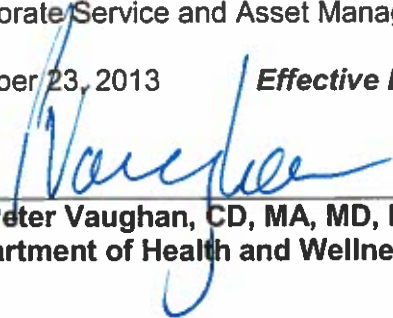

Policy: Joint Service and Access Policy (Pharmacies and Dispensing Physician)

Originating Branch: Corporate Service and Asset Management

Original Approval Date: October 23, 2013 **Effective Date:** April 1, 2016

Approved By: 

**Dr. Peter Vaughan, CD, MA, MD, MPH, Deputy Minister,
Department of Health and Wellness**

Version #: 3

1. POLICY STATEMENT

- 1.1. The purpose of this policy is to define the requirements for access and privacy with respect to the Drug Information System (DIS) and Users of the DIS.

2. DEFINITIONS

In this policy:

- 2.1. **Client Registry (CR)** – means a component of the Nova Scotia Electronic Health Record that lists all patients and their relevant personal information and supports central storage and retrieval.
- 2.2. **Consent Directive** – means an individual's withdrawal of their consent to disclosure of their personal health information in accordance with the *Personal Health Information Act (PHIA)*.
- 2.3. **Default Provider** – means a generic identifier for a provider in the DIS when the actual provider identification information is unknown or unavailable.
- 2.4. **DHW Contractors** – persons or organizations employed by DHW under contract to provide a specific service or support e.g. Deltaware or staff of Deltaware.
- 2.5. **DIS Program** – means the Program of the Nova Scotia Department of Health and Wellness responsible for standards, funding, strategy, performance, and accountability of the DIS.
- 2.6. **DIS Support Website** – means the internet website maintained by the Information Services Support Provider for the purpose of providing information related to the support of the DIS.

- 2.7. **DIS Website** – means the internet website maintained by the DIS Program for the purpose of providing information related to the DIS Program.
- 2.8. **Dispensary Staff** – means pharmacists, pharmacy technicians, pharmacy assistants, the dispensing physician, and staff of the dispensing physician.
- 2.9. **Health Card Number (HCN)** – means a unique identifier that provides access to provincial health care services in Nova Scotia.
- 2.10. **Information Services Support Provider** - means the support organization for provincial health information technology applications that facilitate health care delivery in Nova Scotia. This organization was formerly referred to as Health Information Technology Services Nova Scotia (HITS-NS). May also refer to a successor organization due to government Shared Services changes.
- 2.11. **Masking** – means the limitation of disclosure of personal health information collected by the DIS.
- 2.12. **Nova Scotia Prescription Monitoring Program (NSPMP)** – Mandatory Nova Scotia program that monitors controlled drugs under the Controlled Drugs and Substances Act (Canada).
- 2.13. **nshealth.ca** – means the private network connecting all hospital facilities in the province of Nova Scotia and the provincial data centre. It is the enabler of the health information technology applications delivered throughout Nova Scotia.
- 2.14. **Personal Health Information** – means information that custodians collect to help make decisions about an individual's healthcare. It may include information about an individual's:
- health condition, treatment and family history;
 - healthcare provider's information;
 - registration information or health card number; or,
 - substitute decision-maker
- 2.15. **Pharmacy Manager** – means the individual within a licensed pharmacy in Nova Scotia who holds the role of Pharmacy Manager as defined in the *Pharmacy Practice Regulations* under the *Pharmacy Act*.
- 2.16. **Pharmacy Software** – means an electronic application that manages prescription dispenses and other pharmacy healthcare services.
- 2.17. **Pharmacy Software Vendor** – means a company which provides and supports a pharmacy or dispensing physician with Pharmacy Software.
- 2.18. **PHIA** – means the *Personal Health Information Act*, which is Nova Scotia's health privacy law that governs how regulated health care professionals and organizations collect, use, disclose, and retain, and destroy personal health information.

- 2.19. **Privacy and Access Office (PAO)** – Unit within the DHW that plans, develops, and implements privacy and access policies, processes, and communication initiatives to facilitate the appropriate use and protection of personal information and personal health information within the Department.
- 2.20. **User** – means an individual who is authorized to access the DIS.
- 2.21. **User Organization** – means the dispensing physician or a pharmacy whose employees access the DIS.

