

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

TABLE OF CONTENTS

- 1. SERVICEPOINT: CMIS/HMIS SYSTEM 1
- 2. PROJECT OVERVIEW 2
- 3. CONTACT INFORMATION 2
- 4. PURPOSE..... 2
- 5. SCOPE 2
- 6. GOVERNING PRINCIPLES 2
- 7. DEFINITIONS 3
- 8. EQUIPMENT, MATERIALS AND SUPPLIES 3
- 9. FORMS and DOCUMENTS (incorporated by addendum and subject to change)..... 4
- 10. CONFIDENTIALITY & SECURITY 4
- 11. ROLES AND RESPONSIBILITIES 5
- 12. DATA STANDARDS 8
- 13. DATA EXPECTATIONS..... 9
- 14. REPORTS/DATA SUBMISSIONS 9
- 15. PRIVACY REQUIREMENTS 9
- REVISION HISTORY..... 11

1. SERVICEPOINT: CMIS/HMIS SYSTEM

Client Management Information System (CMIS)/Homeless Management Information System (HMIS) is a locally administered, electronic data collection system that stores longitudinal person-level information about persons who access the service system.

City of Portland, Portland Housing Bureau (PHB) has instituted the use of ServicePoint as the CMIS/HMIS system in response to Congressional Directive and U.S. Department of Housing and Urban Development (HUD) support for Homeless Management Information Systems (HMIS).

ServicePoint (trademarked and copyrighted by Bowman Systems) is a web based Client Information System that provides standardized assessment of a Client’s needs, creates individualized service plans and records the use of housing and services which communities can use to determine the utilization of services of participating Service Providers, identify gaps in the local service continuum and develop outcome measurements.

For more information regarding Client/Homeless Management Information Systems (CMIS/HMIS) Policy and Procedures, please contact the CMIS/HMIS System Administrator.

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

2. PROJECT OVERVIEW

NW Social Service Connections (NWSSC) is the administrative entity that governs a multi Continuum of Care implementation of CMIS/HMIS used to record and share information among service-providers on services provided to homeless and near homeless Clients.

The City of Portland, Portland Housing Bureau (PHB) is the owner and operator of the NWSSC CMIS/HMIS and serves as the NWSSC System Administrator and custodian of data in the system. NWSSC is a collaboration of multiple Continuums of Care and Service System Partnerships in accordance with PHB intergovernmental Agreements or Memorandums of Understanding.

The NWSSC System Administrators are ServicePoint dedicated program staffs from PHB, additionally each of the Continuums of Care or Service System Partnerships have identified staff functioning as ServicePoint System Administrators for their respective jurisdictions.

3. CONTACT INFORMATION

Clackamas County Community Development
Public Services Building, 2nd Floor
2051 Kaen Rd.,
Oregon City, OR 97045
<http://www.clackamas.us/cd/>

System Administrator
Susan Johnson
503-650-5668
susanj@co.clackamas.or.us

Portland Housing Bureau
421 SW 6th Avenue, Suite 500
Portland, OR 97204
<http://www.portlandonline.com/PHB/>

NWSSC Program Manager/System Administrator
Wendy Smith
503-823-2386
wendy.smith@portlandoregon.gov

4. PURPOSE

This document is to define the general requirements and provide an overview of the CMIS/HMIS System.

5. SCOPE

These Policies and Procedures apply to ALL Persons or Organizations, using any portion of the CMIS/HMIS system.

6. GOVERNING PRINCIPLES

- 6.1. ALL Persons using CMIS/HMIS are expected to read, understand, and adhere to the Final Revised HMIS Data Standards; March 2010
(http://www.hmis.info/ClassicAsp/documents/Final%20HMIS%20Data%20Standards-Revised%20_3.pdf) and the Department of Housing and Urban Development Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice; Notice
(<http://www.hmis.info/ClassicAsp/documents/HUD%20Data%20and%20Technical%20Standards.pdf>)
- 6.2. ALL Persons using CMIS/HMIS are expected to read, understand, and adhere to the spirit of these principles, even when the Policies and Procedures do not provide specific direction.
- 6.3. All information entered into the CMIS/HMIS system, the Service Providers, Participants, their respective staff, and end users are bound by all applicable federal and state confidentiality regulations and laws

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

that protect the Client records that will be placed on the HMIS system; in accordance with the Participation Agreement.

