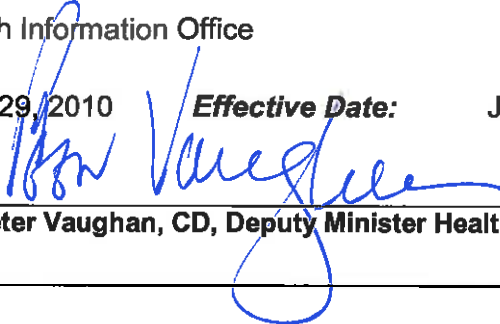


NOVA SCOTIA
Health and Wellness

Policy: SHARE Privacy and Security Policy

Originating Branch: Health Information Office

Original Approval Date: June 29, 2010 **Effective Date:** July 1, 2015

Approved By: 
Dr. Peter Vaughan, CD, Deputy Minister Health and Wellness

Version #: 2

1. POLICY STATEMENT

- 1.1. In managing personal health information, a key objective is to provide timely and secure access to all relevant aspects of a patient's health history in a manner that respects patient rights to privacy and confidentiality. The Department of Health and Wellness (DHW) has a responsibility to:
- 1.1.1. protect the privacy of each individual whose information they manage; and,
 - 1.1.2. establish requirements for information systems used in the health-care system.
- 1.2. Protection of privacy is the individual responsibility of every user of SHARE.
- 1.3. The information stored in SHARE is subject to legislation and regulations which includes the:
- *Health Authorities Act;*
 - *Freedom of Information and Protection of Privacy Act (FOIPOP);*
 - *Personal Information Protection and Electronic Documents Act (PIPEDA);*
 - *Personal Information International Disclosure Protection Act (PIIDPA)*
 - *Personal Health Information Act (PHIA);*
 - *Nova Scotia Department of Health and Wellness Privacy Policy;*
 - *Nova Scotia Health Authority/IWK Information Protection and Privacy Breach Policy and Procedures; and,*
 - any other legislation relevant to the use and access of SHARE.
- 1.4. This policy is not breached in circumstances where a user is required to disclose personal information from SHARE pursuant to applicable laws or court orders.

2. DEFINITIONS

- 2.1. **Challenge and Response form:** a form filled out by each user and submitted to the information services support provider for the purpose of verifying a user's identity for password changes.
- 2.2. **Client Registry:** A component of the Nova Scotia Electronic Health Record, known as SHARE that contains demographic information for all patients who have received healthcare in Nova Scotia. The Client Registry supports patient identification and the retrieval of patient information from provincial health systems.
- 2.3. **Consent Directive:** Section 17.1 of PHIA states that "an individual may limit or revoke the individual's consent to the collection of personal health information or to the use or disclosure of personal health information in the custody or control of a custodian by notice to the custodian". This notice is referred to as a Consent Directive.
- 2.4. **Health Privacy Office (HPO):** 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. The HPO holds legislative responsibility for personal health information collected, used, disclosed, retained, disposed and destroyed by the DHW. The HPO may also be referred to as the Privacy and Access Office (PAO).
- 2.5. **Information Services Support Provider:** means the support organization for provincial health information technology applications that facilitate health care delivery in Nova Scotia.
- 2.6. **nshealth.ca:** 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.
- 2.7. **Organization:** means the Nova Scotia Health Authority, the IWK Health Centre, or a public or private organization that:
- 2.7.1. provides health care services in the Province of Nova Scotia and participates in the SHARE Program; or,
 - 2.7.2. provides support for and administration of SHARE.
- 2.8. **Personal Information:** means recorded information about an identifiable individual, including:
- name, address or telephone number;
 - race, national or ethnic origin, colour, religious or political beliefs or associations;
 - age, sex, sexual orientation, marital or family status;

