.400 et seq.

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 2.600 Breach Notification Policy
- 2.601 Breach Notification Procedure
- 4.200 External HIE Privacy, Security and Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 and other applicable Federal and State law. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Duty to Mitigate. Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable, the harmful effects that are known to the Participant of an access, use or disclosure of protected health information through the System that is in violation of applicable laws and/or regulations and/or these Rules and that is caused or contributed to by the Participant or its workforce members, agents, and contractors. Steps to mitigate could include, but are not limited to, Participant notification to the individual or Participant request to the party who improperly received such information to return and/or destroy impermissibly disclosed information.

- II. Duty to Cooperate. A Participant that has caused or contributed to a privacy breach related to the System or that could assist with mitigation of the effects of such breach shall cooperate with healtheConnect Alaska in accordance with **2.600 Breach Notification Policy** and **2.601 Breach Notification Procedure**. Participant shall also assist another Participant that has the primary obligation to mitigate a breach in order to help mitigate the harmful effects of the breach. This obligation exists whether the Participant is directly responsible or whether the breach was caused or contributed to by members of the Participant's workforce or by its BAs or contractor or their workforce.

- III. Notification to healtheConnect Alaska. A Participant primarily responsible to mitigate a breach related to the System shall notify healtheConnect Alaska of all events requiring mitigation and of all actions taken to mitigate. healtheConnect Alaska may facilitate the mitigation process if asked. healtheConnect Alaska shall attempt to use examples of breaches and mitigation steps for education and for policy and other safeguard development.

- IV. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs through the terms of their business associate agreements, if the BAs will have access to the System.

4.210 MITIGATION PROCEDURE		
APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/03/2015 V2
	REVIEWED:	03/16/2016 V2
Name change from AeHN to healtheConnect Alaska	REVIEWED:	07/19/2017 V2
	REVISED:	11/26/2018 V2.1

4.211 Investigations; Incident Response System Procedure

Procedure Summary

This procedure requires Participants to investigate and assist in the response and investigation of security incidents and breaches.

Purpose

The purpose of this procedure is to ensure healthConnect Alaska and the Participants act appropriately in response to the discovery or notification of a breach of PHI or PII.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This applies to all Participants, both HIE and DSM.

Regulatory Category, Type, Legal Regulatory Reference

45 CFR 165.400 et seq.; AS 45.48.010 et seq.

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 2.600 Breach Notification Policy
- 2.601 Breach Notification Procedure
- 4.200 External HIE Privacy, Security and Compliance Policy

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Duty to Investigate. Each Participant shall promptly investigate reported or suspected privacy breaches implicating privacy or security safeguards deployed by healthConnect Alaska (or its contractors), or involving unauthorized access, use or disclosure of the System, according to its own policies. Upon learning of a reported or suspected breach related to the System, as defined by HIPAA or the Alaska Personal Information Protection Act, the Participant shall notify healthConnect Alaska and any other Participant whom the notifying Participant has reason to believe is affected or may have been the subject of unauthorized access, use or disclosure. The healthConnect Alaska Privacy and Security Officer shall be notified within one business day of such breach. healthConnect Alaska shall have the right to participate in the investigation and to know the results and remedial action, if any, taken, except that healthConnect Alaska need not be notified of specific workforce disciplinary actions. Each investigation shall be documented. At the conclusion of an investigation, a Participant shall document its findings and any action taken in response to an investigation. A summary of the findings shall be sent to healthConnect Alaska. healthConnect Alaska shall attempt to use examples of breaches for education and for policy and other safeguard development.

- II. Incident Response. healthConnect Alaska shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by Participants or discovered by healthConnect Alaska. This is described further in **2.600 Breach Notification Policy** and **2.601 Breach Notification Procedure**. The incident response system shall include the following features, each applicable as determined by the circumstances:
 - A. Cooperation in any investigation conducted by the Participant or direct investigation by healthConnect Alaska;
 - B. Notification of other Participants or authorized users as needed to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the breach;
 - C. Cooperation in any mitigation steps initiated by the Participant;
 - D. Furnishing audit logs and other information helpful in the investigation;
 - E. Developing and disseminating remediation plans to strengthen safeguards or hold Participants or authorized users accountable;
 - F. Any other steps mutually agreed to as appropriate under the circumstances; and
 - G. Any other step required under the incident reporting and investigation system contained in the healthConnect Alaska Security Rules.