- 6.4. Clients may not be denied access to their own records. Clients have the right to see their information on ServicePoint, within the time frame specified in the Privacy Notice to Clients. If a Client requests, the Participant/User must review the information with the client.
- 6.5. Bowman Internet Systems will host our implementation of ServicePoint; all Client information in ServicePoint is encrypted.
- 6.6. Confidentiality
 - 6.6.1. The rights and privileges of clients are crucial to the success of CMIS/HMIS. These policies will ensure clients' privacy without impacting the delivery of services, which is the primary focus of agency programs participating in this project.
 - 6.6.2. Policies regarding client data are founded on the premise that a client owns his/her own personal information and provide the necessary safeguards to protect client, agency, and policy level interests.
- 6.7. Data Integrity
 - 6.7.1. Client data is the most valuable and sensitive asset of CMIS/HMIS. These policies will ensure integrity and protect this asset from accidental or intentional unauthorized modification, destruction or disclosure.
- 6.8. System Availability
 - 6.8.1. The availability of a centralized data repository is necessary to achieve the ultimate system/community wide aggregation of unduplicated statistics. The System Administrators are responsible for ensuring the broadest deployment and availability for participating service providers.
- 6.9. Compliance
 - 6.9.1. Violation of the policies and procedures set forth in this document will have serious consequences. Any deliberate or unintentional action resulting in a breach of confidentiality or loss of data integrity may result in the withdrawal of system access for the offending entity.

7. DEFINITIONS

- 7.1. Refer to Homeless Management Information System (HMIS) Data Standards- Revised Notice – March 2010 Section 1.4 Definitions for terms used throughout the notice and applicable to CMIS/HMIS.
- 7.2. Refer to CMIS/HMIS Community Data Standards Section 2.
- 7.3. Refer to funder or program documentation for terms used by those funders or programs.

8. EQUIPMENT, MATERIALS AND SUPPLIES

- 8.1. Participating Agencies are responsible for providing their own technical support for all Hardware and Software systems used to connect to CMIS/HMIS.
- 8.2. Computer Workstation (PC, Personal Computer).
 - 8.2.1. Minimum hardware and software requirements for workstations (subject to change).
 - 8.2.1.1. Computer: PC with a 2 Gigahertz or higher processor
 - 8.2.1.2. 40GB Hard Drive
 - 8.2.1.3. 512 MB RAM
 - 8.2.1.4. Microsoft Windows 2000 or XP
 - 8.2.1.5. Browser: Most recent version of Microsoft Internet Explorer or Firefox
 - 8.2.1.6. Connectivity: Minimum - 56 Kbps || Optimal – 128 Kbps – 1.5 mps

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

9. FORMS and DOCUMENTS (incorporated by addendum and subject to change)

HMIS Participation Agreement

HMIS Policy and Procedure *which includes the following attachments*

attachment 1	Community Data Standards
attachment 1a	Data Expectations and Exceptions
attachment 2	HMIS and HIPAA
attachment 3	User Agreement
attachment 3a	User Agreement – Special User
attachment 4	Remote Access Policy
attachment 4a	Remote Access Policy Agreement
attachment 5	Notice to Clients of Uses Disclosure
attachment 5a	Notice to Clients of Uses Disclosure for Posting
attachment 6	HMIS Data Quality Training Plan
attachment 7	Business Associates Agreement (Behavioral Health)
attachment 7a	Security Addendum to Business Associates Agreement (Behavioral Health)

10. CONFIDENTIALITY & SECURITY

- 10.1. CMIS/HMIS System administrators have full and complete access to all ServicePoint features and functions for their respective jurisdictions. If it is requested, the CMIS/HMIS system administrator must be willing to sign the confidentiality oaths of the Affiliated Service Providers.
- 10.2. For all information entered in the CMIS/HMIS system the Service Providers, Users and Agencies are bound by all applicable federal and state confidentiality regulations and laws that protect the Client records that will be placed on the CMIS/HMIS system.
- 10.3. CMIS/HMIS Service Providers have a primary duty to protect the confidentiality and security of client records. If a Service Provider using the CMIS/HMIS system receives a request to release client level information, the Service Provider must verify that a current hard copy Release of Information form is on file. The Release of Information form must be signed by the client or authorized client representative and include all specific parties to whom the information may be released. A general release of all client information is prohibited.

