North Dakota Sexually Transmitted and Bloodborne Pathogens Security and Confidentiality Policy

This policy outlines the confidentiality and security measures for the North Dakota Department of Health and Human Services, Disease Control and Forensic Pathology Section.

Date of Last Review: 02/06/2025

NORTH Dakota Be Legendary. | Health & Human Services

TABLE OF CONTENTS

1.0 PROGRAM POLICIES AND RESPONSIBLITIES

The North Dakota Department of Health and Human Services, Disease Control & Forensic Pathology Section (HHS, DC) Security and *Confidentiality Policy was developed to comply with the Centers for Disease Control and* Prevention (CDC) "Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action." This policy applies to all employees, contractors and visitors with access to protected health information (PHI).

This document will be reviewed and updated as needed and/or annually. All staff will be informed of the changes and the location of the most recent policy.

OVERALL RESPONSIBLE PARTY

The director of the Disease Control and Forensic Pathology Section, Kirby Kruger, is designated the overall responsible person (ORP). The ORP is responsible for determining how PHI will be protected when it is collected, stored, analyzed, released, and disposed (i.e. managed). The ORP must certify that the security standards in this policy are in place and all program requirements are met, as stipulated by the Centers for Disease Control and Prevention (CDC) cooperative agreements.

ACCESS AND ROLES

Highly confidential PHI will be provided only to employees and approved visitors on a need-to-know basis, as determined by the ORP and the Sexually Transmitted and Bloodborne Pathogens (STBP) Unit Director in order to conduct necessary work. This information will only be provided after the employee or approved visitor has completed the security and confidentiality training and has signed the confidentiality oath. The definition of highly confidential PHI in this instance includes full view access to HIV.STD.TB or Viral Hepatitis case reports that include information detailing the disease status, ongoing case management and personally identifying information of cases. The list of roles, system access and level can be found in Appendix A.

SECURITY BREACH

Authorized personnel, by signing the confidentiality oath, agree to accept responsibility to challenge unauthorized users of HIV data, to report suspected security breaches, and to be responsible in securing their workstations, passwords and keys.

All breaches of confidentiality and security will be immediately reported to the STBP program manager and ORP for prompt investigation. The investigation will also include the HHS HIPAA Privacy officer and Security and Transactions Officer dependent on the type of breach that occurred. The ORP follow the **Breach of Confidentiality Response Policy** will decide if legal consultation is necessary in a case by case basis. After the investigation is complete, updates and changes will be made to the security and confidentiality policy to prevent future breaches. A breach that results in the release of highly confidential HIV information about one or more individuals should be reported immediately to the team leader of the Reporting and Analysis Section, Surveillance Branch, DHAP-SE, NCHSTP, CDC.

Documentation of the breach will be maintained by the ORP describing the investigation findings and corrective actions taken in hard copy located in a secure location at the Disease Control & Forensic

Pathology Section. The ORP will determine whether the breach warrants report to law enforcement agencies.

A breach in confidentiality may be grounds for termination of employment and prosecution under state statute NDCC 23-07.5-08. The statute sets a penalty of a Class C felony with a $5,000 fine and/or imprisonment for up to five years for each breach of confidentiality.

A breach is defined as, "the disclosure of confidential information to: any person outside the HHS, DC who lacks legal right of access, or to HHS DC employees who do not need access to the information for a completion of assigned duties."

SECURITY AND CONFIDENTALITY TRAINING

New Employees

All newly hired staff members must receive and pass Security and Confidentiality training within one week of hire. All newly hired staff must sign a confidentiality agreement which will be kept on file by ORP within one week of hire. All HHS, DC staff members must take departmental trainings required on HIPAA as required by the HHS. Documentation of this training will be kept in the employee's personnel file.

All HHS, DC Employees

All HHS, DC staff must receive annual Security and Confidentiality Training. Training will be based on this document and will cover:

- Personal responsibilities
- Procedures for ensuring physical security of PHI
- Policies and procedures for data sharing
- Procedures for reporting and responding to security breaches.
- Review of relevant laws and regulations.

After training, all staff will resign a confidentiality agreement and verify that they attended the annual training. This document will be kept on file by the ORP.

