Alaska Division of Public Health
Prevention Promotion Protection

Alaska Section of Epidemiology Confidentiality Policies and Procedures and Data Release Protocols

Updated May 2020

Table of Contents

Links:
- Alaska Statutes and Regulations
- Section of Epidemiology Data Request and Sharing Agreement Forms
- DHSS Request for Access to PHI Form

I. Confidentiality Policies and Procedures

Confidentiality procedures in the Section of Epidemiology (SOE) are intended to protect the privacy of patients and the facilities reporting these patients to SOE, to ensure the integrity of data, and to comply with confidentiality-protecting legislation and administrative rules. All Programs within SOE must adhere to these policies and procedures; additional more stringent policies may be developed by individual Programs that are tailored to their specific needs.

A. State Laws and Regulations

Alaska state law directs the Department of Health and Social Services (DHSS) to promulgate regulations for the control of communicable diseases and other reportable conditions (Attachment 2). Alaska statutes (AS) authorize the Department to (among other activities) collect confidential information, provide for certain laboratory testing, and respond to public health threats. Alaska regulations operationalize that authority by mandating reporting to the Division of Public Health of certain conditions of public health importance and setting forth recommended investigatory and follow-up practices.

Statutes and regulations also specify conditions for handling confidential information received by the Division and make misuse of confidential information by a public employee a misdemeanor.

B. Definitions

1. *Authorized Personnel*—Any SOE staff including full- or part-time employees, contractors, and federal assignees who require access to confidential information to conduct their duties. Other persons may also be authorized access to confidential information as described below.

2. *Confidential Data*—For the purposes of this document, confidential data is synonymous with protected health information or other protected information (defined in #10 below).

3. *Confidentiality*—The obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for, and to protect and preserve, the privacy of others.

4. *Department Security Officer* (DSO)—Staff person in DHSS assign to develop, implement and oversee security policies. Reachable at hss-security@alaska.gov

5. *External Report*—Any report written by SOE staff that will be shared with an outside agency or person.

6. *Limited Data Set*—Protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.

7. *Other Authorized Persons*—Other persons who are not SOE employees (e.g., trainees, students, volunteers, interns, etc.) may under certain circumstances be authorized to access

confidential information for a specific project or purpose. All requests for such persons to be authorized must be approved by the Section Chief.

8. *Overall Responsible Party* (ORP)—The Overall Responsible Party (ORP) for the Section of Epidemiology is the Section Chief, who is responsible for the security of public health data Section Programs collect and maintain.

9. *Program Manager*—Program Managers are employees who report directly to the Section Chief and are responsible for overseeing one or more of the Section's programs.

10. *Protected Health Information* (PHI)—Any information held by a covered entity about health status, provision of health care, payment for health care, or other protected information that can be linked to an individual. Identifiable health information is defined by Alaska Statute (see page 31, AS 18.15.395(13)). For the purposes of the Section of Epidemiology Confidentiality Policy, PHI refers not only to data that are explicitly linked to a particular individual (i.e., identifier information), but also includes health information with data items which reasonably could be expected to allow individual identification. The U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996 lists the following 18 identifiers:
    a. Names;
    b. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    c. Dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
    d. Phone numbers;
    e. Fax numbers;
    f. Electronic mail addresses;
    g. Social Security numbers (SSN);
    h. Medical record numbers;
    i. Health plan beneficiary numbers;
    j. Account numbers;
    k. Certificate/license numbers;
    l. Vehicle identifiers and serial numbers, including license plate numbers;
    m. Device identifiers and serial numbers;
    n. Web Universal Resource Locators (URLs);
    o. Internet Protocol (IP) address numbers;
    p. Biometric identifiers, including finger, retinal and voice prints;
    q. Full face photographic images and any comparable images; and
    r. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

11. *Additional Protected Information*—For the purposes of the Alaska Violent Death Reporting System, the following personal information should be treated in the same manner as PHI. Personal information documents include, but are not limited to, employer records (e.g., training, accident reports), law enforcement reports, public safety records, court records, first responder records, military investigation reports, occupational regulatory documents, vital statistic certificates, autopsy reports/records, or other federal notification/investigative documents (e.g., NTSB, OSHA).

12. *Secondary Data*—Data that have been collected by an agency other than the SOE and provided to the SOE for use are considered secondary data. Examples of secondary data include population census data, vital statistics data, and school enrollment data. Secondary data may or may not contain confidential information.

13. *Syndromic Surveillance Data*—Data that are part of the BioSense/ESSENCE application that stream to a cloud-housed system to which SOE grants access. Data represent individual patient encounters with health care facilities that populate the Alaska Health Information Exchange.

14. *Summary Data*—Data provided by the SOE may include summary information grouped by age, sex, or geographic area and displayed so that individual patients, physicians or institutions are not identifiable.