In the event the request is in the form of a subpoena, the Service Provider shall immediately notify the local System Administrator, who in turn shall immediately notify the NWSSC Project Director/System Administrator for assistance. This includes a review of the validity of the request and obtaining only the information identified in the request. Hard copy releases are not required in the event a valid subpoena is received.
- 10.4. The Service Provider shall ensure that all staff, volunteers and other persons are issued a unique User ID and password for CMIS/HMIS and receive confidentiality training on the use of CMIS/HMIS and applicable confidentiality laws.
 - 10.4.1. The Service Provider is responsible to contact the Agency or System Administrator for revoking, adding or editing User access in a timely manner.
- 10.5. Unauthorized disclosure of Protected Personal Information may be grounds for legal action.
- 10.6. Sharing of CMIS/HMIS data among Affiliated Service Providers is encouraged but not required. The CMIS/HMIS data items excluded from sharing include medical, legal, case management, case notes, and file attachments, unless specifically released by Client.
- 10.7. HIPAA Privacy Rules take precedence over CMIS/HMIS privacy standards. If an agency is a HIPAA covered agency, they must abide by HIPAA regulations.

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

- 10.8. Creating anonymous records may mean that reports will not provide a true unduplicated count and therefore this option should only be used if absolutely necessary. Please contact the System Administrator for other options.
- 10.9. ServicePoint™ shall only be accessed from the Organization's network, desktops, laptops, and mini-computers.
 - 10.9.1. NWSSC System Administrators are allowed to access the database from remote locations for purposes specific to their job. All staff that access the database remotely must meet the standards detailed in the System Security (above) and may only access it for activities directly related to their job. These approved remote locations include:
 - 10.9.1.1. Private Home office to provide system support as needed.
 - 10.9.1.2. Community Agency offices to support agency use of the system.
 - 10.9.1.3. Private Hotel Rooms on secure networks when providing services while in the field.
 - 10.9.1.4. Training Centers when providing services in the field.
- 10.10. Remote Access (In special circumstances access from remote locations may be permitted after application and approval by Agency and System Administrators)
 - 10.10.1. The ServicePoint Remote Access Agreement must be completed and submitted for approval.
 - 10.10.2. The Agency Administrator must review the need for remote access and investigate other options.
 - 10.10.3. If no other valid options are available the Agency Administrator must approve in writing remote access for a user.
 - 10.10.4. Once remote access agreement has been approved and signed by the Agency Administrator a copy will be filed with the System Administrators for final approval.
 - 10.10.5. Remote Access is subject to change at the NWSSC System Administrator's discretion.
 - 10.10.6. Agency and System Administrators will periodically audit all remote access.
- 10.11. Public Key Infrastructure (PKI)
 - 10.11.1. When a computer is used for ServicePoint, the Service Provider is responsible to contact the System Administrator for the PKI Certificate, password and installation instructions.
 - 10.11.2. When a computer is no longer used for Service Point, the service provider needs to remove the PKI Security Certificate .

11. ROLES AND RESPONSIBILITIES

- 11.1. If it is requested of the CMIS/HMIS system administrators he must be willing to sign the confidentiality oaths of the Affiliated Service Providers.
- 11.2. PHB and the NWSSC System Administrator**
 - 11.2.1. Liaison With HUD
 - 11.2.2. Project Staffing
 - 11.2.3. Overall Responsibility For Success Of NWSSC CMIS/HMIS
 - 11.2.4. Creation Of NWSSC Project Forms And Documentation
 - 11.2.5. NWSSC Project Policies And Procedures And Compliance
 - 11.2.6. Keeper Of Signed Memorandums Of Understanding and Intergovernmental Agreements
 - 11.2.7. Procurement/Renewal of Server Software And Licenses
- 11.3. ALL Lead Organizations**
 - 11.3.1. Liaison with NWSSC System Administrator
 - 11.3.2. Project Staffing
 - 11.3.3. Creation of Local project Forms and Documentation
 - 11.3.4. Data quality reviews