- identifying number, symbol or other particular assigned to the individual (such as Health Card Number);
 - fingerprints, blood type or inheritable characteristics;
 - health care history, including physical or mental disability;
 - educational, financial, criminal or employment history;
 - anyone else's opinions about the individual; and/or
 - the individual's personal views or opinions, except if they are about someone else.
- 2.9. **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.
- 2.10. **Privacy Breach:** Any situation where personal information is collected, viewed, used, disclosed or retained in a way that is inconsistent with this policy and applicable privacy legislation. A privacy breach occurs when personal information is stolen, lost or subject to unauthorized access, use, disclosure or copying. This may include loss or unauthorized access to equipment and/or technology that is used for remote access to SHARE.
- 2.11. **Private Healthcare Organization (PHCO):** means a private sector association, partnership or person that provides health care services in the Province of Nova Scotia. It does not include public sector health care organizations, such as the Department of Health and Wellness, the Nova Scotia Health Authority or the IWK Health Centre.
- 2.12. **Remote access:** means access to the SHARE system residing on the nshealth.ca network from a PHCO location not directly connected to the nshealth.ca network, where a secure connection to the nshealth.ca network can be established.
- 2.13. **SHARE:** Nova Scotia's Electronic Health Record system, which is comprised of the following: Client Registry, Provider Registry, Clinical Repository, Clinical Portal and Drug Information System.
- 2.14. **User:** means an individual who is authorized to access SHARE.

3. POLICY OBJECTIVES

3.1. This policy:

- Defines the requirements or processes for allowing authorized users to access and print information within SHARE in a private and secure manner.
- Builds on existing requirements for policies, procedures and practices to protect the privacy of personal information, including, but not limited to requirements under FOIPOP, PHIA, PIPEDA and PIIDPA.

4. APPLICATION

4.1 This policy applies to all users of SHARE. There are two categories of users:

4.1.1. Individuals who have been granted access to SHARE:

- All policy directives apply to these users with the exception of directive 5.3.2

4.1.2. Employees of information services support providers who are involved in support and administration of SHARE, and employees of Medavie who are involved in data quality support for the Client Registry component of SHARE:

- All policy directives apply except 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.3.1 and 5.6

4.2. Nothing in this policy diminishes the existing privacy and confidentiality obligations on individuals with access to SHARE as defined in their employee contracts, confidentiality agreements with their employer, and the code of conduct, regulating legislation and relevant privacy legislation of their profession.

5. POLICY DIRECTIVES

5.1. Access to information in SHARE

User Access

5.1.1. No user shall be authorized to have access to SHARE until s/he has:

5.1.1.1. completed the mandatory privacy training;

5.1.1.2. completed and submitted an approved User Access Request Form; and,

5.1.1.3. signed a Conditions of Appropriate Use document (for public health care organizations) or a Remote Access / Terms of Use Agreement document (for private health care organizations).

PHCO Access

- 5.1.2. In addition to the requirements in 5.1.1, PHCOs are required to sign an Access Agreement before users in their organizations will receive access.
- 5.1.3. The Access Agreement shall be signed by the individual who has authority to sign on behalf of the PHCO and returned to DHW.
- 5.1.4. The individual who has authority to sign on behalf of DHW will sign the Access Agreement and return a copy of the Agreement to the PHCO

Access Restricted to Canada

- 5.1.5. Access to SHARE is prohibited from outside Canada unless a user has applied for and received permission from DHW in writing in advance of the access.

Secure Network Connection

- 5.1.6. DHW through the information services support provider will determine and support provincially appropriate technology solutions and/or mechanisms to be used to facilitate a secure remote connection to SHARE on the nshealth.ca network.
- 5.1.7. The information services support provider shall only support secure remote access connections to the nshealth.ca network that are endorsed by the information services support provider.
- 5.1.8. Prior to connecting to SHARE from a wireless network, users should review the inherent risks of wireless networks and ensure that safeguards are in place to minimize these risks.

Updated Technology

- 5.1.9. All computers that are connected to the nshealth.ca network via remote access technologies shall use up-to-date firewall, anti-virus and remote access software or similar session securing technology approved by the information services support provider. The computers shall have the latest system security patches as provided by the operating system's vendor.

5.2. Support

Unsupported software

- 5.2.1. Installation and use of any application software used to access SHARE remotely but which is not approved by DHW, is done so at the sole discretion of the private healthcare organization and its users. DHW and its information service support provider shall not be responsible for any technical (personal computer, network, internet, or other) problem encountered as a result of installation and/or use of said software.

PHCO-managed equipment

5.2.2. The information service support provider will provide technical expertise to users of remote access services. The information service support provider cannot, however, be responsible to resolve remote access problems related to the malfunction of PHCO-managed equipment.

Remote Support Software

5.2.3. The information service support provider will collaborate with PHCOs on the appropriate use of software that may be required to provide remote support, if necessary.

