Privacy and Security Procedures for Grantees

POLICY:

This policy and its accompanying procedures are based on the following: (1) DHSS's obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (42 U.S.C. 1320d – 3120d-8), the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5) (the "HITECH Act") and their implementing regulations at 45 C.F.R. 160 and 45 C.F.R. 164 (the "Privacy and Security Rule") to protect the privacy and security of protected health information (2) where applicable, the obligations of grantees under HIPAA, HITECH Act and the Privacy and Security Rule; (3) where applicable, the obligations of grantees that are federally assisted alcohol and drug abuse programs and subject to the confidentiality protections of 42 C.F.R. Part 2; and (4) obligations for records retention and transfer of records codified as 7 AAC 78.250 - 78.255.

It is the policy of DHSS that the following procedures be incorporated as terms of DHSS's grant agreements. When used in the accompanying procedures, the following terms shall be defined as set forth at 45 C.F.R. Parts 160 and 164: "electronic protected health care information," "protected health information," "use," "disclosure," "workforce," "availability," "confidentiality," "integrity," "security," "breach," and "health oversight agency."

PROCEDURES AND REQUIREMENTS:

1. Security Practices. The grantee that creates, receives, maintains, or transmits electronic protected health information in its role as grantee shall undertake the following acts regarding such information:

    a. Ensure the information's confidentiality, integrity, and availability. 45 C.F.R. 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures and documentation requirements) shall apply to the grantee in the same manner that such sections apply to DHSS, and shall be implemented in accordance with HIPAA, the HITECH Act, and the Privacy and Security Rule. The additional requirements of Title XIII of the HITECH Act contained in Public Law 111-5 that relate to security and that are made applicable to covered entities shall also apply to the grantee and are incorporated into this Privacy and Security Procedures.

    b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information, including during its transmission to and from the grantee.

    c. Protect against reasonably anticipated uses or disclosures of such information when the use or disclosure is not required or permitted by law.

    d. Implement protections that govern the receipt, removal, disposition, and re-use of hardware and electronic media (which includes, but is not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, handheld electronic devices and removable storage devices such as floppy disks, zip disks and memory cards) that contain or have contained electronic protected health information. In particular, the grantee shall:

        i. Ensure that all hardware used or electronic media developed by the grantee for the grant project be cleaned with a wipe utility that prevents the recovery of any

information from the device, prior to the hardware or device being re-used, salvaged, surplussed, or disposed.

ii. For each piece of hardware or electronic media to be re-used, salvaged, surplussed, or disposed, furnish a Disposal Assurance Form (attached as Exhibit 1 to these procedures) to the grants administrator named in the Grant Agreement.

e. Ensure that its workforce protect the security of such information.

2. Privacy Practices. The Grantee that creates, receives, maintains, or transmits protected health information in its role as grantee shall undertake the following acts regarding such information:

a. Establish physical, technical, and administrative safeguards that prevent the improper use or disclosure of the information, including:

i. Designating a person or persons to be responsible for assuring the privacy of the information.

ii. Developing and implementing privacy policies and procedures regarding required and permissible use and disclosure of the information. Toward that end, the grantee may only use and disclose protected health information owned by DHSS that it accesses, maintains, retains, modifies, records, stores, receives, or transmits if the use or disclosure is in compliance with each applicable requirement of 45 C.F.R. 164.504(e) of the Privacy Rule. The additional requirements of Subtitle D of the HITECH Act contained in Public Law 111-5 that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to the grantee and are incorporated into this Privacy and Security Procedures.

To the extent that the grantee discloses protected health information to a third party, the grantee must obtain, prior to making any such disclosure: (1) reasonable assurances from the third party that the protected health information will be held confidential as provided in this Privacy and Security Procedures and only disclosed as required by law or for the purposes for which it was disclosed to the third party; and (2) an agreement from the third party to notify the grantee within one business day of any breach of confidentiality of the protected health information, to the extent it obtained knowledge of the breach.

iii. Identifying a contact person responsible for receiving complaints, appropriately investigating, and, if necessary, taking prompt corrective action to cure any deficiencies that result from breaches of security, intrusion, or unauthorized use or disclosure of grant recipient information.

iv. Permitting the disclosure of the information to DHSS as a health oversight agency (without requiring the authorization of a recipient of services) for purposes of DHSS's determination of grant compliance, grant administration, grant termination, or grant assignment.

b. Take reasonable steps to mitigate the harmful effects of any improper use or disclosure of the information.

c. Discipline workforce that violate the grantee's privacy policies and procedures.

d. Not coerce, discriminate, or retaliate against any person for exercising his or her rights regarding such information or for reporting any alleged violation of the grantee's privacy policies and procedures.