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

- 11.3.4.1. Data Quality
- 11.3.4.2. Data Validity
- 11.3.4.3. Data Completeness
- 11.3.5. Adherence To HUD Data Standards
- 11.3.6. Adherence to Community Data Standards
- 11.3.7. Adherence to Project Data Standards
- 11.3.8. User Administration
 - 11.3.8.1. Manage User Licenses
 - 11.3.8.2. Process User Agreement forms
- 11.3.9. Training
 - 11.3.9.1. Curriculum Development
 - 11.3.9.2. Training Documentation
 - 11.3.9.3. Confidentiality Training
 - 11.3.9.4. Application Training For Agency Administrators and End Users
 - 11.3.9.5. New Provider training
 - 11.3.9.6. Upgrade, enhancement, refresher or other training
- 11.3.10. Outreach/End User Support/Technical Assistance/Password Resets
 - 11.3.10.1. Password Resets require some sort of user Identity verification.
- 11.3.11. Coordinate any application customizations with the NWSSC System Administrator
- 11.3.12. Will use universal naming conventions, in order to better standardize, when creating new assessment questions, sub-assessments, and any other system wide modifications.
- 11.3.13. All Local documentation including P&Ps and agreements must be no less restrictive than NWSSC documents.

11.4. Contributory HMIS Organization (CHO) Responsibilities:

- 11.4.1. The CHO must make available to users a secure system to access ServicePoint, including but not limited to firewall and virus protection.
- 11.4.2. The CHO must be current all related contracts.
- 11.4.3. The CHO shall follow, comply with and enforce the Agency Agreement.
- 11.4.4. The CHO shall abide by all data standards and all policies and procedures.
- 11.4.5. The CHO shall keep abreast of all ServicePoint updates and policy changes.
- 11.4.6. The CHO shall identify and approve their respective Agency Users.
- 11.4.7. The CHO shall designate one User to be the Agency's Key User/Agency Administrator.
- 11.4.8. The CHO shall be responsible for entering Client data (profile, household, needs, services, referrals, any other Client data you may require), following up on referrals, and running reports in a timely manner.
- 11.4.9. The CHO shall have representation at agency administrators/regional data quality review meetings.
- 11.4.10. The CHO shall collect data on all clients as called out in the Data Element Matrix
- 11.4.11. CHO Exceptions may include non-homeless CMIS organizations, and DV Comparable database organizations. Please contact the System Administrator for information and waiver.

11.5. User Responsibilities:

- 11.5.1. The User shall provide an email contact to the System Administrators for communication purposes.
- 11.5.2. The User shall follow, comply with and enforce the User Agreement.
- 11.5.3. The User shall comply with all data standards and policies and procedures.
- 11.5.4. Each User is provided with an access level as required by his/her role. This access level controls who can see which information, lower levels of access allow ONLY viewing of basic demographics, while the middle levels of access allow additional information to be viewed. The

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

highest levels of access are limited to administrators. Confidentiality is a primary concern and these levels of access help control access to information.