5.3. Authorized versus unauthorized access

Access for Health Care Purposes

5.3.1. A user is only authorized to access information in SHARE in the performance of the user's role within the health care system. Specifically, users may access and use information in SHARE when:

- 5.3.1.1. they are in a current care relationship with the individual who is the subject of the information,
- 5.3.1.2. they are providing health services to the individual either in the presence or absence of that individual,
- 5.3.1.3. their access to the information is necessary for the provision of the health service or for making a determination for a related health service, and
- 5.3.1.4. the information is related to and necessary for the current session of care.

Access to Provide Support

5.3.2. Employees of DHW and information services support providers with access to SHARE are only authorized to access SHARE information in the performance of their roles to provide support and administration of SHARE.

Unauthorized Access

5.3.3. Unauthorized access to information in SHARE is prohibited. Unauthorized access is defined as access to information in SHARE that is not required to perform the functions of a user's role as described in directives 5.3.1 and 5.3.2.

5.4. Consent Directives

5.4.1. In accordance with Section 17 of PHIA, processes may be implemented to facilitate consent directives from individuals who may want to revoke consent for the disclosure of their personal health information. There are two reasons under which authorized users can override a consent directive to disclose an individual's personal health information:

- When the patient is in need of healthcare and accessing SHARE will avert or minimize an imminent and significant danger to the health or safety of a patient; or,
- When the patient provides consent to the health-care provider to override their directive during that specific health-care interaction.

5.4.2. Once a user has overridden a patient's consent directive, the patient's personal health information in SHARE may be viewed by that user while the patient view remains active or is in context during the user's current login session. 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.

5.5. Printing information from SHARE

Authorized Printing

5.5.1. Authorized users are permitted to print information from within SHARE using the SHARE or DIS print functionality for purposes as described in directives 5.3.1 and 5.3.2.

5.5.2. No user shall print information for any other purpose.

Access to Printed Information

5.5.3. No user shall share or disseminate information printed from SHARE with any other person unless that person is authorized to have access to the information for the purposes described in directives 5.3.1 and 5.3.2.

Retention and Disposal of Printed Information

5.5.4. Any information printed from SHARE shall be appropriately retained or securely destroyed pursuant to the user's organizational records management policies and procedures.

Visibility of Printed Information

5.5.5. Users shall take reasonable precautions to ensure that information printed from SHARE is not visible to any person without authorization to view the information.

5.6. User Profiles

Responsibility for User Administration

- 5.6.1. DHW is responsible for the establishment, maintenance and updating of user profiles.

5.7. Password Protocol

User Responsibility

- 5.7.1. No user shall reveal his/her password to another person, or allow it to be accessible to another person.

Password Breaches

- 5.7.2. If a user suspects that his/her password has become available to another person s/he shall change his/her password immediately and notify his/her supervisor immediately.

Password Sharing

- 5.7.3. Users shall not access SHARE information under another person's password, and shall not allow another person to access SHARE information using their password.

User Authentication by Service Desk

- 5.7.4. The information services support provider's Service Desk shall not reset a user's password until s/he has provided the required information in his/her Challenge & Response form.

Password Changes

- 5.7.5. Users will be required to change their password in accordance with the SHARE Program password protocol.

5.8. Protection of SHARE Information on Computer Screens

Visibility of SHARE Information

- 5.8.1. Users shall take reasonable precautions to ensure that the information accessed from SHARE is not visible to any person not authorized to view the information.

Screen Locking

- 5.8.2. Computers shall not be left unattended when connected remotely. Users shall either logout of the application and terminate their secure connection, or lock the screen on their computer. The screen lock shall be configured to require a password to reactivate the screen.

5.9. Audit and Monitoring

Authority to Audit

5.9.1. DHW has the authority to audit and monitor all access to SHARE at any time without notice or warning.

5.10. Privacy Breach & Remediation

Appointment of a Privacy Officer

5.10.1. Each Organization shall appoint a Privacy Officer who will be responsible for privacy and security of SHARE personal health information within the User Organization.

Reporting Breaches - Users

5.10.2. All users shall immediately report any breach or suspected breach of privacy or security to the organization's Privacy Officer.

Reporting Breaches - Organization

5.10.3. An organization will report any breach or suspected breach of SHARE information privacy or system security that comes to their attention to the DHW Health Privacy Office (HPO).

Response to Breaches – HPO and Organization

5.10.4. In the event of a suspected breach of privacy or security, the Province will follow the DHW Privacy Breach Protocol which may require the HPO to contact and collaborate with the organization's Privacy Officer to conduct an investigation.