3. Reporting of Unauthorized Disclosures and Breaches. The grantee that creates, receives, maintains, or transmits protected health information in its role as grantee shall notify DHSS within 24 hours of any suspected or actual breach of security; intrusion; or unauthorized acquisition, access, use or disclosure of protected health information in violation of any applicable federal or state law. The grantee shall use a Notification of Suspected Breach Form (attached as Exhibit 2 to this Privacy and Security Procedures) to the grants administrator named in the Grant Agreement and to the Privacy and Security Officers of DHSS. The grantee shall identify for DHSS the individuals whose unsecured protected health information has been, or is reasonably believed to have been, breached so that DHSS can comply with any notification requirements if necessary. The grantee shall also indicate whether the protected health information subject to the suspected or actual breach; intrusion; or unauthorized acquisition, access, use or disclosure was encrypted or destroyed at the time. The grantee will be responsible for complying with any notification requirements under HIPAA, the HITECH Act, the Privacy and Security Rule or other law. The grantee will take prompt corrective action to cure any deficiencies that result in breaches of security; intrusion; or unauthorized acquisition, access, use, and disclosure. The grantee shall indemnify and hold harmless DHSS for any civil monetary penalty imposed, monetary settlement with, or award of damages against, DHSS for acts or omissions in violation of HIPAA, the HITECH Act, or the Privacy and Security Rule that are committed by the grantee or a member of its workforce. Grantee shall also reimburse DHSS for all costs incurred by DHSS that are associated with any mitigation, investigation, or notice of breach DHSS undertakes or provides under HIPAA, the HITECH Act, the Privacy and Security Rule, or other applicable law as a result of a breach of DHSS's PHI caused by Grantee or Grantee's agent or subcontractor. The grantee is not an agent of DHSS.

4. Internal Practices. The grantee shall make its internal practices, books and records relating to the use and disclosure of DHSS's protected health information available to DHSS and all appropriate federal agencies to determine DHSS's compliance with HIPAA, the HITECH Act and the Privacy and Security Rule.

5. Substance Abuse Treatment Records. DHHS is mindful that some grantees are subject to 42 C.F.R. Part 2, because they are in receipt of federal funds for the operation of alcohol and drug abuse programs. Such grantees shall undertake the following acts regarding protected health information concerning such programs for which the grantee also receives grant funding from DHSS:

a. Protect the confidentiality of alcohol and drug abuse patient records as required by 42 C.F.R. Part 2, including:

i. Restricting the use and disclosure of information, whether recorded or not, which would identify a patient as an alcohol or drug abuser, all as permitted or required by 42 C.F.R. Part 2;

ii. Providing security for written records as required by 42 C.F.R. § 2.16;

iii. Adopting written procedures which regulate and control access to and use of written records, as required by 42 C.F.R. § 2.16(b);

iv. Applying the restrictions for disclosures of information with patient consent, as set forth at 42 C.F.R. §§ 2.31 - 2.35; and

v. Applying the restrictions for disclosures without patient consent, as set forth at 42 C.F.R. §§ 2.51 -2.67.

6. Resolve any conflict between these procedures or any other law in favor of the protection of the confidentiality of alcohol and drug abuse patient records.

7. Retention of Records. The Grantee shall undertake the following acts:

a. Retain documents relating to the grantee's privacy and security practices for six years.

b. Ensure that its records are retained as required by 7 AAC 78.250, which includes the following obligations:

i. Retaining and preserving financial and administrative grant records, including records of the receipt and disposition of grant income that are necessary to meet auditing requirements, for at least three years. Such records shall be retained longer, all as set forth at 7 AAC 78.250, if:

(A) An audit is in progress or audit findings, litigation, or claims involving the records are pending; or

(B) The records pertain to non-expendable personal property of the grant project.

ii. Retaining and preserving records that relate directly to the care and treatment of a recipient of services for at least seven years following the termination of services to that recipient, subject to the following:

(A) Any additional obligations required by AS 18.20.085 for hospital records;

(B) If a minor's care is at issue and the grantee is not a hospital already subject to AS 18.20.085, retaining and preserving records that relate directly to the care and treatment of a minor for at least seven years after the minor has reached the age of majority or until seven years after the termination of services, whichever is longer.