- 11.5.5. Every User of the CMIS/HMIS system is authenticated with a unique User ID and password. This provides a level of security and accountability for the CHO's database. Sharing of User IDs or passwords is forbidden.
 - 11.5.6. The User shall only enter individuals in the CMIS/HMIS database that exist as Clients under the Service Provider's approved area of service. The User shall not misrepresent its Client base in the CMIS/HMIS database by entering known, inaccurate information. The User shall not knowingly enter false or misleading data under any circumstances.
 - 11.5.7. The User shall consistently enter information into the CMIS/HMIS database and will strive for Real Time data entry, and be obligated to weekly data entry. A different time frame may be arranged if justified by program need and approved by the local System administrator.
 - 11.5.8. The User will not alter information, with known inaccurate information, in the CMIS/HMIS database that has been entered by another Service Provider (i.e. Service Provider will not purposefully enter inaccurate information to over-ride information entered by another Service Provider).
 - 11.5.9. The User shall utilize the CMIS/HMIS database for business purposes only.
 - 11.5.10. The User shall not use the CMIS/HMIS database with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.
 - 11.5.11. The User shall not cause in any manner, or way, corruption of the CMIS/HMIS database in any manner.
 - 11.5.12. In the event that data entry cannot be made Real Time and the User utilizes hard copy paper forms, once the data has been entered into CMIS/HMIS, the forms shall be securely stored or suitably disposed of.
 - 11.5.13. The User shall enter data into CMIS/HMIS
 - 11.5.13.1. Universal Data elements shall be entered on all Clients.
 - 11.5.13.1.1. In addition to the Universal Data elements all HUD Funded CHO Users, at a minimum, shall also enter the additional data elements required by the Data Standards for all Clients.
 - 11.5.13.1.2. In addition to the Universal Data elements all Non-HUD funded CHO Users, at a minimum, shall also enter funder or program specific data elements as required.
 - 11.5.14. Sharing data is optional but entering data is not optional. An electronic ROI shall be completed for all clients, even if not sharing data.
 - 11.5.15. The User is responsible for data entry accuracy and correctness.
 - 11.5.16. The User shall log off the CMIS/HMIS and shut down the browser when not using CMIS/HMIS.
 - 11.5.17. The User shall utilize the password protected screen savers that automatically turn on to mitigate the burden of shutting down the workstation when momentarily stepping away from the work area.
 - 11.5.18. Report any discrepancies in the use of the PHB CMIS/HMIS system, including without limitation access of information and entry of information, to the Service Provider Key User or to the System Administrator.
 - 11.5.19. The User shall periodically, when instructed by the Agency or System Administrator, review data quality reports, making corrections to ensure data accuracy and completeness.
- 11.6. Key User/Agency Administrator Responsibilities:**
- 11.6.1. The Key User/Agency Administrator shall observe all User Responsibilities.
 - 11.6.2. The Key User/Agency Administrator shall use Agency NewsFlash only for distribution of CMIS/HMIS information.

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

- 11.6.3. The Key User/Agency Administrator shall act as the first level of Service Provider administration and support in the CMIS/HMIS system.
- 11.6.4. The Key User/Agency Administrator shall be responsible for the initial training of new Users in his/her Agency.
- 11.6.5. The Key User/Agency Administrator shall regularly run and review audit reports to ensure policies are being followed by staff.
- 11.6.6. The Key User/Agency Administrator will be responsible for monitoring all User access within their own Agency.

11.7. System Administrators Group

- 11.7.1. Is made up of at least 1 representative from each of the lead organizations of the NWSSC CMIS/HMIS and other participant representatives or advocates as invited by the NWSSC Administrators.
- 11.7.2. Review and make recommendations on all NWSSC HMIS documents, attachments, and related forms
- 11.7.3. Identify and prioritize system enhancements
- 11.7.4. Determine the guiding principles that should underlie the HMIS implementation activities of the project and participating organization and service programs
- 11.7.5. Setting minimum data collection requirements
- 11.7.6. Encourage continuum-wide provider participation
- 11.7.7. Facilitate consumer involvement
- 11.7.8. Recommend criteria, standards, and parameters for the usage and release of all data collected as part of the HMIS
- 11.7.9. Recommend continuum-level mechanisms for monitoring and enforcing compliance with the approved policies and procedures
- 11.7.10. Enhance the implementation and operations of the system for service-providers so they can protect the interests and privacy of their clients
- 11.7.11. Enhance and improve the quality of data being reported to various levels throughout the Continuum
- 11.7.12. Create and implement procedures for additional system issues for Participating Agencies.