C. Responsibility to Safeguard Confidentiality

Every person working in the Section of Epidemiology (SOE) has an ethical and legal obligation to protect the privacy of the persons whose records the SOE maintains.

1. *Personal Identifiers*—No information which identifies a specific individual, health care provider, or hospital is to be shared with anyone except as delineated by these policies and procedures. If an outside agency, institution or individual (e.g., news media) possesses confidential information, SOE staff will neither confirm nor deny the accuracy of the confidential information held outside the SOE, except as necessary for the performance of their duties as described in Section E below. The obligation to protect confidential information extends indefinitely, even after the death of the patient or termination of employment in the Section, Department, or State.

2. *Signed Agreement*—All SOE staff and any other authorized person as defined above **must** sign a confidentiality agreement **prior** to being allowed access to confidential data (see Attachment 1). In addition, all staff will be provided a copy of this policy and have an opportunity to ask questions and have them answered. Failure to observe the confidentiality policies will be grounds for immediate disciplinary action and could constitute grounds for immediate termination and criminal proceedings. Program Managers must ensure that their staff are aware of updates or changes to SOE's Confidentiality Policies and Procedures.

3. *Human Subjects Training*—The Section Chief will determine which program managers and program staff should successfully complete the CITI (Collaborative Institution Training Initiative) Program research ethics course every 3 years.

4. *HIPAA Training*—All staff will be required to successfully complete on-line DHSS HIPAA training on an annual basis, or more frequently if mandated.

5. *Data Security and Confidentiality Training*—All staff with access to data that contains PHI will be required to review SOE data security and confidentiality training annually or more frequently if policies are substantially updated in the interim.

6. *Requirements for Contractors and Grantees*—Appropriate language reflecting DHSS confidentiality policy and practices must be incorporated into all contracts and grants awarded by SOE for which there will be sharing of PHI by the recipient. These additions should include information about how to report breaches and potential consequences.

D. Release of Summary Public Health Data in Reports

Published data, e.g., data published in an Epidemiology *Bulletin* or as a fact sheet that was previously publicly available, can be released by any SOE employee. Release of data or reports that were previously available to a limited group of stakeholders should be considered on a case-by-case basis in consultation with the Program Manager and Section Chief. SOE staff are required to obtain review by Program Managers of all reports to be released externally to ensure that confidentiality has been maintained.

Release of summary data to other parties wishing to perform analyses is addressed in Section II. All requests for data release will be reviewed by the appropriate Program Manager, and then subsequently by the Section Chief for final approval. Requests for data should be submitted on an SOE Summary Data Request and Utilization Agreement Form (see Attachment 3).

E. Release of Information for Public Records Request

Before releasing any reports and documents containing medical information pursuant to a public records request, Program Managers should:

- Redact or withhold any information that contains PHI or additional protected information;
- Release the materials as a public record unless another Public Records Law exemption prohibits the release; and
- Ensure that staff from the Attorney General's Office are aware of the request and have provided guidance on what can be legally released.

F. Release of Confidential Data to Health Care Providers, Health Officials, and Patients

Staff must protect the identity of patients while working with external organizations. In some instances, non-confidential information may be used to identify individual patients or institutions through indirect means (e.g., combinations of variables might be enough to specifically identify an individual living in a small community). Great caution must be exercised in the use of such data because of the potential to breach confidentiality. The following guidelines apply to the release of confidential SOE data to hospitals, health care providers, and other state or federal agencies that provide or oversee direct health-care services.

1. *Release of Data to Hospitals, Health Care Providers, and Public Health Officials*—Certain SOE Programs (e.g., HIV/STD, TB/Infectious Disease) must confer with health care providers and hospitals to determine the final diagnosis and need for further investigation. As such, SOE staff will need to discuss confidential information with appropriate health care and public health workers. Release of confidential data to hospitals or health care providers is dependent on the type of information and program. Staff within Programs should check with appropriate Program Managers for policies regarding routine releases. For unusual release requests or situations, Program Managers should confer with the Section Chief prior to releasing data.

2. *Request from Patients for Data Related to Them*—Staff should review *DHSS Policy and Procedure #709*, which describes patient right of access to records held by DHSS Programs. All requests for access to information by a patient or a patient representative must be in writing, using the *DHSS Request for Access to PHI Form* (Attachment 4). SOE will respond to such requests within the required time frame of 30 days. Request for access by a patient or authorized representative will generally be granted, although a number of exceptions exist and are described in detail in *DHSS Policy and Procedure #709.* SOE staff will at all times prevent inadvertent release of information about patients who have not authorized that confidential data be released. Again, for unusual release requests or situations, Program Managers should confer with the Section Chief prior to releasing data.