HHS Staff (Non-HHS, DC)

All HHS (Non-HHS, DC) staff who have access to PHI shall receive annual security and confidentiality training. Training will be based on this document and will cover:

- Personal responsibilities
- Procedures for ensuring physical security of PHI
- Policies and procedures for data sharing
- Procedures for reporting and responding to security breaches.
- Review of relevant laws and regulations.

After training, all staff will re-sign a confidentiality agreement and verify that they attended the annual training. This document will be kept on file by the ORP.

External Partners

All external partners will sign a confidentiality agreement which will be kept on file by the ORP.

All external partners will receive program specific security and confidentiality training annually.

DISASTER RECOVERY PLAN

The disaster recovery plan for HHS, or Continuity of Operations Plan (COOP), provides the framework for the Department to restore essential functions in the event of an emergency that affects operations. The COOP provides information on how the Department will sustain the capability to perform essential functions during and after disruption in internal operations whether caused by severe weather, other natural and man-made disasters, or malevolent attack. This plan will be used only in the event it is needed. The COOP plan is distributed and/or made accessible electronically to all Department staff, based on specific program area processes. Training is provided to personnel with identified responsibilities. The COOP is reviewed annually and updated as needed.

2.0 DATA COLLECTION & USE

Data collected by HHS, DC programs are for the purpose of public health related to HIV/AIDS, STI, TB, VPDs and other reportable conditions. Public health purposes include disease surveillance, disease and premature death prevention, or health promotion among members of a community through activities such as:

- Assessing the health needs and health status of a community through public health surveillance and epidemiology
- Developing public health policy
- Responding to public health needs and emergencies
- Evaluating public health programs
- Treatment

Before implementing new data collection processes, programs shall specify minimum data elements necessary and consider whether collection and use of personally identifiable data is necessary to achieve the public health goal.

The minimum information requirement will vary based on the activity. When considering a new data collection, consider the following:

- Specify minimum data elements, and include only the information needed to achieve the public health goal(s) including required reporting data elements.
- Minimize or avoid collecting information because it might be of use later or because it is easily accessible.
- Refer to similar high-quality data collection efforts or data-sharing activities with proven success.
- Avoid unnecessary retention or creation of multiple data collection or data management systems.

The use of identifiable data must be approved by the ORP first, then obtain internal review board (IRB) approval, and the signing of a confidentiality agreement regarding the rules of access and final disposition of the information. The use of non-identifiable data for research is generally permissible, but might still require IRB approval, depending on the amount and the type of data requested. Consultation on whether or not a project is practice vs. research, subject to human subject regulations and with the IRB chair to determine if IRB approval is necessary.

3.0 DATA SHARING & USE

This section applies to the sharing of data with other like public health programs that require access to data for a related public health function. The ORP must approve any data sharing or data release.

Prior to sharing PHI, the ORP and appropriate program staff must assess:

- Is access necessary to achieve a specified public health function?
- Have all alternatives to sharing such data been explored?
- Is the proposed use within the scope of the data release policy and for legitimate public health purpose?

DATA SHARING

Data sharing outside HHS, DC

For individual cases, the sharing highly confidential and confidential PHI with respective out-of-state programs will be conducted by division directors or surveillance coordinators. Comparison of disease registries will be accomplished by division directors or surveillance coordinators for the benefit of the respective program or the benefit of other public health programs.

For all other situations where data sharing (datasets) is requested, written agreements must be established prior to data sharing. The written agreement will be developed and approved by the ORP. This includes data sharing between public health use as well as non-public health use.

- Memorandum of Agreement (MOA)—internal; other programs within the HHS
- Data Sharing Agreement (DSA)—external; Local Health Departments, Universities, NGO, research, etc.

Databases containing identifiable information will not be released to any third party for research or special studies unless the need for names is clearly demonstrated in writing, and approved by the institutional review board, the ORP, program managers and the state health officer. If the request is approved, the requesting party must read and understand the security and confidentiality policy, and sign the confidentiality oath and a memorandum of understanding, which describes compliance regarding rules of access and final disposition of the information.

Access to PHI or data for non-public health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law and with approval by the ORP.

Access to PHI or data for public health purposes, such as case management, disease management and other purposes for the health and benefit of the individual will require those individuals to be authorized to have access to that information by the ORP and will be carefully managed to not impede public health activities or affect the perception of confidentiality. All persons with access to disease registries must comply with these S & C guidelines and must attest annually to uphold them.

All data released under this policy that contains PHI will be assessed for quality before dissemination by the Sexually Transmitted and Bloodborne Pathogens Unit Director.

This policy does not apply to summary data or data that does not contain PHI. Data will be released in summary to stakeholders according to the HHS policy on data release.

Data Sharing within HHS, DC

Information about reportable conditions can be exchanged freely between all programs within HHS, DC for whom staff are authorized to conduct surveillance for those conditions as necessary for public health purposes. Staff that will have access to these data will have had S&C training and have filed a current confidentiality oath.

DATA RELEASE

Surveillance data will be published and posted on the HHS, DC website on an as needed basis. This would include data published in tables, graphs and annual reports.

Surveillance data will not be released in cell sizes less than or equal to 5. Exceptions to this release will be evaluated by the program manager and ORP on a case-by-case basis to ensure that the data are not identifiable.

The release of rates of certain conditions should take into account situations where there are small denominators in a demographics subgroup. Typically, a release of a rate among a particular subgroup or geographic area should have a numerator of 5 or more and a denominator of 100 or more. Situations where this is not the case should be evaluated by the unit director and ORP before released.

Caution should be used when analyzing categories where there can be inadvertent identification of individuals. Examples include:

- Infrequent race/ethnicity categories
- Transgender or other infrequent gender categories
- Small or single-year age groups
- Infrequent risk behavior categories (e.g., perinatal, needlestick)
- Small geographic areas.

The use of GIS mapping can be used with precaution. Addresses and their equivalent latitudes and longitudes and identifies must be safeguarded in the same method names are safeguarded. Results of GIS analyses must not be released in the form of a spot map that identifies a specific geographic location, such as an address that could be identifying. Care must be used when using demographics or risk behavioral subsets to ensure that individuals cannot be identified.

Prior to the release of any product containing surveillance data must be approved by the unit director and/or the ORP.

LEGAL AUTHORITY FOR DATA SHARING AND RELEASE

The North Dakota Department of Health and Human Services is bound by NDCC (23-07-02.2) for personally identifiable information (PHI) which states: A report required by section 23-07-02.1 and held by the state department of health and human services is confidential information. The information may

not be disclosed, shared with any agency or institution, or made public, upon subpoena, search warrant, discovery proceedings, or otherwise, except that:

1. Disclosure may be made of medical or epidemiological information for statistical purposes in a manner such that no individual person can be identified;
2. Disclosure may be made of medical or epidemiological information to the extent necessary to enforce section 23-07-02.1 and this section and related rules concerning the treatment, control, and investigation of human immunodeficiency virus infection by public health officials; or
3. Disclosure may be made of medical or epidemiological information to medical personnel to the extent necessary to protect the health or life of any individual.

No officer or employee of the state department of health may be examined in any judicial, executive, legislative, or other proceeding regarding the existence or content of any individual's report retained by the department under section 23-07-02.1.

4.0 PHYSICAL SECURITY

BUILDINGS / OFFICES

All PHI, in electronic or paper form, must be maintained in a secure, locked area with limited access. A secure area is an area in which it is protected by at least one level of physical security. Rooms where PHI is stored or viewed should not have windows. If the room does have a window, it cannot be placed in an area in which it can be seen through the window. Keys or key cards cannot be loaned or shared at any time. All visitors must be signed into the building by a HHS, DC staff member and wear a visitor's badge. All visitors must be escorted by an HHS, DC staff member while they travel through the building. Visitors are any persons who otherwise do not have access to the workspace. Exemptions include employees from other areas of the North Dakota Department of Health who have key card access to the building. Persons with authorized access to the HHS, DC must be able to identify when a visitor is present and must adjust behaviors accordingly. Secured doors must remain closed unless prior approval from the ORP is obtained to have them opened or disabled.

COMPUTER WORKSTATIONS

All computer workstations with access to confidential information must be in a secure area. Screens must not be readily observable by non-authorized uses as they pass through the office area, work within the workspace or approach a reception area. Computers used to access PHI must be password protected at the Windows login level and require login anytime the screen is dormant. All network/computer passwords must follow current HHS password guidelines. Network/computer passwords must expire based on current HHS password guidelines. New or temporary user passwords must be changed by the user upon receipt of the password. Passwords must not be shared with others, written down or stored where others have access. Networks or computers should not be accessed by individuals using another person's access. If security is ever in doubt, passwords should be changed immediately. Workstations must be locked (Ctl+Alt+Delete—Lock) when a workstation is left unattended for any period of time. Confidential data must not be accessed or worked with on any computer or device that is not issued by the HHS. Computer workstations are equipped with BitLocker to assure that data cannot be removed without the use of authorized user passwords.

All computer workstations and laptops must be protected from hot and cold extremes to ensure the integrity of the machine is conserved. All computer workstations must kept in a location that is protected from destruction by natural or manmade forces (tornado, fire, explosion, etc.) to the best of the Department's ability. All devices will be equipped with up to date virus protection.

DOCUMENT DISPOSAL

Duplicate copies of documents (paper or electronic) and/or files shall be kept to a minimum. Once a file or duplicate copy is used for its intended purpose, it will be immediately shredded in a commercial quality machine with a crosscutting feature or securely deleted. Policies regarding the duration of storage of documents is referenced in Appendix B: Records Retention. Electronic media (diskette, CD, DVDs, etc.) must be shredded with a crosscutting shredder.

DOCUMENT STORAGE

In the office/in secure areas

All documents containing PHI, when not in use, must be stored with two levels of security. PHI must not be left unattended in any place to which unauthorized persons may reasonably gain access. Documents with PHI must not be readily observable by unauthorized users as they pass through the office, use workstations, or approach reception areas. Documents that are removed from the secure area, they must be transported in a secure, sealed manner.

The eHARS centralized computer registry will be located within the North Dakota Department of Health, Section of Disease Control secure area. Access to the eHARS registry is limited to the STBP division director, HIV/AIDS surveillance coordinator, and the Disease Control IT specialist.

No remote eHARS sites are located outside the Section of Disease Control. Laptops can access the eHARS centralized computer using a remote desktop connection over the network. The laptop cannot access the eHARS centralized computer if it is removed from the network. No confidential or highly confidential data can be stored on any laptop or other device that is accessible away from the North Dakota Department of Health, Section of Disease Control secure area and servers.

Outside the office/outside secure areas

Transportation and use of PHI in an unsecure area must be minimized and carefully controlled. It is preferred that documents removed from secure areas not contain both identifiable information and disease-specific information. During an investigation, confidential information must not be taken to a private residence, place of business, or any other location other than the client's residence. The only documents taken in this situation should only be relevant to that specific client. When documents are taken from secured areas, they must contain only the minimal amount of confidential information necessary to do business. The contents of any files will not be divulged to any unauthorized persons. They will be carried in a manner that prevents easy viewing and theft (i.e. must be inside a satchel or bag that can be securely closed or locked). All documents with PHI must be returned to a secure environment by the close of business each day unless prior approval has been received from the ORP.

Confidential, Highly Confidential and Privileged information can be access away from the North Dakota Department of Health, Section of Disease Control secure space via the North Dakota Electronic Disease Surveillance System (MAVEN) by staff only when there is an imminent need for information relating to case work and follow-up. All work should be done where there is no risk of any other individual without security clearance seeing any identifying information. All notes or physical copies of information is required to be destroyed by using a cross-cutting shredder once entered into MAVEN. Every effort to use patient ID codes and limit the amount of identifying information when taking PHI off site should be considered.

MAIL (INCOMING AND OUTGOING)

Incoming mail that is marked confidential or addressed to the Section of Disease Control shall be opened only by approved staff and kept secure until processed. Senders of confidential information are to be instructed to address mail to the appropriate staff member or program. Whenever confidential information is mailed, it must be double enveloped or the equivalent and sent with "return services requested." No reference to any disease should be on the envelope of confidential or highly confidential PHI that is mailed. If a disease is referenced in the material to be mailed, patient-specific identifiers (e.g., name, address, date of birth) will be separated from the remaining information and

mailed separately. Only the addressee shall open incoming mail that is marked "confidential." If the addressee of the mail marked "confidential" is unavailable for an extended period of two or more days, the appropriate program manager (or the ORP in their absence) may open the mail and forward the contents to the appropriate person.

Each person within HHS, DC will have an individual mailbox. Any mail addressed to employees who have left the division will be presented to the ORP for final determination of dissemination.

Outgoing mail that contains information on cases will be marked "confidential". Whenever confidential information is mailed, double envelopes should be used with the inside envelope clearly marked as "confidential". No mention of the disease will be on the envelope or mailing materials.

PHONE/TEXT MESSAGING

Telephone calls concerning PHI must be made in a secure area. If possible, telephone calls concerning PHI should be made in an area where conversations cannot be overheard. Staff must ascertain that phone contacts have legitimate rights to discuss PHI before any conversation concerning that information is conducted. Staff may only share the appropriate amount of information necessary to do business. Confidential information may not be left on voicemail systems.

Text messaging can be utilized as a last resort to communicate PHI only if all other options to reach/interview the individual have been exhausted.

5.0 ELECTRONIC DATA SECURITY

ELECTRONIC DATASETS & STORAGE

Any electronic files containing confidential data and information will be stored in a secure location behind state firewalls. All computer files containing highly confidential PHI must be guarded by a minimum of two levels of security—the computer must be maintained in a locked office and must be password protected. All passwords to computer files containing highly confidential information must be changed according to HHS password policy to maintain the highest level of security. Once a password has been compromised, that password must be changed immediately.

The workstation that stores eHARS data is solely dedicated to maintaining eHARS, thus reducing the risk of virus infection. Also, all computers with network access have the latest anti-virus software and are routinely scanned for viruses. The eHARS workstation uses the Windows Server operating system, limiting access through password protection to the surveillance coordinator and the information technology coordinator. The computer's screen saver defaults to network login after 5 minutes, forcing authorized access only. Three failed attempts will result in the workstation being locked.

The eHARS database is backed up nightly to the backup hard drive on the workstation. eHARS data are also backed up weekly, at a minimum, to an encrypted drive, that meets Advanced Encryption Standards (AES), and stored in the HHS, DC record room under two levels of security. The drive is placed in a locked file cabinet behind a locked door. Only HHS, DC personnel authorized by the ORP have access to the door and cabinet keys. Back-ups may be done more frequently if extensive registry changes are made.

Analysis datasets that can be accessed from outside the secure area shall be stored with protective software and removal of all personal identifiers should be verified. Analysis datasets shall be located on a virtual serve and all personal identifies shall be removed. The inclusion of sensitive or linkable data elements such as lab ID, accession number, medical record number, or case report number shall be limited to those required for analysis and shall not be included in analysis datasets.

ELECTRONIC DATA TRANSFER

Electronic transfer of data shall be approved by the ORP and is subject to access controls. Designated HHS, DC staff can send encrypted data after approval by the division director and ORP. Identifiable data shall be encrypted meeting AES standards before being transferred. Extracts from systems outside HHS, DC shall meet the minimum-security standards outlined in this document. Electronic records shall be protected through security devices, such as sign-on passwords, encryption and audit trails. External sources will be encouraged to review their procedures. Approved data transfer methods shall be used when designing electronic reporting mechanisms for laboratories, providers, etc.

Encrypted data shall be transferred over secure data network (SDN) or virtual private network (VPN) connection with certificates in both the sending and receiving ends, or similar secure network. If SDN or VPN cannot be used, then it shall be transferred via secure application such as secure file transfer protocol (sFTP) for which certification is required on at least one end.

All staff that have authorized access to confidential information are individually responsible for protecting their assigned laptop or other portable devices including, but not limited to: cell phone,

tablet, laptops, flash drives, diskettes, CD-ROMS, Zip disks, tape backups, removable hard drives and/or smart cards.

MOBILE DEVICES & LAPTOPS

Laptops used as a work computer follow the same security and confidentiality guidelines as workstations. Devices (laptops, cell phones, tablets, etc.) shall never be left accessible in non-secure areas. Devices shall be stored in a secure area when not in use. PHI on a laptop must be encrypted according to AES and stored on an external storage device or removable hard drive. The external storage or removable hard drive must be separated from the laptop and stored under lock and key while not in use. Mobile devices without external storage capability must have encryption software that meets AES.

EXTERNAL STORAGE DEVICES AND REMOVABLE HARD DRIVES

All external storage devices and removable hard drives containing PHI must include the minimum amount of information necessary to accomplish an assigned task as determined by the ORP or program manager, be encrypted according to AES, under lock and key when not in use and must be erased immediately following a given task is accomplished. This is excused for the purposed of back-ups.

E-MAIL

Any PHI sent via e-mail must be sent as an AES encrypted attachment and contain only the minimum amount of information necessary. If PHI is sent non-encrypted, the ORP must be notified. Inform the sender that PHI has been sent in a non-encrypted format and do not reply to the e-mail containing the PHI.

Email, encrypted or non-encrypted, must not be used to transmit confidential information except those that meet the HHS-specific treatment exception (see below). Emailing attachments containing confidential information is also prohibited. The eHARS city no., state no., and UID are considered identifying variables and should not be included in emails or attachments.

Staff must include a signature in the email body stating, *"Please do not reply to this email with any patient identifying information. This includes name, phone number, DOB, address, and medical record numbers. Please call me on my private line at (###) ###-#### with this information."*

Treatment Exception: Emails being used for the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another may be sent using HHS agency email. Any PHI must be in a file that is encrypted and attached to the email, not in the body of the email itself. The HHS agency email policy for sharing confidential PHI must be followed, it states.

> Confidential HHS information and an individual's full name, or first initial and last name along with restricted personal information, such as social security number, government-issued identification number, driver's license number or Medicaid number and PHI transmitted over network connections must be encrypted using the 'Secure Mail' email function or otherwise protected as required by rule or law and agency policy and procedures. Do not include confidential information in the subject line of the email since the subject line is not encrypted.

TEXTING

The standards for maintaining client confidentiality must be followed in all types of communications involving any individual who may have been exposed to HIV, STDs, Tuberculosis and/or Viral Hepatitis.

To ensure compliance with the Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Pub L No. 104-191), text messages sent by a health department employee should never include an individual's protected health information.

Text messages should never include a reference to “STD”, “HIV”, “Syphilis”, “TB”, or any other identified health condition.

The following guidelines must be followed:

- Initial text messages sent to clients should encourage them to make contact via phone. While some clients may insist on texting only, text messages should be worded to motivate the client to call since protected health information may not be shared via text.
- Text messaging should only be done from an encryption-protected, agency-issued device. Personal devices should not be used to send text messages for public health follow-up.
- For retention concerns, text messages are considered as transitory information and must be deleted within 24 hours after entering information into the official system of record.
- If an agency-issued device that is used for text messaging is lost or stolen, the employee must immediately report the loss/theft to their supervisor and the overall responsible party (ORP). This must be handled as a possible breach.
- If a client texts you information that needs to be kept (ex. address, contact information, etc.) you must update the system of record (MAVEN) within 24 hours and then delete the text message from the device.
- Some appropriate uses for text messages include: appointment reminders, requests for the client to contact you, confirming date and location of an appointment/interview, etc., including a comment discouraging the client from responding to the text message with any personal information. Always contact your supervisor or ORP if you are uncertain about how to word a text message or before responding to a text message from a client who is asking for more information.
- Avoid getting into a texting conversation; state for the protection of client privacy you are not allowed to share confidential information via a text message.

