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 PMP.

User Organization Accountabilities

5.3.5 Each User Organization shall appoint a User Organization representative(s) who will be responsible for privacy and security of personal health information within the User Organization.

5.3.6 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.

5.3.7 Each User Organization shall appoint a User Organization approver(s) who will be responsible to manage the User roles for the User Organization.

5.3.8 Each User Organization approver will be responsible to 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 representative responsible for privacy and security of personal health information and the User Organization approver may be the same individual.

5.3.10 The User Organization shall provide HITS-NS with the contact information for its User Organization representative responsible for privacy and security of personal health information and its User Organization approver and notify HITS-NS of any updates to the contact information.

5.3.11 The User Organization is responsible for providing HITS-NS 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 HITS-NS 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 HITS-NS of any potential duplicate and non-human records that may exist of 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 health-care providers can override a Consent Directive to 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.

Only Users who are regulated health professionals have the authority to override a Consent Directive to allow access to an individual's masked data in the DIS. Once an individual's masked data is accessed, Dispensary Staff within the individual's circle of care may view the profile under the authority of the regulated health care professional.

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 HITS-NS 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 at 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 HITS-NS 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 at Schedule B.