3. *Releases and Requests Specific to an Immunization Information System*—The intent of an Immunization Information System (IIS), i.e., VacTrAK in Alaska, is to collate immunization data for individuals and allow access to that information by authorized health care providers and patients, and other entities covered under permitted disclosures [see 7 AAC 27.893(b)]. Agreements and policies covering these specific incidences should be referred to the Alaska Immunization Program Manager.

4. *Releases and Requests Specific to Syndromic Surveillance Data*—Syndromic surveillance data that are accessible to the Section of Epidemiology originate from health care facilities statewide and are collated by external partners, e.g., the Alaska Health Information Exchange, and ASTHO (Association of State and Territorial Health Officials). Data requests should be made with the standard Data Request and Utilization Agreement Form; however, releases may be subject to additional provisions specific to attributes of syndromic surveillance.

G. Release of a Limited Data Set

A limited data set (LDS) may be used and disclosed for research, health care operations, and public health purposes. The LDS must lack 16 of the 18 identifiers itemized by the Privacy Rule; specifically, an LDS must **NOT** include the following identifiers:

- Name
- Postal address information, other than town or city, State, and zip codes;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;

- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

The difference between an LDS and de-identified information is that an LDS can contain dates and certain geographic information associated with an individual that are absent from de-identified information. An LDS can contain, for example:

- Dates of birth
- Dates of death
- Dates of service
- Town or city
- State
- Zip code

Requests for data should be submitted on an SOE Summary Data Request and Utilization Agreement Form (see Attachment 3). All requests for limited data set release will be reviewed by the appropriate Program Manager, and then subsequently by the Section Chief for final approval. Prior to release of the data set, a data use agreement promising specified safeguards for the PHI or additional protected information within the LDS must be approved by the Section Chief. Program Managers are responsible for maintaining records of data requests and subsequent data releases.

H. Release of Secondary Data

Except as pertaining to VacTrAK Alaska's immunization information system and BioSense (syndromic surveillance data), SOE does not release original, individual-level data that were collected by another agency and then reported to SOE. Persons requesting data from SOE that did not originate in SOE should be referred to the agency or institution with primary responsibility for collecting the data.

I. Transmission of Confidential Data

After assuring that the requirements described in Sections C and F have been met, authorized SOE staff may transmit confidential information.

1. *Transmission via Telephone*—When transmitting confidential information by telephone, staff members must:

- Verify the identity of all requestors seeking the disclosure of confidential information over the telephone by obtaining a written request for data if the party or agency is unknown to SOE staff members.

- Whether using landlines, cellular telephones, or public telephones, disclose confidential information by telephone only from a secure or private area.
- Never leave messages with confidential information on voicemail, answering machines or with individuals other than the data subject or their personal representative *unless* the voicemail/answering system is known to be protected (e.g., that of a public health nurse). Information left in messages shall be generic in nature and not indicate the services being performed or the provider of such services, unless the data subject has directly requested otherwise and this is documented in the data subject's record. An example of a generic message is, "My name is Emily Smith. Please return my call at 907.269.8000."
- Provisional approval has been granted by the DSO to use video-chatting applications on cell phones for transmission of personal health information for the purposes of tuberculosis management. This use is limited in scope and must adhere to the written policies of the Infectious Disease Program.

2. *Transmission via Mail*—When sending confidential information by U.S. mail, SOE staff must:
- Verify that the correct confidential information is being mailed to the correct individual(s);
- Send the information in a security envelope marked "Confidential;"
- Include the sender's name and a return address;
- To the extent possible, verify that the recipient's address is correct; and
- Whenever feasible, send the information by registered or certified mail, or another method that provides delivery tracking.

3. *Transmission via Delivery or Courier Service*—When sending confidential information by hand delivery or courier service, SOE staff must:
- Verify that the correct confidential information is being delivered to the correct individual(s);
- Verify the name and address of the intended recipient;
- Seal the information under protective cover (e.g., a folder or envelope) and mark the package "Confidential;"
- Use a reputable courier service known to the Division;
- Request identification from the courier, record the courier's name and time of pick-up; and
- If possible, retain a tracking number so that in the event the intended recipient informs you that the package was not received, you are able to track the item with the delivery service.

4. *Transmission via Facsimile (Fax)*—When sending confidential information by facsimile machine, staff members must:
- Verify the fax number of the intended recipient;
- Aside from faxes to routine/known recipients (e.g., public health centers), telephone the recipient to alert him/her that a fax containing confidential information is to be transmitted;
- Transmit the fax using a SOE-specific cover sheet that contains a confidentiality statement and instructions directing the unauthorized recipient of a misdirected fax to contact the sender. In the event of a misdirected fax, the unauthorized recipient should be directed to immediately destroy the fax or return the information to the sender, as directed by the sender.

- For faxes to non-routine recipients, if the recipient does not confirm receipt within a reasonable period of time, call the recipient to confirm receipt.
- Remove the faxed documents from the vicinity of the fax machine, including the fax activity confirmation sheet after transmission. Keep fax activity confirmation sheets with original documents.
- Locate fax machines in a secure, lockable area to which only authorized SOE staff have access.

5. *Transmission via Electronic Mail (E-mail)*—Standard electronic mail must **not** be used directly to send or receive confidential data, regardless of whether an email is sent to an outside party or to another SOE staff member. However, as approved by the Department, selected software products that can encrypt messages (such as Direct Securing Messaging) are acceptable for transferring PHI or additional protected information. Program Managers must ensure that staff are aware of and adhere to the Department policies governing the use of encryption products. Program Managers will work with staff to request outside agencies who communicate confidential information to SOE not to include any identifying information on electronic mail messages. Other agencies may have their own encryption software for electronic mail (e.g., Providence Hospital, Alaska Native Medical Center); check with the DSO about whether that use is acceptable on a case-by-case basis.

6. *Transmission via Scanner*—Hard copy data that contains PHI may sometimes need to be transformed to an electronic format to be saved or archived. The DHSS policy is to temporarily assume the risk involved with scanning a document and delivering it to a state email address. However, SOE policy is more restrictive in that all documents with PHI should be scanned only to a secure encrypted jump drive and then saved to a secure network location or attached to an e-mail using previously described secure methods (see #5 above).

7. *Exemption for Transmission of Employment Records*—Employment records held by a covered entity in its role as employer may be transmitted electronically via e-mail or scanner (45 CFR 160.103).

J. On-Site Security

All SOE employees are responsible for data security. There are many aspects to securing data and it is critical to have several levels of data security to ensure the confidentiality of patients as well as to ensure data integrity.

1. *Workstation Security*—To minimize the opportunity for SOE staff or worksite visitors to inadvertently view confidential health information to which they should not have access, SOE staff shall adhere to the following guidelines at all times:

- Workstations at which confidential data are handled are to be located in secure areas of SOE or Department property.
- Computer monitors should be turned so that they are not facing hallways or other heavily trafficked areas. If a monitor must be placed facing the hallway, a security screen should be used.

- When creating passwords, SOE staff should select at least an 8-character alphanumeric combination. Obvious choices such as children's names, repeating numbers, birthdays, and telephone numbers should not be used.
- Passwords must not be shared.
- No one should use a computer while it is operating under another person's password.
- Passwords should not be displayed in the work area.
- Documents containing confidential information should be turned face-down when the workstation is unattended during work hours; these documents should be stored in a locked file cabinet before leaving the workspace at the end of the day.
- SOE staff must log off or lock their computers when stepping away from their desks for an extended period or leaving at the end of the day.
- Work should not be saved to individual computer hard drives (i.e., C:drive) but rather to shared secured network drives.

2. *Office Access*—SOE offices in the Frontier Building are secured with outer doors with suitable locks to prevent access by unauthorized personnel. During the work day, public entrance to SOE is limited to access only through Suite 540; other hallway doors will be secured at all times. The Administrative Officer and Administrative Assistant are responsible for maintaining door codes and changing codes, if necessary. All guests must sign in at the front desk and wear a visitor badge that is clearly visible. Access codes to offices are controlled by computers. State employees should only be accessing the office after hours as required for their work duties.

Non-state employees, interns, volunteers or contractors must be instructed by their SOE sponsor as to which offices and work spaces they may access during business hours. If outside normal business hours, such persons must be escorted and monitored by a state employee the entire time they are in the SOE offices.

3. *Internal Access to Offices*—Program Managers or their designees are responsible to ensure the security of staff work areas. When not in use by authorized personnel, program offices where confidential data are stored will be locked. Keyed office access will be limited to those individuals designated by the Program Managers.

4. *Paper-Based Confidential Information*—SOE staff must properly store on-site paper-based files as follows:

- Store paper-based confidential information in a locked file cabinet;
- Position file cabinets or other storage sites away from public areas, preferably in low-traffic areas, and if possible closest to staff who will be regularly accessing the data stored within;
- Store file cabinets without locks in rooms that can be locked or otherwise secured; limit access to rooms with unlocked cabinets based on need–to-know, role-based access.
- Staff should immediately retrieve papers that contain confidential information from printers and copy machines.

5. *Electronic Confidential Information*—Electronic confidential information shall be maintained by the data custodian in a manner that protects the confidentiality, integrity, and availability of the information.

- A computer from which confidential information is accessed must be password-protected and configured to adhere to the current DHSS standard of encryption technology.
- Confidential information stored on any removable media (e.g., thumb drives) must be saved using encryption technology that meets DHSS standards.
- Confidential information stored on any portable devices (e.g., laptops) must be saved using encryption technology that meets DHSS standards.
- Program Managers should ensure that staff members have been trained on the appropriate use of the various SOE network drives.
- Workforce members shall not circumvent prescribed access rights by sharing their passwords or utilizing another workforce member's password to access confidential information beyond the scope of their authority.

6. *Records Retention*—Records, whether electronic or in hard copy, must be retained per the SOE's Records Retention Schedule that was last updated in 2012. Schedule available at: http://archives.alaska.gov/pdfs/records_management/schedules/hss/public_health/06-214.pdf

7. *Changes to Employment Status*—When an SOE staff member resigns, retires, is terminated or transferred, SOE administrative staff must ensure that the appropriate steps have been taken to restrict future access of the non-employee to SOE offices. Specifically, the SOE Administrative Officer will ensure that:

- The individual passcodes to locked doors are inactivated centrally; and
- DHSS Information Technology staff (IT) are immediately notified to immediately terminate former employees rights and access.

K. Off-Site Security

SOE staff shall not remove confidential information, including paper or electronic information, from the work site unless it is required for a field visit, meeting, or otherwise necessary for work-related purposes and only if authorized by the Program Manager. Appropriate measures shall be taken in each instance to ensure that confidential information removed from the worksite is secured from unauthorized access and not left unattended in an unsecured area or container. This includes securing documents when permitted to be taken home away from other household members or visitors to the home.

1. *Data Collection Using Portable Computers*—Laptop computers, PDAs, and other portable devices on which confidential information is stored should be protected at all times and should not be left unattended. While in automobiles, laptops, PDAs, and other portable devices should be kept out of sight (e.g, in a trunk or hidden under a seat) and locked when the car is unattended. Laptops, PDAs, and other portable devices on which confidential information is stored should not be loaned to any unauthorized person, including family members.

SOE staff may collect data in the field onto a state-issued laptop (portable) computer outfitted with appropriate encryption software. Each staff member will be responsible for securing the data collected to prevent access by unauthorized personnel. If air travel is involved, laptop computers, PDAs, and other portable electronic devices will be handled as carry-on luggage. When not in use, the computer, PDAs, and other portable devices will be kept in a secure area. PHI data should not

be viewed on laptops or other devices when the screens cannot be secured in a public space, e.g., while working on an airplane.

Upon returning from the field, staff will bring the portable computers and any backup portable storage devices to the SOE office and data will be transferred to the employee's desktop computer and stored on a secure hard drive. PHI data will then be permanently deleted from the portable computers and any backup portable storage devices. Alternatively, the backup portable storage devices may be secured (locked) in an archive file and retained according to the State retention schedule.

Work that will use PHI may NOT be done on a home computer, or any other device that is not state-issued and thus equipped with approved security technology.

2. *Data Collection [Using Other Methods]*—When SOE staff collect data in the field that are hard copies in the form of medical records, forms, handwritten abstracts or other paper materials, these data will be secured by each individual staff member to prevent access by unauthorized personnel. If air travel is involved, the case will be handled as carry-on luggage. When not in the staff member's possession, it will be kept in a secure area. Hard copy data should not be left unattended in automobiles. Upon returning from the field, staff will bring the hard copy data to the SOE office and secure it in a locked filing cabinet until the collected data can be transferred to another media. All hard copy data will be retained according to the State retention schedule.

3. *Alternate Work-Sites*—In the event of an emergency, SOE may need to relocate staff and computers to an alternate work site location. Temporary work stations will be set-up according to Alaska DHSS IT security standards. The general principles of measures to protect the confidentiality of data will be in effect, although may need to be adapted to the current circumstances, i.e., no locking offices, therefore records may need to be stored in locking portable filing cabinets.

L. Disposal of Confidential Data

Confidential data that are no longer needed shall be destroyed or archived, in accordance with the Department's record retention and disposal policies. Data will be destroyed as follows:

- Hard copy data will be shredded on-site prior to disposal.
- Confidential data stored on fixed and removable electronic media must be destroyed so that it cannot practicably be read or reconstructed. Data destruction techniques and procedures are made official by the DHSS Security Officer.
- Only after the above steps have occurred will material be placed in general office waste.

M. Notification of Breaches of Confidential Information

A breach of confidential data is the use of or disclosure of confidential data in violation of the SOE's Confidentiality Policy and Procedures. A workforce member who is responsible for a breach of confidentiality or who is aware of such a breach must immediately report it to his or her supervisor. The supervisor must report the breach to the SOE Section Chief (or ORP) who will notify the DSO. Failure to report a breach of confidentiality of which SOE staff has knowledge

may result in disciplinary action. SOE staff who make a report in good faith of a suspected or actual violation will not be retaliated against for making the report. However, reporting a breach of confidentiality in bad faith or for malicious reasons is grounds for disciplinary action.

Sub-grantees or contractors of SOE must also be required to report breaches; conditions of reporting must be included in all contracts/grantee documents.
There are three categories of breaches:

1. *Level I Breach*: The unintentional or careless violation of the SOE Confidentiality Policy and Procedures. Examples include, but are not limited to unintentionally:

- Discussing confidential information in public areas;
- Leaving a copy of client confidential data in a public area;
- Inadvertently faxing confidential data to the wrong fax number; and
- Leaving a computer unattended in a publicly accessible area with confidential data unsecured.

2. *Level II Breach*: The intentional access to or disclosure of confidential data that is inconsistent with the SOE Confidentiality Policy and Procedures but not for personal gain. Examples include, but are not limited to:

- Looking up the birth dates or addresses of friends or relatives;
- Disclosing confidential data to someone known to be without appropriate authorization;
- Reviewing a public personality's confidential data; and
- Accessing and reviewing confidential data out of curiosity or concern.

3. *Level III Breach*: Access to, review, or disclosure of confidential data for personal gain or malicious intent. Examples include, but are not limited to:

- Using or disclosing confidential data for commercial advantage or to improve one's position; and
- Using or disclosing confidential data for harassment or to spread gossip.

The nature of a breach will be formally documented in writing and may be placed in an employee's personnel file after review by the Program Manager and Section Chief. Breaches may be grounds for dismissal.

The State will take legal action for suspected or confirmed releases of data or PHI or additional protected information by former employees.

II. Summary Data Release Protocol

Requests for Alaska Section of Epidemiology (SOE) data should be submitted on an SOE Summary Data Request and Utilization Agreement Form (see Attachment 3).

The purpose of this protocol is to protect the confidentiality of patient information when SOE releases public health data to external stakeholders. Summary data are information grouped by age, sex, geographic area, or other variables and displayed so that individual patients cannot be directly identified. Summary data may be presented as a table, figure, diagram, chart, narrative, line list, or other similar format. Examples of summary data are the annual infectious disease reports, the sexually-transmitted disease summaries, and the HIV and AIDS summaries routinely published in the Epidemiology *Bulletin*. Summary data also may be produced on an *ad hoc* basis for various agencies and entities upon request.

In general, data will be reported to requestors in counts and not as rates. Rates may be requested; however, depending on the counts involved and the purpose for the data, the Section Chief may decide that rate reporting is not appropriate for certain situations. If researchers or other stakeholders would like more specific information about incident cases of a reportable condition than the rule of ones allows, such requests will be reviewed on a case-by-case basis, in consultation with the Epidemiology Section Chief, taking into consideration the potential risks and benefits of such disclosure.

Although summary data do not include confidential data such as a patient's name, summary data may lead to *de facto* identification of a particular person if the combination of age, sex, place of residence, or other variable(s) defines only one person — this is particularly important for communities with a relatively small population. Both numerators and denominators should be considered when releasing data; it is never acceptable to release summary data that could reasonably be expected to lead to the identification of an individual patient through indirect means. Because of this potential for a breach of confidentiality, great caution must be exercised in the distribution and use of such data.

Before summary data are released, SOE program managers must carefully review and approve the data format to ensure that the release is consistent with the guidelines in this protocol. If there is a question as to whether the release is consistent with the guidelines in this protocol, program managers should consult with the Section Chief prior to granting approval. In some circumstances, the guidelines might not be sufficiently restrictive to prevent identification of individuals because of the distribution of the health condition or the population affected. In those instances, parameters more restrictive than the general guidelines should be instituted before data can be released. Program Managers are responsible for maintaining records of data requests and subsequent data releases.

In certain situations, a limited data set (LDS) may be requested and subsequently released by SOE following review and approval by both the appropriate Program Manager and the Section Chief. See Section G of the SOE Confidentiality Policies and Procedures document for more information about LDS. Record-level data involving personal identifiers will not generally be released except by formal application and approval by the Section Chief. Such data will be released to researchers or public health partners only for approved research and surveillance activities with a signed data

sharing agreement and/or a signed memorandum of understanding, per the Section Chief's discretion.

Overview of General Algorithm/Process

1. Apply the scoring schema from Table 1, Alaska "Rule of Ones" (see below).
   - Adjust variables as appropriate to obtain a score ≥1.

2. Ensure that all cells with a numerator value <5 are evaluated for possible confidentiality concerns. Suppress data in these cells or aggregate to generate larger cell sizes as appropriate.

3. Ensure that all cells with a denominator of <500 people are evaluated for possible confidentiality concerns.
   - Avoid sub-stratification if cell denominators are <250 people.

4. Review final data to be released to ensure that users cannot derive confidential information through a process of subtraction.

5. Ensure that standard caveats about the limitations or generalizability of the data accompany the data to the requestor, including caveats regarding stability of rates calculated with small numbers, etc.

Alaska "Rule of Ones"

Table 1 is adapted from the New Hampshire Division of Public Health Services[1] and involves the "Rule of Ones" for six different characteristics or variables described below. Each characteristic is given a value; the product of the six values must be ≥1 to allow for acceptable release of data. Details are given about what constitutes a value of one, and how to adjust that value up or down based on the granularity of the characteristic. In addition, regardless of adjustments, minimum and maximum values are given for each characteristic.

Notes:

- For *annual* state-wide reports of common diseases, sex, race, and age-group (5-year intervals) will usually be given and may be given for certain rare diseases.
- The "Rules of Ones" applies mainly to counts of disease; however, the general guidelines also apply to the subsequent calculation of rates, i.e., avoiding calculation when the numerator is <5 or the denominator is <500.

a. **Incidence rate:** What is the disease of interest? More common diseases (e.g., chlamydia) are assigned a value of 1; less common diseases (e.g., botulism) may be discounted, per the discretion of the Section Chief. As a general rule of thumb, if the incidence of the disease is <5 cases per 100,000 population per year, use 1/2.
   Minimum value: 1/2 Maximum value: 1

[1]New Hampshire Division of Public Health Services, Health Statistics and Data Management Section. Guidelines for the Public Release of Public Health Data. September 2008. Available at: http://www.dhhs.nh.gov/dphs/hsdm/documents/publichealthdata.pdf.

b. **Population size:** In what region or population strata will the data be provided (total denominator across all age and sex groups)? A population or strata of 5,000 is assigned a value of 1; therefore, populations/strata of 10,000 have a value of 2 and populations/strata with 2,500 have a value of 1/2.

- Use the current Alaska Population Overview as the reference for the population size in a region http://live.laborstats.alaska.gov/pop/popestpub.cfm. Note that the size of boroughs and census areas range from <500 to ~300,000 people.
- Community sizes should be rounded down to the nearest 500.
- See #3 in the overview above for communities with populations <500 people.

Minimum value: 1/10 Maximum value: 50, for any population 250,000+

c. **Time interval of data:** In what unit of time, months or years, will the data be provided? A year is assigned a value of 1; a single month has a value of 1/12. Data will not be provided in intervals smaller than 1 month.
Minimum value: 1/12 Maximum value: 5, for any interval ≥5 years

d. **Age-group:** In what number of years will age-groups be provided? A 5-year age-group is assigned a value of 1; therefore, a 10-year age-group has a value of 2. Note that data with age-groupings of less than 5 years will generally not be provided. Age-grouping must be divisible by five; and map to standard intervals if possible, i.e., 0–4 years of age instead of 1–5 years of age.
Minimum value: 1 Maximum value: 5, for ≥25-year age-groups

e. **Sex distribution:** Will data be stratified by sex? If data are not stratified by sex, a value of 1 is assigned. If data are stratified by sex, a value of 1/2 is assigned.
Minimum value: 1/2 Maximum value: 1

f. **Race distribution:** Will data be stratified by race? If data are not stratified by race, a value of 1 is assigned. If data are stratified by all four race groupings (e.g., white, American Indian/Alaska Native [AI/AN], black, Asian/Pacific Islander), value of 1/8 is assigned. If data are stratified by AI/AN and non-AI/AN only, a value of 1/5 is assigned.
Minimum value: 1/8 Maximum value: 1

Table 1. Scoring of Criteria Used to Evaluate Acceptable Summary Data Releases.

Characteristic	Standard Denomination	Score
a. Incidence rate	Common	1
b. Population size	5,000	1
c. Time interval	1 year	1
d. Age-group	5-year	1
e. Sex distribution	All	1
f. Race distribution	All	1
Product (a)(b)(c)(d)(e)(f)	**=**	**1**

Example A. Is it acceptable to release 2008 data for chlamydia in Palmer (2009 population 5,500) by 5-year age-groups?

Characteristic	Standard Denomination	Score	Example A
a. Incidence rate	Common	1	Chlamydia = 1
b. Population size	5,000	1	Palmer = 1
c. Time interval	1 year	1	2008 = 1
d. Age-group	5-year	1	5-year = 1
e. Sex distribution	All	1	All = 1
f. Race distribution	All	1	All = 1
Product (a)(b)(c)(d)(e)(f)	**=**		**1**

Answer: Score ≥1; this is acceptable.

Example B. Is it acceptable to release 2008 data for chlamydia in Palmer (2009 population 5,500) by 5-year age-group and by sex?

Characteristic	Standard Denomination	Standard Score	Example B
a. Incidence rate	Common	1	Chlamydia = 1
b. Population size	5,000	1	Palmer = 1
c. Time interval	1 year	1	2008 = 1
d. Age-group	5-year	1	5-year = 1
e. Sex distribution	All	1	M vs. F = 1/2
f. Race distribution	All	1	All = 1
Product (a)(b)(c)(d)(e)(f)	**=**		**1/2**

Answer: Score <1; this is not acceptable.