- III. healthConnect Alaska Cooperation. healthConnect Alaska shall cooperate with a Participant in any investigation of the Participant's privacy and security compliance related to the System, whether conducted by an agency of state or federal government or conducted as a self-investigation by the Participant, when the investigation implicates

healthConnect Alaska conduct, or the conduct of another Participant or authorized user, or the adequacy or integrity of System safeguards.

- IV. Participant Cooperation. Each Participant shall cooperate with healthConnect Alaska in any investigation of healthConnect Alaska or of another Participant into healthConnect Alaska's or such other Participant's privacy and security compliance related to the System, whether conducted by an agency of state or federal government or conducted as a self-investigation by healthConnect Alaska or the other Participant, when the investigation implicates such Participant's compliance with External HIE Privacy, Security and Compliance Policy and related procedures or the adequacy or integrity of System safeguards.

- V. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs through the terms of their business associate agreements, if the BAs will have access to the System.

- VI. Responsibility for Costs. Each of the parties is responsible for their own costs in investigating or assisting in the investigation of a security incident or breach. If healthConnect Alaska is asked to provide assistance unrelated to its role in the breach, it may charge a reasonable fee for such assistance upon prior written consent of the requesting party.

4.211 INVESTIGATIONS; INCIDENT RESPONSE SYSTEM PROCEDURE		
APPROVED BY: healthConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/03/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healthConnect Alaska	REVISED:	11/26/2018 V2.1

4.212 Authorized User Controls Procedure

Procedure Summary

This procedure describes the process and responsibilities related to granting access to individual users.

Purpose

This procedure is to ensure that all Participants who are using the HIE and other data exchange services are authorized to do so, which will help to build trust in the System and among other Participants.

Scope/Applicability

The following procedure applies to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

This applies to all Participants, both HIE and DSM.

Regulatory Category, Type, Legal Regulatory Reference

Administrative Safeguards, Standard, Implementation, 45 CFR 164.308(a)(3)(i);
Technical Safeguards, Standard 45 CFR 164.312(a)

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 4.200 External HIE Privacy, Security and Compliance Policy
- 4.204 Access to and Use and Disclosure Procedure
- 4.206 Minimum Necessary Procedure

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Participant Responsibilities. Each Participant is responsible to:
 - A. Designate its responsible contact person who shall be initially responsible on behalf of the Participant for compliance with these policies and to receive notice on behalf of the Participant from healthConnect Alaska and from individuals requesting information from Participant regarding the System. For Participants that have their own system administrator, this shall ordinarily be the system administrator.
 - B. Designate its own authorized users from among its workforce, and designate business associates (BAs) and contractors authorized to act as (or designate from among their workforce) authorized users on its behalf in accordance with **4.204 Access to and Use and Disclosure of Information Procedure**, Paragraph 9 and **4.206 Minimum Necessary Procedure**. A list of these authorized users, along with the dates of authorization (and termination, if applicable) shall be made available to healthConnect Alaska on a quarterly basis, or upon reasonable advanced written notice by healthConnect Alaska.
 - C. Train and supervise its authorized users and require any BA or contractor to train and supervise its authorized users consistent with the Participant's and healthConnect Alaska's privacy and security policies and with the terms of the Participant's privacy and security policies and the BA Agreement as applicable. Participants are responsible for privacy training, and are required to do the training for malpractice and other liability purposes. Participants using EHRs have additional attestations they have to submit to malpractice insurers about use and privacy of EHRs. healthConnect Alaska does not know any organization's individual policies and cannot train on those areas.
 - D. In the case of Participants with a System Administrator, suspend, limit or revoke access authority as soon as possible but no later than 72 hours upon a change in job responsibilities or employment status of an authorized user. Revocation shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant. Participant's list of authorized users should be updated to reflect such change. If there is any risk associated with an authorized user's access, that access should be terminated immediately.
 - E. For Participants without their own System Administrator, immediately notify healthConnect Alaska of the change so that healthConnect Alaska may revoke access authority. Notification shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participant. If there is any risk associated with an authorized user's access, healthConnect Alaska should be notified immediately.
 - F. Hold their authorized users accountable for compliance with healthConnect Alaska and the Participant's policies and, as applicable, the terms of any BA Agreement.