3. POLICY OBJECTIVES

This policy:

- 3.1. Defines the mutual responsibilities of the DIS Program and Users of the DIS and ensures they are aware of the rules associated with accessing and providing access to the DIS; and,
- 3.2. Assists in the protection of privacy with respect to the personal health information collected, used, disclosed and retained in the DIS.

4. APPLICATION

- 4.1. This policy applies to User Organizations and DHW as defined in section 2.
- 4.2. This policy does not apply to:
 - a) Pharmacy software vendors
 - b) Individuals who are clients of a user organization
- 4.3. The information stored in the DIS is subject to legislation and regulations which includes the:
 - Personal Health Information Act (PHIA);
 - Freedom of Information and Protection of Privacy Act (FOIPOP);
 - Personal Information Protection and Electronic Documents Act (PIPEDA);
 - Pharmacy Act and associated regulations
 - Prescription Monitoring Act;
 - Medical Act; and,
 - any other legislation relevant to the use and access of the DIS.

5. POLICY DIRECTIVES

5.1. User Connection to the DIS

Acceptance of the Policy

- 5.1.1. The *Confirmation of Acceptance Form* attached at Schedule A must be signed by the User Organization before the DIS Program provides the User Organization with access to the DIS.
- 5.1.2. If the User Organization is closing or changing ownership, it is the responsibility of the User Organization to notify the DIS Program within 30 days in advance of transfer/closing.

Changes to the Policy

- 5.1.3. This policy shall be amended as necessary with review at least every two years.
- 5.1.4. Notification of any required changes to this policy will be made available through the DIS Website and by other electronic means no less than 60 days in advance of updating the policy.

Notice of Termination

- 5.1.5. A User Organization may terminate acceptance of this policy with 30 days' notice by sending a written notice of termination by registered mail to the DIS Program Director.

Access to the Policy

- 5.1.6. A current version of the policy will be available on the DIS Website.

Collection, Use, and Disclosure of Personal Health Information in the DIS

- 5.1.7. Collection, use, and disclosure of personal health information within the DIS will be in accordance with PHIA. Collection, use, or disclosure of personal health information within the DIS for any other purpose is strictly prohibited.

5.2. Responsibilities of the DIS Program

DIS Service and Support

- 5.2.1. The DIS Program will make all reasonable efforts to provide DIS services and support to the User Organization. Hours of support and procedures for obtaining support are available on the DIS Support Website.
- 5.2.2. The DIS Program is responsible for the support of all DIS-related software, hardware, and infrastructure that lies within the nshealth.ca network.
- 5.2.3. The Information Services Support Provider is the single point of contact for support services on behalf of the DIS Program.

DIS Support – Remote Access

- 5.2.4. The Information Services Support Provider will collaborate with User Organizations on the appropriate use of software that may be required to provide remote support for the DIS, if necessary.

Communication of Service and Support Notices

- 5.2.5. The DIS Program is responsible for ensuring timely communication of DIS-related notifications to Pharmacy Software Vendors, corporate pharmacy support groups, and User Organizations. Notifications may include or be related to:
 - The timing of the maintenance window;
 - Scheduled downtime (outside the maintenance window);
 - Unscheduled downtime;
 - Persistent system issues;

- Critical incidents and resolutions;
 - System upgrades;
 - Education updates;
 - Updates to policies, procedures, and guidelines; and,
 - Any other DIS-related event that may affect the operations of the User Organization.
- 5.2.6. The DIS Program shall provide reasonable notice to Pharmacy Software Vendors, corporate pharmacy support groups, and User Organizations of scheduled downtime outside of the regular maintenance window.
- 5.2.7. Deviations from scheduled downtimes along with status updates will be communicated to Pharmacy Software Vendors, corporate pharmacy support groups, and User Organizations.

Network Connections

- 5.2.8. The DIS Program will provide User Organizations with access to the DIS via static IP addresses. Where the technology is not available, it will be treated as an exception and an alternative will be determined.

Privacy of Personal Health Information in the DIS

- 5.2.9. DHW shall be ultimately responsible for ensuring that the privacy of the personal health information collected, used, disclosed, and retained by the DIS is maintained in compliance with PHIA.

Monitoring/Security and Privacy Breaches/Complaints

- 5.2.10. DHW reserves the right to monitor and audit the use of the DIS access connections and to employ any tools and applications it may deem appropriate to assist in monitoring and auditing.
- 5.2.11. Collection and use of DIS data will be tracked, logged, and subject to audit. All overrides of Consent Directives will also be tracked, logged, and subject to audit.
- 5.2.12. The DIS Program reserves the right to suspend or terminate the access of any User Organization without notice, at the sole discretion of the DIS Program, to protect the security of the nshealth.ca network and/or the privacy of the personal health information in the DIS.
- 5.2.13. In the event of a suspected breach of privacy or security, the DIS Program will follow the DHW Privacy Breach Protocol which may require the DIS Program to contact and collaborate with the User Organization representative responsible for privacy and security to conduct an investigation. The DIS Program should also follow the recommendations outlined in the *DIS Privacy and Security Guidelines for Best Practices*, attached to this Policy as Schedule B.
- 5.2.14. The PAO reserves the right to follow-up on, and investigate where necessary, any notifications or suspicions of privacy breaches, and any privacy concern with respect to the DIS.

Integrity of Data

- 5.2.15. The DIS Program in collaboration with the Information Services Support Provider will ensure that processes, procedures, and controls are in place to maintain the integrity of DIS data within its custody.

DIS Program Accountabilities

- 5.2.16. The DIS Program shall identify one or more individuals who will be responsible for the monitoring of privacy and security of DIS data.
- 5.2.17. The DIS Program shall designate Users employed by or associated with the DIS Program who are authorized to access, collect, use, and disclose personal health information within the DIS. The DIS Program accepts responsibility for ensuring their authorized Users comply with this Policy and do not improperly access, use, disclose, dispose, or destroy DIS data.
- 5.2.18. The DIS Program shall appoint an individual employed by or associated with the DIS Program who will be responsible to manage and designate Users and User roles for DHW.

Education

- 5.2.19. The DIS Program is responsible to maintain education on the appropriate use of the DIS and the appropriate procedures for the collection, use, and disclosure of DIS data.

Maintaining a Public DIS Website

- 5.2.20. The DIS Program shall maintain a public DIS Website which shall provide information that is useful and informative to the public about the DIS Program.
- 5.2.21. The DIS Program shall make reasonable efforts to ensure that the public DIS Website is available to the public via the internet on a 24x7x365 basis.

Maintaining a DIS Support Website

- 5.2.22. The Information Services Support Provider will make a DIS Support Website available which will provide useful information, notifications, and services to Pharmacy Software Vendors, corporate pharmacy support groups, and User Organizations.
- 5.2.23. The Information Services Support Provider will make a reasonable effort to ensure the DIS Support Website is available on a 24x7x365 basis, with the exception of scheduled downtimes, and is supported for incident resolution from Monday – Friday (excluding statutory holidays) from 8 am – 4 pm.

Confidentiality Agreement

- 5.2.24. DHW must sign the *Confidentiality Agreement* attached to this Policy at Schedule C.

- 5.2.25. The DIS Program shall ensure that all Users employed by DHW who require access to the DIS also sign confidentiality agreements that address the privacy and security of any DIS proprietary information or personal health information and verifies that they have read this Policy document and all Provincial Privacy and Security Policies applicable to the access to and use of the DIS, such as:
- Government Privacy Policy (Province)
 - Joint Privacy Policy (Executive Council Office, Treasury Board Office, Office of Policy and Priorities, Chief Information Office)
- 5.2.26. The DIS Program shall ensure that all Users affiliated with DHW and DHW Contractors who require access to the DIS also sign confidentiality agreements that address the privacy and security of any DIS proprietary information or personal health information and verifies that they have read the *DIS Privacy and Security Guidelines for Best Practices*, attached to this Policy document at Schedule B.

5.3. Responsibilities of the User Organization

Dispensing

- 5.3.1. User Organizations are required to send all dispenses, only for humans, to the DIS.

Transactions Completed During Outages

- 5.3.2. User Organizations must ensure that all DIS supported transactions completed (excluding queries) during a DIS outage are sent to the DIS within a mutually agreed time frame once the system is made available, in a manner that does not unduly interfere with the User Organization's business operations.

Business Continuity Plan

- 5.3.3. User Organizations are responsible for their own business continuity plans to support their pharmacy business processes when the DIS is unavailable.

