DESCRIPTION:

The HIPAA Security Rule focuses on the safeguarding of Electronic Protected Health Information (ePHI). The primary goal of the Security Rule is to protect the confidentiality, integrity and availability of ePHI.

All employees are required to follow the Washoe County Information Security Policy located at https://www.washoecounty.us/humanresources/files/hrfiles/TS_%20Security_Policy_8_2005.pdf and complete the HIPAA training every two years from http://www.webnettraining.com.

1) **Employees are not to use unauthorized personal mobile devices (laptops, smartphones, external drives etc.) to store, access, send or process ePHI or confidential data unless: they are password protected; auto logoff or password protected screen savers are used; and encryption of stored data by acceptable encryption software approved by a Business Technologist.**
2) Access to ePHI is granted only to individuals authorized.
3) Northern Nevada Public Health (NNPH) computer equipment should only be used for authorized purposes in the pursuit of accomplishing your specific duties.
4) Disclosure of ePHI via electronic means is strictly forbidden without appropriate authorization.
5) Installation of software without prior approval is prohibited.
6) Do not use computer equipment to engage in any activity that is in violation of the NNPH policies and procedures or is illegal under local, state, federal, or international law.
7) All NNPH computer systems are subject to audit.
8) All computers should be manually locked, locked via a screen saver, or logged off when unattended.
9) Computer screens with ePHI or confidential data should not be viewable by the public.
10) Shut down your computer when you leave for an extended period of time.
11) You must access NNPH information utilizing your username and password!
12) Password sharing is not permitted.
13) Maintain your password in a secure and confidential manner.
14) Let your supervisor know promptly if an electronic breach occurs that may have decreased the privacy of client health information. Upon resignation, termination or transfer of employee all NNPH network and PC access is terminated, all ePHI and computer equipment should be retrieved.

PROTOCOLS

Roles and Responsibilities

1. Overall Responsible Party (ORP)
   For NNPH the Administrative Health Services Officer serves as the ORP. Within individual divisions the Directors serve in this role. The ORP signs applicable grant documentation pertaining to surveillance, prevention, and health care on a yearly basis, and certifies appropriate handling and maintenance of security measures. Additionally, the position reviews current security and confidentiality protocols as well as assessment of evolving technology in collaboration with Washoe County's Technology Services. The ORP ensures security and confidentiality of relevant information and establishment of appropriate measures to ensure proper delivery of revised security and/or confidentiality information to the Division's users.

2. Site Security Officer (SSO)
   Program Supervisors in the specific programs operate in the role of SSO for their program area. If the Program Supervisors are not available, the appropriate Program Coordinator becomes the interim SSO.

   All security-related issues and/or concerns for each program shall be reported immediately to this position. This position maintains oversight and signature authority of security-related accessibility to the Division's physical site locations, as well as database(s) and IT network-related accessibility. The SSO also maintains the Division's oversight of annual staff security training completion and associated databases.

3. HIPAA Privacy and Security Staff
   Overall HIPAA privacy and security activities are provided through NNPH's Administrative Health Services Division. The Administrative Health Services Officer serves as the HIPAA Privacy Officer. All HIPAA and Personal Health Information (PHI) related protocols, issues, and partnerships with any outside vendor or community partner are reviewed by the Assistant District Attorney assigned to represent NNPH.

4. Program Staff
   All program staff, contractors, and volunteers are expected to maintain security and confidentiality of all PHI as a requirement of their positions and to safeguard the public's trust. As public health professionals working for a government agency or people connected to these programs, we depend upon the cooperation of the public and of the medical community to help us to accomplish our mission. Any breach of confidentiality, whether deliberate or inadvertent, could jeopardize this cooperation and seriously damage our ability to protect public health. Therefore, any breach in confidentiality would be considered grounds for termination. Protection of this trust and responsibility carries into challenging any situation that is a potential breach of security to safeguard data and PHI. These situations may include questioning colleagues and co-workers if a situation risks a potential breach of security.

   Employees, interns, contractors, and volunteers will not divulge in any conversations with any unauthorized person or persons including, but not limited to; friends,

family, acquaintances, or the news media any confidential information obtained as a result of their affiliation with NNPH.

5. New Hires, Interns, Contractors, and Volunteers
   Any new hires or transfers, student interns, contractors, or volunteers with NNPH will be required to read the confidentiality policy. The new employee, intern, contractor or volunteer and the designee will sign a statement of confidentiality before the person is assigned duties that expose him/her to confidential material which will be retained in the person's personnel file.