Participant is solely responsible under this Agreement for all acts and omissions of Participant and/or Participant's users who access the Network either through Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from Participant or any of Participant's authorized users, with respect to the System, the System services and/or any confidential and/or other information accessed in connection therewith.

II. healthConnect Alaska Responsibilities. healthConnect Alaska is responsible to:

A. Grant access (Credentials Service Provider) authority to individuals designated by a Participant, subject to reserved authority to suspend, limit, or revoke such access authority as described later in this procedure.

B. Train and supervise its own authorized users on these policies and the standard terms required by its BA Agreement with Participants.

C. Suspend, limit or revoke access authority for its own authorized users or any authorized user who is a member of the workforce of any subcontractor of healthConnect Alaska as required by these policies or the terms of its BA Agreement in the event of breach or non-compliance.

D. Immediately revoke access authority upon a change in job responsibilities or employment status of its own authorized users or the authorized user of its contractor.

E. Suspend, limit, or revoke the access authority of an authorized user on its own initiative upon a determination that the authorized user has not complied with the Participant's privacy policies, Network Responsibilities or the terms of the user agreement, if healthConnect Alaska determines that doing so is necessary for the privacy of individuals or the security of the System.

F. Terminate access of Participant's authorized users upon notification from Participant that access should be terminated

G. Monitor access and notify Participants if a user may not have used the system for a prolonged period of time, or if healthConnect Alaska notices any other reason to review an authorized user's access for potential suspension or termination.

III. Application to BAs and Contractors. Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs through the terms of their business associate agreements, if BAs will have access to the System.

IV. Denial of Access. Participants should be aware that individuals may be denied access to the System based on past performance or behavior reported by a former employer or other participating entity. Participants may request information regarding a potential new hire, to determine if access will be denied prior to hiring an individual.

4.212 AUTHORIZED USER CONTROLS PROCEDURE

APPROVED BY: healtheConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/03/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healtheConnect Alaska	REVISED:	11/27/2018 V2.1

4.213 Sanctions Procedure

Procedure Summary

healthConnect Alaska ensures the confidentiality, integrity and availability of its information systems containing PHI by implementing appropriate and reasonable policies, procedures and controls to prevent, detect, contain, and correct security violations. healthConnect Alaska's security management program relies on Participants understanding and compliance with these policies and procedures by the workforce, and enacting similar sanction policies for non-compliance.

Purpose

This procedure reflects healthConnect Alaska's commitment to ensure the confidentiality, integrity, and availability of its information systems containing PHI by implementing sanctions or requiring Participants to implement sanctions in the event of identified security violations.

Scope/Applicability

The following rules apply to the access, use and disclosure of protected health information by Participants through the healthConnect Alaska Health Information Exchange ("HIE") and other data exchange services being made available to Participants in healthConnect Alaska (the HIE and other services are collectively referred to as the "System").

Regulatory Category, Type, Legal Regulatory Reference

"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

Administrative Safeguards, Standard, 45 CFR 164.308(a)(1)(ii)(C)

Procedure Authority/Enforcement

healthConnect Alaska's Executive Director (ED) and Privacy and Security Officer (PSO), in collaboration with the Participants, are responsible for monitoring and enforcement of this procedure.

Related Policies & Procedures

- 2.204 Employee Sanctions Procedure
- 4.200 External HIE Privacy, Security and Compliance Policy
- 4.201 through 4.213 External HIE Privacy, Security and Compliance Procedures

Renewal/Review

This procedure is to be reviewed annually to determine if the procedure complies with current HIPAA Privacy and Security regulations, AS 18.23.300 and other applicable Federal and State laws. In the event that significant related legal, regulatory or technological changes occur, the procedure will be reviewed and updated as needed.