Providers

- 5.3.4. Users must ensure they use the provider's license number when dispensing prescriptions for providers licensed in Nova Scotia. A Default Provider must only be used for situations where the provider is licensed outside of Nova Scotia and is not registered with the NSPMP.

User Organization Accountabilities

- 5.3.5. Each User Organization will be responsible for the individuals and the activities of the individuals within their organization who are authorized to access, collect, use, and disclose personal health information within the DIS. Each User Organization accepts responsibility for ensuring their authorized Users comply with this Policy.
- 5.3.6. The Pharmacy Manager of each licensed pharmacy within the User Organization shall be the central point of contact for the DIS Program for all audit, privacy, security, user access and data quality related matters.

- 5.3.7. Each User Organization may also appoint a User Organization privacy and security representative(s) who, in conjunction with the Pharmacy Manager, will be responsible for:
- Privacy and security of personal health information within the User Organization;
 - Receiving reports and communication related to any suspected or confirmed privacy breaches involving the personal health information within the User Organization; and
 - Collaborating with the PAO to investigate and contain suspected breaches of privacy or security.
- 5.3.8. Each User Organization may also appoint a User Organization approver(s) who, in conjunction with the Pharmacy Manager, will be responsible to:
- Manage the User roles for the User Organization; and
 - Verify that each User with permission to access the DIS is properly authorized for a particular role and has all necessary licenses and authorities associated with that role.
- 5.3.9. The User Organization approver, privacy and security representative, and Pharmacy Manager may be the same individual.
- 5.3.10. The User Organization shall provide the DIS Program with the contact information for approver, privacy and security representative, and Pharmacy Manager, and notify the DIS Program of any updates to the contact information.
- 5.3.11. The User Organization is responsible for providing the Information Services Support Provider with updated contact information for its locations in order to facilitate DIS support when necessary.
- 5.3.12. Where DIS data is disclosed to the User Organization through a system to system interface, the User Organization agrees to utilize Pharmacy Software that supports the defining of appropriate User roles as suggested in the *DIS Privacy and Security Guidelines for Best Practices*, attached to this Policy document at Schedule B.

Network Connections

- 5.3.13. Unless the technology is not available, User Organizations will access the DIS via static IP addresses provided by Internet Service Providers, (e.g. Bell Aliant/Eastlink).

Accuracy of Data

- 5.3.14. Each User Organization will be responsible for ensuring that any data collected and provided by the User Organization and its Users is reasonably accurate, and that the User Organization has taken reasonable steps to ensure the accuracy of data disclosed to the DIS.

- 5.3.15. Where necessary, User Organizations will collaborate with the Information Services Support Provider to make corrections to data.
- 5.3.16. In the interest of individuals' safety, Dispensary Staff should:
- Only add an individual to the CR if an individual cannot be located; and,
 - Notify the Information Services Support Provider of any potential duplicate and non-human records that may exist or which the User Organization becomes aware, within the DIS in order that triage and data remediation take place.

Consent Directives and Overrides

- 5.3.17. In accordance with Section 17 of PHIA, the DIS program will implement a process to facilitate Consent Directives from individuals who may want to revoke consent for the DIS to disclose their personal health information. This process will mask all of the patient's DIS profile except demographic information.

There are two reasons under which authorized users can override a Consent Directive to temporarily view (un-mask) an individual's personal health information:

- When the patient is in need of healthcare and accessing the DIS will avert or minimize an imminent and significant danger to the health or safety of a patient; or,
- When the patient provides consent to override their directive.

Once a user has overridden a patient's consent directive, the patient's personal health information in SHARE may be viewed by that user. Viewing a patient's personal health information after overriding a consent directive is subject to the terms and conditions of the *Personal Health Information Act* and its regulations, this policy and all other applicable legislation, policies, procedures and guidelines.

Note: All instances of overriding a Consent Directive will be automatically flagged by the DIS for audit.

DIS Support

- 5.3.18. User Organizations are responsible for the support of all software, hardware, and infrastructure that lies outside of the nshealth.ca network.

DIS Support – Remote Access

- 5.3.19. The User Organization and the Information Services Support Provider will collaborate on the appropriate use of software that may be required to provide remote support for the DIS, if necessary.

User Training/ Education

- 5.3.20. Each User Organization is responsible to facilitate education recommended by the DIS Program within the User Organization.