8. Storage and Transfer of Records.

a. If a grantee's business or organization closes or ceases to exist as a service provider under the grant, or if the records must be transferred for any other reason, the grantee must notify the

grants administrator named in the Grant Agreement within 48 hours of such decision. The notice shall:

i. Be signed by the grantee's board of directors or chief executive officer;

ii. Indicate whether the grantee will retain and store its records in an appropriate, secure fashion or transfer its records to a continuing board, another organization, or to DHSS; and

iii. Include a formal plan for the retention or transfer of records that provides:

(A) A description of how and when the grantee will notify each recipient of services regarding where the files will be transferred or stored and how the recipient can continue to receive services and obtain a copy of the recipient's records;

(B) A complete list of all files being transferred or stored; and

(C) A complete list of all recipients who will be sent the notice.

b. A grantee that is storing or transferring records must also:

i. Box all paper records, ensuring:

(A) Financial and operating records are in separate boxes from treatment records; and

(B) As it pertains to treatment records, records of minors are in separate boxes from records of adults.

ii. Contact the grants administrator named in the Grant Agreement for instructions regarding the transfer of electronic records.

b. If the grantee is a federally assisted substance abuse treatment program, the grantee shall follow the procedures for disposition of records set forth at 42 C.F.R. § 2.19. If a specific requirement of 42 C.F.R. Part 2 conflicts with a requirement of these procedures, the grantee shall follow the requirements of 42 C.F.R. § 2.19 as it pertains to any such conflict.

Exhibit 1
STATE OF ALASKA
DEPARTMENT OF HEALTH AND SOCIAL SERVICES
Media Disposal Assurance Form
Grants & Contracts (907) 465-5424

☐ Salvage/Surplus ☐ Destruction ☐ Other: Re-use

Technical Contact Information

Provider or Grantee Agency Name:	Provider/Grantee Technician Contact Name:	Phone #:

Computer or Drive Information (or attach list)

Computer Make:	Computer Model #:	Computer S/N #:	Drive Model #:	Drive Make #:	Drive S/N #:

Provider/Grantee Authorizing Officer Contact Information

Provider or Grantee Authorizing Officer Name:	Phone #:

Terms and Conditions

The Department of Health and Social Services requires all electronic media to be cleaned with a wipe utility that prevents the recovery of any Department data or data acquired in the performance of services on behalf of the Department from the device, prior to being re-used, salvaged, surplussed, or disposed of. The Department further requires:

Re-used/Salvage/Surplus Devices:

- A three (3) pass random wipe, where each sector of a disk is erased and written to a minimum of three times. A wipe utility that is compliant with the DoD 5220.22-M clearing and sanitization method must be used.
- The Media Disposal Assurance Form signed by the Technician performing the electronic wipe and by the Authorizing Officer of the Provider/Grantee Agency confirming the required action.
- A copy of the completed Media Disposal Assurance Form is submitted to the Grants & Contracts office.

Disposal of Devices:

- One of the following approved methods must be used. Please indicate which method was used:

  ☐ A three (3) pass random wipe, where each sector of the disk is erased and written to a minimum of three times.

  Or

  The device destroyed in such a manner that the media is not recoverable.

  ☐ Removal Media – Magnetic Media Cut or Severed

  ☐ Hard drives – Magnetic Platters Drilled or removed and broken
- The Media Disposal Assurance Form signed by the Technician performing the electronic wipe and by the Authorizing Officer of the Provider/Grantee Agency confirming the required action
- A copy of the completed Media Disposal Assurance Form is submitted to the Grants & Contracts office.

I hereby certify the terms and conditions for the Media Disposal Assurance has been met for the device(s) listed above.

Technician Signature and date:	
Authorizing Officer Signature and date:	

Exhibit 2

NOTIFICATION OF SUSPECTED BREACH

Provider or Grantee Organization Name:_____

Provider or Grantee Address:_____

Provider or Grantee Contact Person:_____ _____

Provider or Grantee Contact Person's Telephone Number:_____

Identify the suspected or actual breach of security, intrusion, or unauthorized use or disclosure of grant recipient information (Please be as specific as possible and include names, dates, times, and specific actions or concerns. Use the other side of this form if you need more room. Attach any relevant documents.)

Attached documents include:

Identify actions taken or to be taken to remedy the suspected or actual breach: