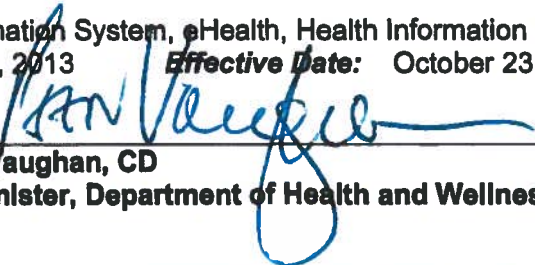



NOVA SCOTIA
Health and Wellness

Policy: Joint Service and Access Policy (Pharmacy Software Vendors)

Originating Branch: Drug Information System, eHealth, Health Information Office
Original Approval Date: October 23, 2013 **Effective Date:** October 23, 2013
Approved By: 

Dr. Peter Vaughan, CD
Deputy Minister, Department of Health and Wellness

Version #: 2

1. POLICY STATEMENT

- 1.1. The policy for access and privacy with respect to the Drug Information System (DIS) and Pharmacy Software Vendors is developed and maintained by the DIS Program as part of the Health Information Office (HIO) of the Nova Scotia Department of Health and Wellness (DHW).
- 1.2. 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;*
 - *Prescription Monitoring Act;*
 - *Medical Act;* and,
 - any other legislation relevant to the use and access of the DIS.

2. DEFINITIONS

In this policy:

- 2.1. **Conformance Testing** – means the process used to verify that Pharmacy Software System integration with the DIS system meets required specifications.
- 2.2. **DHW Contractors** – persons or organizations employed by DHW under contract to provide a specific service or support e.g. Deltaware or staff of Deltaware.

Joint Service and Access Policy (Pharmacy Software Vendors)

- 2.3. **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.
- 2.4. **DIS Support Website** – means the internet website maintained by Health Information Technology Services Nova Scotia (HITS-NS) for the purpose of providing information related to the support of the DIS.
- 2.5. **DIS Website** – means the internet website maintained by the DIS Program for the purpose of providing information related to the DIS Program.
- 2.6. **Health Card Number (HCN)** – means a unique identifier that provides access to provincial health care services in Nova Scotia.
- 2.7. **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.
- 2.8. **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
- 2.9. **Pharmacy Software** – means an electronic application that manages prescription dispenses and other pharmacy healthcare services.
- 2.10. **Pharmacy Software Vendor** – means a company which provides and supports a pharmacy or dispensing physician with Pharmacy Software.
- 2.11. **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.
- 2.12. **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.
- 2.13. **Re-conformance** – means a repeat of Conformance Testing.
- 2.14. **User** – means an individual who is authorized to access the DIS.
- 2.15. **User Organization** – means the dispensing physician or a pharmacy whose employees access the DIS.

Joint Service and Access Policy (Pharmacy Software Vendors)

- 2.16. **VIG** – means the DIS Vendor Implementation Guide (Pharmacy Software Vendors).

3. POLICY OBJECTIVES

This policy:

- 3.1. Defines the mutual responsibilities of the DIS Program and Pharmacy Software Vendors 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 Pharmacy Software Vendors and DHW as defined in section 2.
- 4.2. This policy does not apply to:
- a) User organizations
 - b) Individuals who are clients of a user organization

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 Pharmacy Software Vendor before the DIS Program provides DIS access to a User Organization utilizing the Pharmacy Software Vendor's software.

Changes to the Policy

- 5.1.2. 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

- 5.1.3. A Pharmacy Software Vendor 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

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

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

- 5.1.5. 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

Conformance Testing

5.2.1. The DIS Program will provide Pharmacy Software Vendors with access to the DIS conformance environments as required.

Re-conformance

5.2.2. HITS-NS will notify the DIS Program when a patch or update to Pharmacy Software will have an impact on integration with the DIS.

5.2.3. The DIS Program will collaborate with HITS-NS and the Pharmacy Software Vendors to determine under which circumstances and timeframes Re-conformance testing will be required. (Refer Section 5.3.4).

DIS Service and Support

5.2.4. The DIS Program will make all reasonable efforts to provide DIS services and support to User Organizations. Hours of support are posted on the DIS Support Website.

5.2.5. The DIS Program is responsible for the support of all software, hardware, and infrastructure that lies within the nshealth.ca network.

5.2.6. The DIS Program will make all reasonable efforts to provide Pharmacy Software Vendors with access to the DIS sandbox environment on a 24x7x365 basis.

5.2.7. HITS-NS is the single point of contact for support services on behalf of the DIS Program.

5.2.8. If necessary, HITS-NS will collaborate with the Pharmacy Software Vendor to resolve any technical issues that may hamper the ability to provide DIS Service to a User Organization.

5.2.9. Except in the case of an emergency, if it becomes necessary to apply a patch or update to the DIS software, HITS-NS will provide notification in a timely manner to Pharmacy Software Vendors.

5.2.10. In the event of an emergency where it becomes necessary to apply a patch or update to the DIS software, HITS-NS will make all reasonable efforts to provide notification to Pharmacy Software Vendors.

DIS Support – Remote Access

5.2.11. HITS-NS 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

5.2.12. 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.

5.2.13. The DIS Program shall provide notice to Pharmacy Software Vendors, corporate pharmacy support groups, and User Organizations of scheduled downtime outside of the regular maintenance window.

5.2.14. Deviations from scheduled downtimes along with status updates will be communicated to Pharmacy Software Vendors, corporate pharmacy support groups, and User Organizations.

Network Connections

5.2.15. 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

5.2.16. 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

5.2.17. 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.

5.2.18. Collection and use of DIS data will be tracked, logged, and subject to audit.

5.2.19. 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.

5.2.20. 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 Pharmacy Software Vendor and/or the User Organization representative(s) 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 document at Schedule B.

- 5.2.21. 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

- 5.2.22. The DIS Program in collaboration with HITS-NS will ensure that processes, procedures, and controls are in place to maintain the integrity of DIS data within its custody.

DIS Program Accountabilities

- 5.2.23. The DIS Program shall identify one or more individuals who will be responsible for the monitoring of privacy and security of DIS data.
- 5.2.24. 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.
- 5.2.25. 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

- 5.2.26. 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

- 5.2.27. 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.
- 5.2.28. 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

- 5.2.29. HITS-NS 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.
- 5.2.30. HITS-NS 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

- 5.2.31. DHW must sign the *Confidentiality Agreement* attached to this Policy at Schedule C.
- 5.2.32. 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)
- 5.2.33. The DIS Program shall ensure that all Users associated 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 Section 5.3 of this Policy document and the *DIS Privacy and Security Guidelines for Best Practices*, attached to this Policy document at Schedule B.

5.3. Responsibilities of the Pharmacy Software Vendor

DIS Vendor Implementation Guide (VIG)

- 5.3.1 The Pharmacy Software Vendor shall make a reasonable effort to follow the implementation requirements outlined in the DIS VIG.

Conformance Testing

- 5.3.2 The Pharmacy Software Vendor must successfully complete conformance testing as per specifications before a User Organization which uses the Pharmacy Software Vendor's Pharmacy Software can be connected to the DIS.

Re-conformance

- 5.3.3 The Pharmacy Software Vendor must provide HITS-NS with release notes prior to any patches or updates to Pharmacy Software that will have an impact on the integration with the DIS.
- 5.3.4 Vendors understand that Re-conformance will be required in any of the following circumstances:
- as part of an update to the DIS where it is determined that the update will have an impact on the integration with Pharmacy Software; or,
 - as part of an update to Pharmacy Software that will have an impact on the integration with the DIS.

The need and extent of Re-conformance will be determined by the DIS Program in collaboration with HITS-NS and Pharmacy Software Vendors, depending on the nature of the update and the impact on the integration with the DIS.

Pharmacy Software Vendor Accountabilities

- 5.3.5 Each Pharmacy Software Vendor shall appoint a Pharmacy Software Vendor representative(s) who will be responsible for privacy and security of the DIS within the Pharmacy Software Vendor organization.
- 5.3.6 Each Pharmacy Software Vendor will be responsible for the individuals and the activities of the individuals within their organization who provide support to the DIS. Each Pharmacy Software Vendor accepts responsibility for ensuring their authorized Users comply with this Policy.
- 5.3.7 Each Pharmacy Software Vendor shall appoint a Pharmacy Software Vendor approver(s) who will be responsible to manage the user roles for authorized individuals accessing the DIS production environment for the purpose of providing support.
- 5.3.8 Each Pharmacy Software Vendor approver will be responsible to verify that each User with permission to access the DIS production environment is properly authorized for a particular role and has all authorities associated with that role.
- 5.3.9 The Pharmacy Software Vendor representative responsible for privacy and security of the DIS and the Pharmacy Software Vendor approver may be the same individual.
- 5.3.10 The Pharmacy Software Vendor shall provide the DIS Program with the contact information for its Pharmacy Software Vendor representative responsible for privacy and security of the DIS and its Pharmacy Software Vendor approver and notify DIS Program of any updates to the contact information.
- 5.3.11 Where DIS data is disclosed to User Organizations through a system to system interface, the Pharmacy Software Vendor 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 as Schedule B.

User Access

- 5.3.12 Pharmacy Software Vendors must not access the DIS for purposes other than providing technical support.
- 5.3.13 Pharmacy Software Vendors 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 the Province.

Joint Service and Access Policy (Pharmacy Software Vendors)

DIS Support

- 5.3.14 User Organizations are responsible for the support of all software, hardware, and infrastructure that lies outside of the nshealth.ca network.
- 5.3.15 Pharmacy Software Vendors will collaborate with HITS-NS to resolve issues where it is unclear if an issue is with the DIS or with the Pharmacy Software.

User Training/Education

- 5.3.16 Pharmacy Software Vendors are responsible to provide Pharmacy Software specific training within User Organizations.

Confidentiality Agreements

- 5.3.17 The Pharmacy Software Vendor must sign the *Confidentiality Agreement* attached to this Policy as Schedule C.

Monitoring Access/Security and Privacy Breaches/Complaints

- 5.3.18 The Pharmacy Software Vendor shall monitor access of its staff to the DIS to ensure appropriate access and use of the DIS.
- 5.3.19 The Pharmacy Software Vendor shall advise the DHW, Privacy and Access Office if the Pharmacy Software Vendor becomes aware of or reasonably suspects that there has been a security or privacy breach with respect to the DIS.
- 5.3.20 Where applicable, the Pharmacy Software Vendor should follow the recommendations outlined in the *DIS Privacy and Security Guidelines for Best Practices*, attached to this Policy document at Schedule B.

Privacy and Security Safeguards

- 5.3.21 Through Pharmacy Software design, configuration, training, and support, the Pharmacy Software Vendor shall assist the User Organization in following the recommendations outlined in the *DIS Privacy and Security Guidelines for Best Practices*, attached to this Policy document at Schedule B.

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 Executive Director of eHealth, HIO or designate, has responsibility for on going monitoring and enforcement of this policy.



Schedule A
Drug Information System Joint Service and Access Policy
(Pharmacy Software Vendors)
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 Pharmacy Software Vendor with 30 days' notice by sending a written notice of termination by registered mail to the DIS Program Director, 4th Floor Barrington Tower, 1894 Barrington Street, PO Box 488, Halifax, NS, B3J 2R8.

Pharmacy Software Vendor: _____

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, ZXCVCBN
 - 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 or equivalent whenever possible from the patient for encounters that result in queries to the DIS.

Service Desk

- 3.4. Calls to a service desk and resulting service desk tickets should not include personal health information.
- 3.5. Where necessary, personal health information should be sent to support staff via secure methods only (e.g. secure email, secure file transfer).

Privacy Breaches

- 3.6. 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

- 3.7. 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 Pharmacy Software Vendor> are committed to the protection of the privacy of patients' personal health information. All <Name of Pharmacy Software Vendor> 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 Pharmacy Software Vendor>. Authorized users of <Name of Pharmacy Software Vendor> 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 Pharmacy Software Vendor> or during my association with <Name of Pharmacy Software Vendor>. 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 Pharmacy Software Vendor>. 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 Pharmacy Software Vendor>.

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.

Signature: _____

Date: _____

Name (please print): _____

Signature of Witness: _____

Date: _____

Name of Witness (please print): _____