- 5.3.21. Pharmacy system specific training must be completed by all User Organization staff who will be accessing the DIS.

Confidentiality Agreements

- 5.3.22. The User Organization must sign the *Confidentiality Agreement* attached to this Policy as Schedule C.

Monitoring Access/ Security and Privacy Breaches/ Complaints

- 5.3.23. The User Organization shall monitor access of its staff to the DIS to ensure proper access, use, and disclosure of personal health information in the DIS.
- 5.3.24. The User Organization shall advise the DHW Privacy and Access Office if the User Organization becomes aware of or reasonably suspects that there has been a privacy or security breach, or if a client or other individual has raised a privacy or security concern with respect to the DIS.
- 5.3.25. The User Organization should follow the recommendations outlined in the *DIS Privacy and Security Guidelines for Best Practices*, attached to this Policy document as Schedule B.

5.4. Joint Responsibilities of DHW and the User Organization

User Access

- 5.4.1. Users must only access the DIS for the purpose of providing and supporting health care and technical support when necessary.
- 5.4.2. Users shall not access the DIS from outside Canada or transfer information from the DIS to locations/computer systems/networks outside of Canada unless prior written approval has been received from DHW.

Individual Access / Amendments to their Personal Health Information

- 5.4.3. Individuals have the right to access their personal health information stored in the DIS.
Individuals may submit requests to the PAO for a copy of their personal health information stored in the DIS.
- 5.4.4. Individuals have the right to request corrections to their personal health information stored in the DIS.
 - 5.4.4..1. Where necessary and appropriate, the PAO may refer the patient to the User Organization or may consult with the User Organization which entered the data.
 - 5.4.4..2. User Organizations will only make amendments to personal health information stored in the DIS after receiving consent from the subject individual.
 - 5.4.4..3. The PAO retains the authority to determine what type of amendment should be made if an individual's request is not, or cannot be addressed to the satisfaction of the individual by the User Organization.

- 5.4.5. Individuals may submit requests to the PAO for a record of user activity related to an individual's personal health information stored in the DIS.
- 5.4.6. Individuals may submit complaints to the PAO regarding the privacy of their personal health information stored in the DIS.

6. POLICY GUIDELINES

N/A

7. ACCOUNTABILITY

- 7.1. For the purpose of the administration of this policy, accountability is delegated to the Deputy Minister of Health and Wellness.
- 7.2. The Senior Executive Director of Corporate Service and Asset Management, or designate, has responsibility for ongoing monitoring and enforcement of this policy.

8. MONITORING / OUTCOME MEASUREMENT

- 8.1. The DIS Program Director will monitor the implementation, performance, and effectiveness of this policy.

9. REPORTS

N/A

10. REFERENCES

- 10.1. *Personal Health Information Act (PHIA)*
- 10.2. *Freedom of Information and Protection of Privacy Act (FOIPOP)*
- 10.3. *Personal Information Protection and Electronic Documents Act (PIPEDA)*
- 10.4. *Pharmacy Act* and associated regulations
- 10.5. *Prescription Monitoring Act*
- 10.6. *Medical Act*

11. APPENDICES

- 11.1 Schedule A – Drug Information System Joint Service & Access Policy (Pharmacies and Dispensing Physician) – Confirmation of Acceptance Form
- 11.2 Schedule B – Drug Information System Privacy and Security Guidelines for Best Practices
- 11.3 Schedule C – Drug Information System Confidentiality Agreement (Pharmacies and Dispensing Physician)
- 11.4 Appendix A - Employee Confidentiality Form

12. VERSION CONTROL

Version Control:	Version 3, April 1, 2016 – Updates including administrative amendments, additional responsibilities
------------------	---

for Pharmacy Managers, changes to the roles of Privacy and Security Representatives, and clarification of the consent override functionality.

Version 2, July 4, 2014, Administrative Amendments, replaces all previous versions.

Suspected or confirmed privacy breaches are now reported to the Privacy and Access Office, and the privacy contact for each party is now provided to the DIS Program.

13. INQUIRIES

- 13.1. DIS Program Director
DIS Program
Nova Scotia Department of Health and Wellness
Tel. (902) 424-7270
Fax (902) 428-2446
Email DIS@novascotia.ca



Schedule A
Drug Information System Joint Service and Access Policy
(Pharmacies and Dispensing Physician)
Confirmation of Acceptance

By signing below, I confirm that I have reviewed and accepted the attached Department of Health and Wellness, Drug Information System (DIS), Joint Service and Access Policy (Issue: October 23, 2013).

Notification of any required changes to this policy will be made available through the DIS website (<http://novascotia.ca/dhw/dis>) and by other electronic means no less than 60 days in advance of updating the policy. A current version of the policy will be available on the DIS website.

This confirmation of acceptance may be terminated by the User Organization(s) with 30 days' notice by sending a written notice of termination by registered mail to the DIS Program Director, 44-1894 Barrington Street, Halifax, NS, B3J 2A8.

User Organization: _____

Authorized Signature: _____

Printed Name and Title: _____

Address: _____

City: _____ Province: _____

Postal Code: _____ Email Address: _____

Phone: _____ Fax: _____

Alternate Contact (if applicable): _____

Alternate Phone (if applicable): _____

Date: _____

Completed confirmation of acceptance forms must be faxed to: 1 (902) 407-3020.

Schedule B

Drug Information System Privacy and Security Guidelines for Best Practices

1. Purpose

- 1.1. The purpose of this guideline document is to provide users of the Drug Information System (DIS) with recommended practices to help maintain the confidentiality, integrity, and availability of information collected, used, disclosed, and retained by the DIS.

2. Recommended Security Safeguards

User ID and Passwords

- 2.1. Pharmacy Software User ID's should be uniquely identifiable.
- 2.2. Passwords should be at least 8 characters long.
- 2.3. Passwords should contain characters from at least two of the following classes:
- English upper case letters A, B, C, ...Z
 - English lower case letters a, b, c, ...z
 - Westernized Arabic numerals 0, 1, 2, ... 9
 - Non-alphanumeric characters { } [], . , ° ; : ' ? \ ^ ~ ! # \$ % ^ & * () _ - + =
- 2.4. Passwords should not be constructed using only the following:
- Username or User ID
 - Any of the user's names
 - Names of family, pets, friends
 - Email addresses or part thereof
 - Words found in a dictionary
 - Birthday, address, phone numbers
 - Cities
 - Company name and derivatives
 - Letter patterns like QWERTY, ZXCVBN
 - Computer terms
 - Any of the above preceded or followed by a digit (e.g., 1Halifax or Halifax1)
- 2.5. User accounts should be locked-out after 3-10 logon attempts. The lock-out can be permanent or temporary. Temporary lock-outs should be at least one hour.
- 2.6. Users should change their password at least every 120 days.

- 2.7. Users should use a different password each time the password is changed. Pharmacy software systems should remember at least the previous 5 passwords and prevent the user from re-using them.
- 2.8. System and application default passwords should be replaced with strong passwords using the elements described in clauses 2.2 thru 2.4.
- 2.9. Administrator accounts should require strong passwords.
- 2.10. Guest accounts should be disabled.
- 2.11. Access to password files should be restricted.
- 2.12. Users should be reminded of the following regarding their passwords:
 - Don't reveal your password to anyone. This includes your boss, secretary, administrative assistant, family members, helpdesk staff, and co-workers while on vacation.
 - Don't use the same passwords for work and personal use (e.g. Facebook, Hotmail).
 - Don't talk about your password in front of anyone.
 - Don't reveal your password over the phone to anyone.
 - Don't reveal your password in an email message.
 - Don't hint at the format of your password.
 - Don't write your password down.
 - Don't store your password in your office, near your computer or on your computer or phone.
 - Don't reveal your password on questionnaires or security forms.
 - Don't use the "remember password" feature that your browser or some other applications have.

Workstation Controls

- 2.13. Users should take reasonable precautions to ensure that, if confidential information is displayed on a computer screen, the information is not visible to any person not authorized to view the information.
- 2.14. Where practical, users should not leave computers unattended when personal health information is accessible. Computers should be configured to enable screen locking when the system is idle or unattended. This screen lock should require a password to reactivate the screen.
- 2.15. Users should be restricted from saving, copying, or moving any files containing personal health information to their computer hard drive or other medium, e.g. a CD/DVD or USB key.

- 2.16. Operating system security patches should be applied to all computers in a timely fashion.
- 2.17. Virus protection software should be installed on all computers in the pharmacy and should be configured to receive automatic updates of virus definition files.
- 2.18. Host based firewalls (e.g. Windows firewall) should be enabled on workstations and only applications that are necessary for business should be allowed.
- 2.19. Portable computers such as laptops/notebooks should be fitted with physical lockdown devices. These devices are similar to bicycle locks for portable computers.
- 2.20. Personal use of the Internet should be discouraged from workstations which connect to the DIS.