FAX (INCOMING AND OUTGOING)

Facsimile transmission of PHI should only be done when other methods of sending information are unavailable or would delay the timely provision of services. Minimum amounts of confidential information should be included. Fax machines must be kept in a secure area. All fax communications containing PHI must be sent with a cover sheet that includes the name of the intended recipient, confidentiality disclaimer statement, and instructions on what to do if it was received in error. Anyone sending a fax must confirm that the information was received by the intended recipient. If a fax fails to reach the recipient, the internal logging system of the fax machine shall be checked to obtain the number to which the transmission was sent. If the sender becomes aware that the fax was misdirected, contact the receiver and ask that the material be destroyed. Misdirected faxes shall be investigated as a

potential security breach, the ORP shall be informed, and the incident logged for remediation/mitigation.

The use of a close looped, unmanned fax system for the sending and receipt of faxes to a dedicated email is acceptable.

A sample confidentiality disclaimer: *The documents accompanying this fax transmission contain health information that is legally privileged. This information is intended for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and sis required to destroy the information after its stated need has been fulfilled. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.*

SOCIAL MEDIA & OTHER WEB PLATFORMS

The use of social media and other web platforms are not permitted as a mechanism to relay any PHI.

USE OF AI FOR DATA ANALYSIS AND DASHBOARDS

The integration of Artificial Intelligence (AI) into data analysis and dashboard functionalities enhances the ability to process, visualize, and interpret complex datasets efficiently. AI-driven analytics can support real-time surveillance, automate data categorization, detect trends, and provide predictive insights for disease control efforts. However, the use of AI in these capacities must adhere to strict data protection policies to ensure compliance with security and confidentiality standards. Under no circumstances should protected health information (PHI) be used within AI tools. PHI must be excluded from AI models, training datasets, and automated reporting processes to prevent unauthorized exposure and breaches.

To protect sensitive data, dashboards must be configured with strict access controls, ensuring that only authorized personnel have the ability to view specific datasets. Role-based access should be enforced to minimize unnecessary exposure. Any AI-generated reports or visualizations should adhere to data de-identification protocols, ensuring that personally identifiable information (PII) is not displayed or inferable. Additionally, all AI-driven data processing must occur in secure environments that comply with state and federal data security regulations.

Encryption must be implemented to protect data both in transit and at rest, utilizing AES-256 encryption standards or higher. All electronic storage locations for AI-generated reports and datasets must require multi-factor authentication to prevent unauthorized retrieval.

STATEMENT FOR PROTECTION OF CONFIDENTIAL INFORMATION

As an employee, contractor, partner or visitor of the North Dakota Department of Health and Human Services, Disease Control & Forensic Pathology Section, you are assuming the responsibility of maintaining the security of confidential and highly confidential HIV/AIDS case information. All employees, contractors, partners or visitors who have access to confidential and/or highly confidential HIV/AIDS records are required to sign this Confidentiality Oath annually.

I have read and understand the North Dakota Century Code as they pertain to confidentiality requirements, specifically NDCC 23-01.3, 23-07-02.2, 23-07-20.1 and 23-07.5 including Administrative Rule 33-06-03-04, and agree to abide by all provisions.

I have read and understand the "North Dakota Sexually Transmitted and Bloodborne Pathogens Security and Confidentiality Policy" and agree to abide by its protocols.

I have been informed and understand that all client/patient/employee information records compiled, obtained or maintained by me in the course of my duties are confidential. I agree not to divulge or otherwise make known to unauthorized persons any information regarding the same.

In addition, I understand that I am not to read information and records concerning patients and case reports, or any other confidential documents, for my own personal information but only to the extent and for the purpose of enabling me to perform my assigned duties.

I understand that:

· A breach of this policy concerning confidentiality may be grounds for disciplinary action which may include termination of employment;

· Effective August 1, 1999, a person who knowingly discloses protected health information in violation of this chapter is guilty of a class A misdemeanor, pursuant to NDCC 23-01.3-09; and

· The penalties set forth in NDCC 23-07.5-08, a class C felony with a fine of $5,000 and/or imprisonment for up to five years for each breach of confidentiality related to HIV test results.

By signing this, I acknowledge that I have read, understand and will comply with this statement.

