North Dakota-500
Statewide Continuum of Care

Security Policy

CoC Board Approval: July 2023
CoC Membership Approval: August 2023

Next Review: July 2024

I. Introduction

This Policy describes standards for the security of personal information collected and stored in the North Dakota Homeless Management Information System (HMIS), as well as personal identifying information (PII) collected for the purpose of the North Dakota Continuum of Care (ND CoC) Coordinated Access, Referral, Entry, and Stabilization System (CARES). The standards seek to ensure the security of PII. This Security Policy (Policy) is based on principles of fair information practices recognized by the information security and technology communities.

This Policy defines the security standards that will be required of any organization within the state of North Dakota that records, uses, or processes PII on clients at-risk of or experiencing homelessness for HMIS and/or CARES. Organizations must also comply with federal, state, and local laws that require additional security protections, where applicable.

This Policy recognizes the broad diversity of organizations that participate in HMIS and/or CARES, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (e.g., such as those serving victims of domestic violence) may choose to implement higher levels of security standards because of the nature of the clients they serve and/or service provision. Others (e.g., large emergency shelters) may find higher standards overly burdensome or impractical. At a minimum, however, all organizations must meet the security standards described in this Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for organizations with additional needs or capacities.

The following sections discuss the ND CoC Security Policy.

II. ND CoC Statewide Security Policy: Definitions and Scope

Definition of Terms

A. *Personally Identifiable Information (PII).* Any information maintained by or for an agency about a client at-risk of or experiencing homelessness that:

   1. Identifies, either directly or indirectly, a specific individual;
   2. Can be manipulated by a reasonably foreseeable method to identify a specific individual; or
   3. Can be linked with other available information to identify a specific individual.

B. *Agency.* Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes PII on clients at-risk of or experiencing homelessness for HMIS or CARES. This definition includes both organizations that have direct access to HMIS and/or CARES, as well as those organizations who do not but do record, use, or process PII.

C. *Processing.* Any operation or set of operations performed on PII, whether by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.

III. Security Standards

This section describes the standards for system, application, and hard copy security. All agencies must comply with these requirements.

IV. System Security Applicability

A. *Equipment Security.* An agency must apply system security provisions to all the systems where PII is stored, including, but not limited to, an agency's networks, desktops, laptops, mini-computers, mainframes, and servers.

B. *User Authentication.* Each user accessing a workstation that contains HMIS and/or CARES data must have a unique username and password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

1. Using at least one number and one letter or symbol;
2. Not using, or including, the username, the HMIS name, or the HMIS vendor's name; and/or
3. Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.
4. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

C. *Virus Protection.* An agency must protect HMIS and any electronic device used to store PII for the purposes of CARES from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed and/or where PII for the purposes of CARES is stored. An agency must regularly update virus definitions from the software vendor.

D. *Firewalls.* An agency must protect HMIS and any electronic device used to store PII for the purposes of CARES from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, so long as there is a firewall between that workstation and any systems, including the internet and other computer networks, located outside of the organization.

For example, a workstation that accesses the internet through a modem would need its own firewall. A workstation that accesses the internet through a central server would not need a firewall so long as the server has a firewall. Firewalls are commonly included with all new operating systems. Older operating systems can be equipped with secure firewalls that are available both commercially and for free on the internet.

E. *Public Access.* HMIS and any electronic device used to store PII for the purposes of CARES that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure certificates, or extranets that limit access based on the Internet Provider address, or similar means. A public forum includes systems with public access to any part of the computer through the internet, modems, bulletin boards, public kiosks, or similar arenas.

F. *Physical Access to Systems with Access to HMIS Data.* An agency must always staff computers stationed in public areas that are used to collect and store HMIS and/or CARES data. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, a password-protected

screensaver should automatically turn on when the workstation is temporarily not in use. Password-protected screensavers are a standard feature with most operating systems and the amount of time can be regulated by an agency. If staff from an agency will be gone for an extended period, staff should log off the data entry system and shut down the computer.

G. *Disaster Protection and Recovery.* HMIS data is copied on a regular basis to another medium (e.g., tape) and stored in a secure off-site location where the required security standards apply. The software provider that stores the data (WellSky™) in a central server stores that central server in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors are used to protect systems used for collecting and storing all the HMIS data.

H. *Disposal.* In order to delete all HMIS and/or CARES data from a data storage medium, an agency must reformat the storage medium. An agency should reformat the storage medium more than once before reusing or disposing the medium.

I. *System Monitoring.* An agency must use appropriate methods to monitor security systems. Systems that have access to any HMIS and/or CARES data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

V. Application Security

These provisions apply to how all HMIS data are secured by the HMIS application software.

A. *Applicability.* An agency must apply application security provisions to the software during data entry, storage, and review or any other processing function.

B. *User Authentication.* An agency must secure all electronic HMIS and/or CARES data with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

1. Using at least one number and one letter or symbol;
2. Not using, or including, the username, the HMIS name, or the HMIS vendor's name; and
3. Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.
4. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users should not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

C. *Electronic Data Transmission.* An agency must encrypt all HMIS and/or CARES data that are electronically transmitted over the internet, publicly accessible networks, or phone lines to current industry standards. The current standard is 128- bit encryption. Unencrypted data may be transmitted over secure direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections.

D. *Electronic Data Storage.* An agency must store all HMIS and/or CARES data in a binary, not text, format. An agency that uses one of several common applications (e.g., Microsoft Access, Microsoft SQL Server, or Oracle) is already storing data in binary format and no other steps need to be taken.

VI. Hard Copy Security

This section provides standards for securing hard copy data.

A. *Applicability.* An agency must secure any paper or other hard copy containing PII that is either generated by or for the HMIS and/or CARES including, but not limited to reports, data entry forms, and case/client notes.

B. *Security.* An agency must always supervise any paper or other hard copy generated by or for HMIS and/or CARES that contains PII when the hard copy is in a public area. When agency staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.