Procedure

- I. Participant Responsibilities. Each Participant is responsible to:
 - A. Implement policies and procedures to sanction and hold authorized users, workforce members, agents and contractors accountable for failure to comply with any internal policies and procedures set by the Participant with regard to the use, disclosure or access of protected health information accessed through the System.
 - B. Implement policies and procedures to sanction and hold authorized users, workforce members, agents and contractors accountable for ensuring that they do not use, disclose or access protected health information except as permitted by the Participant Agreement and the External HIE Privacy Security and Compliance Policy and related procedures.
 - C. Such sanctions may include, but need not be limited to, verbal and written warnings, required retraining, suspension or termination of access to the System, suspension of employment without pay, and termination of contract or employment.
 - D. Notify healthConnect Alaska in writing of the name of individual, date and nature of violation (as well as action taken to remedy) of security violations.

- II. healthConnect Alaska Responsibilities. healthConnect Alaska is responsible to:
 - A. Impose sanctions on healthConnect Alaska personnel who are determined to have failed to adhere to healthConnect Alaska Privacy and Security Policies. Such sanctions shall be imposed and enforced in accordance with healthConnect Alaska's Employee Sanction Policy and may include, but not be limited to, verbal or written warnings, required retraining, suspension without pay, and termination of contract or employment.
 - B. Upon receiving a report, discovering or being notified of a reportable event from a Participant, healthConnect Alaska shall coordinate with the affected Participant to determine if the appropriate sanctions have been imposed by the Participant. If healthConnect Alaska's privacy and security officer determines that further action is necessary, healthConnect Alaska shall impose one or more additional sanctions, consistent with the violation. Depending on the circumstances, sanctions may be on an individual authorized user level or a Participant level.
 - C. Upon receiving a report, discovering or being notified of a reportable event that cannot be attributed directly to any one Participant, healthConnect Alaska shall impose one or more sanctions on the identified offender, consistent with the violation. Sanctions for an unintentional violation may include, but are not limited to: verbal warnings; written warnings; suspension of access privileges; and revocation of access privileges. Sanctions for an intentional violation may include, but are not limited to:

immediate suspension of access; revocation of access; a complaint filed with the violator’s professional licensing board, if the violator is professional licensed; information turned over to a prosecutor for criminal prosecution; and potential other legal action.

- D. Create a database or other resource to verify if a prospective authorized user has been sanctioned previously or has had a complaint filed against them substantiated for a potential security violation.
- E. Document and maintain records of all reported events for six (6) years, regardless of whether sanctions are imposed.

III. Appeals. Persons who are sanctioned by healthConnect Alaska, or who otherwise have their privileges limited, may appeal the sanctions or limitation to healthConnect Alaska. Appeals must follow the following guidelines:

- A. Appeals must be filed in writing and received at healthConnect Alaska’s offices within 10 business days of the sanction being imposed.
- B. healthConnect Alaska staff will consider the appeal and make a determination of whether to continue the sanction within 10 business days of receiving the written appeal.
- C. healthConnect Alaska will provide the party filing the appeal with a written notice of its decision within 10 business days of making the decision. Sanctions will remain in effect while the appeal is being considered.
- D. If the appeal is denied, and the appealing party believes there has been an error, it may file a request with healthConnect Alaska for an external review. Such requests must be made in writing within 30 calendar days of the appeal being denied. healthConnect Alaska will refer the case to an independent party, which will review the evidence and make a recommendation to healthConnect Alaska’s board of directors, which will make the final decision.

4.213 SANCTIONS PROCEDURE		
APPROVED BY: healthConnect Alaska Executive Director	ADOPTED:	02/20/2013 V1
	REVISED:	06/24/2013 V2
	REVIEWED:	06/06/2014 V2
	REVIEWED:	03/03/2015 V2
	REVIEWED:	03/16/2016 V2
	REVIEWED:	07/19/2017 V2
Name change from AeHN to healthConnect Alaska	REVISED:	11/27/2018 V2.1