Annual Training

All employees are required to complete HIPAA training every two years. Staff within CCHS may be required to complete additional training yearly. Documentation of successful completion of this training will be retained in the employee's personnel file.

WORKSPACE

1. Access
   Computer(s) containing electronic surveillance data must not be left unattended. Authorized staff have access to the common work areas; however, only appropriate staff have access to data systems and/or file rooms containing hard copy records.

2. Keys
   Keys to doors, desks, and cabinets shall be issued only to employees who need these keys to perform their duties. The issuance of door keys is to be documented. Employees are responsible for keeping all keys, desks, and cabinets secure. Employees are not to make any unauthorized copies or loan or give their keys to any unauthorized individuals. Lost keys are to be reported to a supervisor immediately.

   When employment is terminated, the departing employee will turn in all keys. Return of the keys is to be documented and kept in the departing employee's personnel file. At the discretion of the supervisor or ORP, any lock may be changed and keys for that lock reissued.

3. Photocopying, Printing and Photography in Work Areas

There should be no printing or copying of materials with identifying information on general use or non-secure printers or copiers. All printing/copying of such documentation shall occur within the confines of a secure office or administrative area and the print/copy job shall be removed immediately upon completion. Any unnecessary copies shall be shredded immediately, as well as originals once their use is obsolete. Only the mandatory number of copies of such information shall be copied/printed. Any extra or test copies shall be shredded immediately upon completion.

Instances requiring the use of copiers in non-secure areas may arise; however, these circumstances should be kept to an absolute minimum and the copier/printer shall not be left unattended.

Users should not take photographs within the confines of any of the NNPH's secured areas where data is visible to ensure printed or computerized information relative to PHI is not inadvertently included in such photos.

4. Windows
   Rooms containing PHI must not be easily accessible by a window. Window access is defined as having a window that would allow easy entry into a room containing sensitive data. A window with access may be one that opens and is on the first floor of the building. If the office has windows, they must be secured.

5. Cleaning and Building Maintenance Access to Areas
   Access to work areas by cleaning crews and other building maintenance personnel, outside of the contracted janitorial service, must be granted only during hours when personnel are available for escort. Keys to offices containing confidential data, documents, computers, hard drives, etc. are to be different from the usual office keys and only be used to open these offices.

   In addition, the contracted janitorial service contract is for a high-security setting. Background checks are required. Fidelity Bonds are carried by each individual with $5,000,000 per occurrence assigned to Washoe County.

6. Visitors
   When it is necessary for non-employees to enter the work area, the employee who invited the visitor to his/her office is responsible for escorting and making sure that the visitor is not exposed to confidential information. Employees are to challenge anyone encountered in a work area that is unescorted and not recognized as a member of the office staff.

DATA COLLECTION, USE, AND STORAGE

1. Authorized Data & Database Usage

User accounts for confidential databases are maintained by the NNPH and Washoe County's designated Business Technologist (BT) within NNPH Administrative Health Services and Washoe County Technology Services staff. BT staff works with program specific SSOs and Technology Services to ensure network security and access. All security groups and database access are controlled by a "need-to-know" basis, limiting unnecessary access to PHI.

SSOs are responsible for granting or restricting access to databases. User accounts shall be deleted or deactivated immediately upon termination of employment or a change in duties and responsibilities. Additionally, the SSO is responsible for maintain an updated list of all persons (including Technology Services staff, student interns, and contractors) with authorized access to surveillance data and include the date the person completed the annual security training (see Security Training).

Personnel outside of NNPH's Sexual Health and TB programs may gain access to confidential information only if the request for such information 1) has been authorized in writing by the ORP, 2) is deemed an expressed and justifiable public health need, 3) does not compromise or impede surveillance activities, and 4) does not negatively affect public perception of confidentiality of the surveillance system.

Employees that use databases containing client level data (PHI) must log out of the database before leaving their desk. In addition, computers that have the capability to access secure databases must be equipped with a password protected screensaver that activates after no more than ten (10) minutes of inactivity per Washoe County Tech Services security policy.

2. Postal/Mailing Services

Incoming

Incoming mail marked confidential shall only be opened by the intended recipient and SSO should ensure that policies are in place to keep mail from being opened in mail rooms or by other staff.

Outgoing

Confidential information should be mailed in a manner that does not allow information to be revealed without opening the envelope. The number of documents per envelope shall be kept to a minimum. All such information shall be put inside colored paper and be folded towards the inside of the documentation prior to placement inside the envelope. Envelopes shall be taped shut as added security. All such confidential information mailed from NNPH shall be marked "*Confidential".* Other methods that provide delivery tracking can also be used whenever feasible, i.e., certified mail.

When mailing confidential information, use the following procedure:

- Confidential documents are to be folded inside colored paper to eliminate any chance that the document could be read through the envelope.
- The envelope is to be stamped or in some way identified as "confidential".
- The address is to be checked to make sure it is correct.
- The envelope is to be sealed and taped shut with reinforced tape.
- Confidential mail is not to be entrusted into the care of anyone who is not an employee of Northern Nevada Public Health or Mail Room personnel of Washoe County.

3. Mail Slots/In-baskets

Confidential inter-office mail or faxes should be placed in a brown manila envelope, sealed and hand delivered. If that person is not available to receive the envelope, it may be placed in the recipients' mail slot. The envelope is not to be left in the hanging basket on an office door.

4. Telephone Exchange of Confidential Information

The exchanges of confidential information between program personnel at NNPH and with personnel within other health jurisdictions, inside of or outside of Nevada, are part of normal activities. Confidential information will not be left on voice mail unless it is specifically identified as a confidential message system.

5. Portable Devices

   Laptops and other portable devices that receive or store information with personal identifiers must incorporate the use of encryption software. Information must be encrypted and stored on an external storage device or on the laptop's removable hard drive. The external storage device or hard drive containing the data must be separated from the laptop and held securely when not in use. The decryption key must not be on the laptop. Other portable devices without removable or external storage components must employ the use of encryption software that meets federal standards.

   All removable or external storage devices containing personal identifiers must: (1) include only the minimum amount of information necessary to accomplish assigned tasks, (2) be encrypted or stored under lock and key when not in use, and (3) with the exception of devices used for backups, devices should be sanitized immediately following a given task. Before any device containing sensitive data is taken out of the secured area, the data must be encrypted. Methods for sanitizing a storage device must ensure that the data cannot be retrievable using Undelete or other data retrieval software. Hard disks that contain identifying information must be sanitized or destroyed before computers are labeled as excess or surplus, reassigned, or before they are sent off-site for repair.

6. E-Mail

   Confidential information can be emailed via internal computer network to appropriate program staff; however, no emails to external addresses are allowed unless they are encrypted using Washoe County Technology Services specified system. Encrypted email provided to external entities must follow this policy. Staff must place #secure# into the subject line of the email to access the encryption system.

7. Fax

   Confidential information may be faxed only when the following conditions are met:
   - The receiving FAX machine is known to be in a secure location.
   - The authorized person receiving the document is expecting the transmission and standing by to receive it.
   - Extra care is taken to prevent confidential information from inadvertently being transmitted to the wrong place.
   - Confidential documents are not to be left unattended and are to be removed from the FAX tray immediately after transmission.

8. NNPH Provided Cell Phones

   The following actions will help ensure confidentiality:
   - When the cell phone is not in use, it will be stored in a staff person's desk.
   - The phone will be turned off and locked in a desk or file cabinet at the end of each day.
   - Any private text communications will be deleted once the business with the client has been completed.
   - Texts will not be backed up to another system.

9. Online Client Searches
   Employing online searches for client location information can be used after other routine sources of receiving information have been exhausted. A minimum amount of information should be used to conduct the searches to limit the amount of PHI that is kept in search archives. In addition, social security numbers should not be used for searches, although the social security number may be revealed in the search output provided by the database.

10. Interdivisional Data Sharing
    Identifying information from Division databases may be shared/matched only after review and approval by the ORP. The ORP will limit such activities to other systems that demonstrate a justifiable need for the data or provide enhanced information for public health planning. The decision to allow such activity will also be weighed against the benefits and risks of allowing access to specific data and, as necessary, upon certification that the level of security established by the other registry is at least equivalent to the standards described in this document. The final decision regarding the sharing of registry data and data matches remains the sole discretion and responsibility of the ORP.

11. Data Release Procedures
    To ensure patient confidentiality, the Division will ensure data release procedures incorporate numerator and denominator rules, as appropriate, in a consistent manner that provides for reasonable public health data access.

    De-identification of client level data is the preferred course before releasing such data for analysis, research, or other purposes, if approved by the SSO or ORP. Access to any surveillance information containing names, or multiple variables considered as PHI by HIPAA, for research purposes (that is, for other than routine surveillance purposes) must be contingent on a well demonstrated need, Institutional Review Board (IRB) approval, if necessary, receipt of written request and approval by the SSO and ORP. All such requests must be submitted in writing to the SSO who will assess such data requests, based on public health relevance, business need and associated data confidentiality assurances. Access to surveillance data or information without names for research purposes beyond routine surveillance may still require IRB approval.

    Prior to granting access to the data, the requestor must sign a statement certifying that he or she will comply with the security and confidentiality standards of NNPH. Signing this statement indicates that the requestor (1) understands the penalties for unauthorized disclosure, (2) assures that the data will be stored in a secured area, (3) agrees to sanitize or destroy any files, diskettes, or other storage devices that contained the data set when the research project is completed and (4) agrees to provide written notice of data destruction.

    Aggregate surveillance data are available to the public. The Program will confer with NNPH's Division of Epidemiology and Public Health Preparedness when data suppression may be utilized due to small data sets.

The privacy of medical records is protected under NRS. 449.720. Additional protections for communicable disease records are found in NRS 441A.220, NRS 441A.230, NAC 441A.300 and NAC 441A.305.

12. Non-Public Health Access

Requests to access surveillance information or data for non-public health purposes, such as litigation, discovery, or court order, must be reviewed by the ORP with the appropriate program area's legal counsel. After that approval, access to the data shall be granted only to the extent required by law. All subpoenas and other legal papers requesting the disclosure of confidential information served to any work unit within the programs shall be referred to the ORP for consultation with the assigned Washoe County District Attorney.

13. Data Transfers

Data transfers must be encrypted when any moderately or highly sensitive files, any moderately or highly critical information, or any limited access/proprietary information is being transmitted either electronically or physically. Such data should be sent via the Secure Data Network (SDN) or other approved data network.

14. Security of Records Taken Offsite

Except when necessary for the purposes of field work (such as detention center visits, off-site testing, disease investigation activities) all confidential documents, computer hardware and software containing confidential information are not to be removed from the premises or the immediate control of NNPH. All confidential files are to be kept locked and secure after hours or whenever the office is closed.

Information taken from NNPH for fieldwork must be limited and kept secure. When it is necessary to carry confidential documents in the field, they are to be kept secure at all times in a locked briefcase in a locked car or preferably in a locked trunk. Surveillance work material should be returned to the office and secured at the end of the workday.

The SSO, Program Supervisor, or ORP may grant exceptions if storage security can be maintained by the staff person.

When identifying information is taken from the secured area and included online lists, supporting notes, or other hard-copy format, these documents must contain only the minimum amount of information necessary for completing a given task and, where possible, must be coded to disguise any term that could easily be associated with disease status.

Before taking any storage media containing sensitive data out of a secured area, the data must be encrypted. Methods for sanitizing storage media must ensure that the data cannot be retrievable using undelete or other data retrieval software.

15. Shredding of Documents

As appropriate, confidential documents are to be shredded by a crosscut shredder or locked shredder before discarded in the trash.

RECORD RETENTION

All confidential records are stored within secured file rooms or cabinets accessible only by authorized users. Records must be kept according to approved retention guidance and labeled, boxed, and stored in an undisclosed secure location (Refer to NNPH's Record Retention Policy). Only authorized users may have access to document storage locations for review, retrieval, and destruction of such records.

Records meeting the requirement for destruction shall be shredded onsite by authorized users only. Bulk record destruction is provided by Washoe County Records Management staff at the designated, secure Washoe County records storage facility. Records of such activities shall be maintained by the Administrative Health Services Officer and Washoe County Community Services Department, with the SSO having access to the destruction records.

BREACHES OF CONFIDENTIALITY

Any employee who becomes aware of a breach of confidentiality or a potential breach of confidentiality will immediately take appropriate corrective action. The person directly responsible for the security of the information (SSO), Program Supervisor, and the ORP will be notified. An immediate investigation will follow.

If a breach is determined to have resulted in the release of private information about one or more individuals, it must be reported to the Administrative Health Services Officer.

NONDISCLOSURE STATEMENT FOR EMPLOYEES, INTERNS, CONTRACTORS, AND VOLUNTEERS

Employees are asked to sign a Nondisclosure Statement. The signed Nondisclosure Statement will be kept in the employee's personnel file.

U***pdated 5/23/24***