11.8. ServicePoint Agency Administrator Group

- 11.8.1. Agency Administrator Group will be established for the purpose of addressing implementation and ongoing operational issues.
- 11.8.2. Identify and prioritizing system enhancements
- 11.8.3. Providing feedback on system performance
- 11.8.4. Brainstorming the best uses of the HMIS
- 11.8.5. Regularly reviewing compliance with all NWSSC HMIS policies, agreements, and other requirements
- 11.8.6. Reviewing data quality and providing feedback to improve data quality

12. DATA STANDARDS

- 12.1. Homeless Management Information System (HMIS) Data Standards – Revised Notice – March 2010
- 12.2. Homeless Management Information Systems (HMIS); Data and Technical Standards - Final Notice - August 2005
- 12.3. Community Data Standards (may be revised at the discretion of the NWSSC System Administrator)

- 12.4 Data Quality/Training Plan

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

13. DATA EXPECTATIONS

- 13.1. Data will be entered within 5 business days of client contact. Exceptions will be considered by the local System Administrator.
- 13.2. Data will be entered in a timely manner to meet aggregate reporting needs
- 13.3. Data accuracy will be no less than 95% (The file matches data entry)
- 13.4. Universal Data Elements Null/Missing Values will not exceed 5%
- 13.5. Universal Data Elements Refused/Don't Know Values will not exceed 5%
 - 13.5.1. Refused/Don't Know responses are client identified, not the case manager or data entry person's assessment.
- 13.6. No outstanding Corrective Actions from last NWSSC CMIS/HMIS Monitoring

14. REPORTS/DATA SUBMISSIONS

- 14.1 System or Community Wide reporting is done on a regular basis without notification.
- 14.2 The Service Provider/User's access to data about Clients it does not serve shall be limited based on the current status of any release of information on file.
- 14.3 The Data Quality and Training Plan outlines the process by which data quality will be evaluated. It lists the reports that will be pulled on a regular basis, the frequency of the pulls and the responsibility of each player.
- 14.4 The general public can request non-identifying aggregate and statistical data, by submitting a data request.
- 14.5 Non identifying aggregate and statistical data will not contain outliers. Outliers may be removed if they represent less than 5% of any value.
- 14.6 At a minimum, Password secure any document that includes client name or other PPI. Do not email the password with the file.
- 14.7 The CMIS/HMIS System Administrator will address all requests for system or community wide data from entities other than Affiliated Service Providers or clients.
- 14.8 The System Administrator will run system-wide reports to assess the data, quality and level of participation by Affiliated Service Providers. Results of these reports may be shared with Affiliated Service Providers.
- 14.9 The System Administrator may run reports for research use. Information in NWSSC CMIS/HMIS may be used to conduct research related to homelessness and housing programs, service needs, income supports, education and employment, and program effectiveness. Client names and social security numbers will never appear on a research report.

15 PRIVACY REQUIREMENTS

- 15.1 The CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information.
- 15.2 The CHO must publish a privacy notice describing its policies and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request.
- 15.3 The CHO must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures.
- 15.4 If the CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page.
- 15.5 The CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.

NW Social Service Connections / Clackamas County

CMIS/HMIS Policy and Procedure

- 15.6 The CHO must maintain permanent documentation of all privacy notice amendments.
- 15.7 The CHO must allow an individual to inspect and to have a copy of any PPI about the individual.
- 15.8 The CHO must offer to explain any information that the individual does not understand.
- 15.9 The CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual, The CHO is not required to remove such information but they may mark such information as inaccurate or incomplete or supplement such information.
- 15.10 The CHO must require each member of its HMIS-licensed staff (including employees, volunteers, affiliates, contractors and associates) to sign a User Agreement annually that includes information from the privacy notice and that pledges to comply with the privacy notice.
- 15.11 The CHO must require each member of its HMIS-licensed staff (including employees, volunteers, affiliates, contractors and associates) to undergo (annually or otherwise) formal training in privacy requirements.
- 15.12 The CHO must establish a method, such as an internal audit, for regularly reviewing compliance with its privacy notice.
- 15.13 The CHO must establish an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of denial of access or correction rights.
- 15.14 The CHO must protect CMIS/HMIS system from malicious intrusion behind a secure firewall.
- 15.15 The CHO must secure any paper or other hard copy containing PPI that is either generated by or for CMIS/HMIS, including, but not limited to report, data entry forms and signed consent forms.