Example C. But, what if age-group was aggregated to be 10-year increments?

Characteristic	Standard Denomination	Standard Score	Example C
a. Incidence rate	Common	1	Chlamydia = 1
b. Population size	5,000	1	Palmer = 1
c. Time interval	1 year	1	2008 = 1
d. Age-group	5-year	1	10-year = 2
e. Sex distribution	All	1	M vs F = 1/2
f. Race distribution	All	1	All = 1
Product (a)(b)(c)(d)(e)(f)	**=**		**1**

Answer: Score ≥1; this is acceptable.

Example D. Is it acceptable to release 2008 data for botulism by sex, race, and 5-year age-group for the entire state?

Characteristic	Standard Denomination	Standard Score	Example D
a. Incidence rate	Common	1	Botulism = 1/2
b. Population size	5,000	1	AK = 50
c. Time interval	1 year	1	2008 = 1
d. Age-group	5-year	1	5-year = 1
e. Sex distribution	All	1	M vs F = 1/2
f. Race distribution	All	1	4 groups = 1/8
Product (a)(b)(c)(d)(e)(f)	**=**		**50/32 (1.6)**

Answer: Score ≥1; this is acceptable.

Example E. Is it acceptable to release 2008 data for gonorrhea by sex, race, and 5-year age-group for Palmer (2009 population 5,500)?

Characteristic	Standard Denomination	Standard Score	Example D
a. Incidence rate	Common	1	Gonorrhea = 1
b. Population size	5,000	1	Palmer = 1
c. Time interval	1 year	1	2008 = 1
d. Age-group	5-year	1	5-year = 1
e. Sex distribution	All	1	M vs. F = 1/2
f. Race distribution	All	1	4 races = 1/8
Product (a)(b)(c)(d)(e)(f)	**=**		**1/16**

Answer: Score <1; this is not acceptable.

Example F. Is it acceptable to release data for gonorrhea by sex, AI/AN race for Palmer by increasing age-group to 10-year increments and looking for 5 years of data?

Characteristic	Standard Denomination	Standard Score	Example D
a. Incidence rate	Common	1	Gonorrhea = 1
b. Population size	5,000	1	Palmer = 1
c. Time interval	1 year	1	2006-10 = 5
d. Age-group	5-year	1	10-year = 2
e. Sex distribution	All	1	M vs F = 1/2
f. Race distribution	All	1	AI/AN vs non = 1/5
Product (a)(b)(c)(d)(e)(f)	**=**		**1**

Answer: Score ≥1; this is acceptable.

Example G. How many variables could you release for gonorrhea cases in a small community, i.e., Fort Yukon (2009 population 585)?

Characteristic	Standard Denomination	Standard Score	Example D
a. Incidence rate	Common	1	Gonorrhea = 1
b. Population size	5,000	1	Fort Yukon = 1/10
c. Time interval	1 year	1	2001-5 = 5
d. Age-group	5-year	1	10-year = 2
e. Sex distribution	All	1	All = 1
f. Race distribution	All	1	All = 1
Product (a)(b)(c)(d)(e)(f)	**=**		**1**

Answer: To have an acceptable release of data for a common disease in Fort Yukon, you would need to use a 5-year period and release age data in 10 year intervals. Stratification by sex would only be possible if the age-group interval was expanded to ALL (product score =25/20). Stratification by race would not be possible.

ATTACHMENT 1 – Section of Epidemiology Confidentiality Agreement

By signing this Confidentiality Agreement, I state the following to be true:

1. I have read the current Section of Epidemiology's (SOE) Confidentiality Policies and Procedures and fully understand my responsibility to implement SOE's confidentiality policies and procedures regarding confidential information.

2. I agree to observe the confidentiality policies and procedures of the Section of Epidemiology.

3. I realize I have both an ethical and legal obligation to protect the right of privacy of the persons whose records the Section maintains.

4. I will not relate or discuss any information which identifies a specific patient, physician or hospital with anyone other than – Section staff, the source from which the information originated, health care providers involved in the patient's care, or other persons as needed to carry out the Section's responsibilities.

5. I understand that any confidential information I receive in the course of my employment in the Section will remain confidential after I terminate employment in the Section.

6. I understand that the misuse of confidential information could be the basis for an ethics violation under AS 39.52.140 or a criminal prosecution under AS 11.56.860.

7. I understand that failure to observe these confidentiality policies will be grounds for immediate disciplinary action and could constitute justification for termination.

Name: _____

Title: _____

Signature _____ Date:_____

<u>Supervisor</u>

Name: _____

Title: _____

Signature: _____ Date:_____