Response to Breaches – HPO Authority

5.10.5. Without notice, the HPO has the authority to review any instances where a privacy or security breach is suspected or has occurred and may determine mitigation strategies and follow up action, including but not limited to suspension or termination of user access.

5.11. Individual Access/ Amendments to their Personal Health Information

PHIA Requests

5.11.1. As per PHIA, all requests from individuals for:

- records of user access;
 - copies of personal health information;
 - corrections to personal health information; and,
 - complaints regarding personal health information, in SHARE;
- must be directed to the HPO.

5.12. Data Quality

Reporting Data Quality Issues

5.12.1. Users must notify the information services support provider of any potential data quality issues they identify in SHARE, such as data discrepancies or duplicate patient records.

5.13. Change in user employment status

Reporting Changes – Types of Changes

5.13.1. To ensure that user access is properly maintained, every organization shall provide the information services support provider with information related to the following changes in the user's employment status:

- termination of employment;
- change in job functions which changes the individual's need for access where the change is for longer than 30 days;
- suspension of employment;
- maternity or parental leave of over 30 days;
- leave of absence of over 30 days; and
- sick leave, short or long term disability of over 30 days

Reporting Changes – Timing

5.13.2. The organization shall provide the information to the information services support provider prior to or immediately upon the date that the organization confirms that there will be a change in status.

5.14. Business Continuity Plan

PHCO Responsibility

5.14.1. PHCOs are responsible for their own business continuity plans to support their business processes when SHARE is unavailable.

5.15. Privacy and Security Awareness and Communications

Awareness Training for all Users

5.15.1. Organizations must ensure that all users (permanent or temporary employees or third party contractors) who will have access to SHARE:

- 5.15.1.1. Are aware of the SHARE Privacy and Security Policy and existing organizational privacy policies and procedures; and
- 5.15.1.2. Receive communication of updates to the SHARE Privacy and Security Policy and organizational privacy policies and procedures.

Privacy Awareness

- 5.15.2. Organizations must ensure users are aware of the purposes for the collection, use, and disclosure of personal information.
- 5.15.3. Organizations must educate all users on the use of consent directives and the applicable policies and procedures associated with their use.

Data Accuracy Training

- 5.15.4. Organizations must educate all users on the procedures for correcting or amending personal health information.

Communication of Privacy Protection

- 5.15.5. Organizations must make their practices to protect personal health information available to individuals on request.

6. POLICY GUIDELINES

N/A

7. ACCOUNTABILITY

Accountability - Organization

- 7.1. Use of SHARE requires compliance with this policy and all relevant organizational privacy and confidentiality policies and agreements. Organizations will be held accountable for inappropriate access to or use of personal health information in SHARE.

Accountability - Users

- 7.2. Users will be held accountable for any misuse of SHARE access and/or privileges. Any user found to have violated provisions within this policy and/or any other relevant policies and agreements may be subject to suspension or termination of SHARE access privileges and disciplinary action will be managed pursuant to:
- Nova Scotia Health Authority/IWK Medical Staff Bylaws;
 - Other profession-governing and privacy oversight bodies;
 - An organization's disciplinary policy or measures; and,
 - PHIA.

Accountability - DHW

- 7.3. For the purpose of the administration of this policy, accountability is delegated to the Deputy Minister of Health and Wellness.
- 7.4. The Chief Health Information Officer has responsibility for on-going monitoring and enforcement of this policy.

8. MONITORING / OUTCOME MEASUREMENT

8.1. Organizational Privacy Officers /Privacy Leads, in conjunction with the information services support provider, are responsible for monitoring compliance with this policy.

9. REPORTS

N/A

10. REFERENCES

Health Authorities Act

Freedom of Information and Protection of Privacy Act (FOIPOP)

Personal Information Protection and Electronic Documents Act (PIPEDA)

Personal Information International Disclosure Protection Act (PIIDPA)

Personal Health Information Act (PHIA)

Nova Scotia Department of Health and Wellness Privacy Policy

Nova Scotia Health Authority /IWK Information Protection and Privacy Breach Policy and Procedures

11. APPENDICES

N/A

12. VERSION CONTROL

Version Control:

Version #2 replaces all previous versions.

13. INQUIRIES

Director of Privacy and Access

Health Information Office

Nova Scotia Department of Health & Wellness

Tel: (902) 424-3573