_____

Employee's name (please print)

_____ _____

Employee's signature Date

_____ _____

ORP's signature Date

APPENDIX A: LIST OF ROLES, SYSTEM ACCESS LEVEL

Position Title	Employee	MAVEN	eHARS	Lab Reports (Fax/Mail)
Sexually Transmitted and Bloodborne Pathogens Unit				
Unit Director	**Lindsey VanderBusch**	X	X	X
HIV.STD.Viral Hepatitis Surveillance Coordinator	Luke Unger	X	X	X
HIV.STD.Viral Hepatitis Prevention Coordinator	Sarah Weninger	X		X
HIV Prevention Specialist	Mary Bruns	X		X
Ryan White Part B Coordinator	Gordana Cokrlic	X		X
Ryan White Specialist	Courtney Ali	X		X
TB Controller	Laura Cronquist	X		X
TB Program Nurse	Beth Weidler	X		X
Hepatitis Surveillance Epidemiologist	Claire Erickson	X	X	X
Data Quality/Performance Measurement	Sandy Nasr	X		X
Other Disease Control Section Staff				
Section Chief	Kirby Kruger	X		X
Deputy Section Chief	Molly Howell	X		X
State Epidemiologist	Tracy Miller Benjamin Schram	X		
Disease Surveillance Systems	Scott Fried Michael Benz	X	X	X
Field Services	**Brenton Nesemeier** Gino Jose Linda Larson Heather Kontz Rachel Goebel Jenna Bielke Crystal Duncan	X		X

	Samantha Janecek			
Infectious Diseases and Epidemiology	**Michelle Dethloff** Lakin Mauch-Kath Levi Schlosser Amanda Bakken Donna Davidson Jeannie Woolston John Fosu Jill Hanson Amy Hanson Allison Klassen Abbey Fraser Robert Peters Slate Boyer Faye Salzer Jordan Taghon Megan Compson Shea Griffith Morgan Messer	X		X
Immunizations	**Molly Howell** Jenny Galbraith Kristen Vetter Danielle Pinnick Mary Woinarowicz Abbi Berg Miranda Baumgartner	X		X
Administrative Support	Brandy Chap Jennifer Markwed	X		X
Sub-Recipients				
Ryan White Regional Coordinators	Ashley Saylor Alexis Hendrickson Becky Fladeland Heatthyr Haugeberg Jennifer Amundson Jennifer Pelster Kara Gloe Keely Johnston Kelly Ozaki Michael Cumber Tammie Roed Vincent Loos	L		

	Karena Goehner Karen Goyne Kjersti Hintz Madison Verghis			

X = Full System Access; L = Limited to Assigned Cases Only

APPENDIX B: RECORDS RETENTION POLICY

The North Dakota Department of Health provides a centralized, efficient, and secure storage space for Section of Disease Control data, in both electronic and physical format. The policies of the Departments schedule for records retention by condition are as follows:

- **HIV:** Electronic records will be kept for 75 years after the date of the event; physical records once stored electronically will be destroyed according to records disposal policies referenced above. Physical records not stored in electronic format will be retained for 75 years after the date of the event according to storage policies referenced in this document.

- **Chlamydia:** Electronic records will be kept for 75 years after the date of the event; physical records once stored electronically will be destroyed according to records disposal policies referenced above. Physical records not stored in electronic format will be retained for 75 years after the date of the event according to storage policies referenced in this document.

- **Gonorrhea:** Electronic records will be kept for 75 years after the date of the event; physical records once stored electronically will be destroyed according to records disposal policies referenced above. Physical records not stored in electronic format will be retained for 75 years after the date of the event according to storage policies referenced in this document.

- **Syphilis:** Electronic records will be kept for 75 years after the date of the event; physical records once stored electronically will be destroyed according to records disposal policies referenced above. Physical records not stored in electronic format will be retained for 75 years after the date of the event according to storage policies referenced in this document.

- **Tuberculosis:** Electronic records will be kept for 75 years after the date of the event; physical records once stored electronically will be destroyed according to records disposal policies referenced above. Physical records not stored in electronic format will be retained for 75 years after the date of the event according to storage policies referenced in this document.

- **Viral Hepatitis:** Electronic records will be kept for 75 years after the date of the event; physical records once stored electronically will be destroyed according to records disposal policies referenced above. Physical records not stored in electronic format will be retained for 75 years after the date of the event according to storage policies referenced in this document.