User Roles

- 2.21. User accounts in the Pharmacy Software systems should be role-based.
- 2.22. User Roles should be mapped to authorized levels of access to personal health information.

Access Logs

- 2.23. All access to personal health information stored in the DIS is logged and all users of the DIS should be made aware of this.
- 2.24. Access logs should be reviewed regularly to ensure reasonable access to data by authorized users only and to review login and logout attempts including failed attempts. This review function may be automated using tools that search log files and report defined suspicious activity on an ongoing basis.

Audit

- 2.25. Privacy and security audits of pharmacy software systems should be carried out annually or more frequently.
- 2.26. Audits should include the analysis of privacy and security controls and the access to and use of pharmacy software systems.

Networking

- 2.27. A firewall should be implemented to protect the network within the User Organization.
- 2.28. An analysis should be conducted to identify any weaknesses and vulnerabilities related to any wireless networks used by the User Organization and mitigations should be identified and implemented where necessary.
- 2.29. The User Organization should take all reasonable and practicable steps to ensure that all devices connected to the nshealth.ca network use the most up-to-date firewall and anti-virus software and that virus definition patterns are kept current.
- 2.30. User Organizations should work with their Internet Service Provider to ensure internet connections are of sufficient bandwidth to support efficient access to the DIS and any other internet access requirements they may have.

3. Recommended Privacy Safeguards

Confidentiality Agreements

- 3.1. User Organizations and Pharmacy Software Vendors should maintain copies of confidentiality agreements signed by staff who require access to the DIS.

Patient Consent

- 3.2. Dispensing staff should ensure that personal health information obtained from the DIS is not disclosed outside the patient's circle of care without consent of the patient or the patient's substitute decision-maker.

New Patients

- 3.3. Dispensing staff should obtain the Health Card Number (HCN) or equivalent whenever possible from the patient for encounters that result in queries to the DIS. Searching for a patient by HCN (or equivalent) is the most effective way to locate the patient in the Client Registry.
- 3.4. Only add an individual to the Client Registry (CR) if an individual cannot be located.

Service Desk

- 3.5. Calls to a service desk and resulting service desk tickets should not include personal health information.

- 3.6. Where necessary, personal health information should be sent to support staff via secure methods only (e.g. secure email, secure file transfer).

Privacy Breaches

- 3.7. In addition to audit logs, a record should be maintained of every privacy and security breach that may have occurred in the DIS and this record should include details of all corrective procedures taken to diminish the likelihood of future privacy and security breaches.

Printed Information

- 3.8. If it is necessary to print reports and listings of data from the DIS that may include personal health information these should only be printed, displayed, stored, and reviewed in restricted, secured locations to which only authorized users have access.



Appendix A

Employee Confidentiality Agreement

Privacy of Personal Health Information

The Drug Information System (DIS) Program of the Department of Health and Wellness (DHW) along with *<Name of User Organization>* are committed to the protection of the privacy of patients' personal health information. All *<Name of User Organization>* users authorized to access the DIS are responsible for protecting the confidentiality of all patients' personal health information that is collected, used, disclosed, retained or disposed in the course of his/her work or association with the *<Name of User Organization>*. Authorized users of *<Name of User Organization>* are therefore required to sign this pledge of confidentiality:

Pledge of Confidentiality

I hereby pledge to hold in confidence all matters that come to my attention while working in *<Name of User Organization>* or during my association with *<Name of User Organization>*. I will observe and comply with the Joint Service and Access Policy of the DIS Program of the DHW and all policies of *<Name of User Organization>*. Except when I am legally authorized or required to do so as part of my job/association, I will not access or disclose or give to any person any information that comes to my knowledge or possession by reason of having access to the DIS.

I understand my obligations to keep personal health information confidential survives any association with *<Name of User Organization>*.

I acknowledge that any breach of confidentiality or inappropriate use of information obtained through access to the DIS may result in disciplinary action including dismissal and/or a report to my professional regulatory body.

Signature: _____

Date: _____

Name (please print): _____

Signature of Witness: _____

Date: _____

Name of Witness (please print): _____