Privacy Policy and Guidelines

Effective July 4, 2005
Initial Version Approved by the Board of Directors on May 4, 2005
Revised Version Approved by the Board of Directors on November 1, 2014

TABLE OF CONTENTS

NOVA SCOTIA PRESCRIPTION MONITORING PROGRAM

SECTION I

PRIVACY POLICY

Policy statement

1. In managing information, the Nova Scotia Prescription Monitoring Program (the "Program") has a responsibility to:

   a) be accountable to the public for the information it collects and manages;

   b) protect the privacy of each individual whose information they hold and to afford the individual appropriate access to that information; and

   c) use and share information, including information regarding the prescribing and dispensing of monitored drugs, to effectively promote the appropriate use of monitored drugs and the reduction of the abuse and misuse of monitored drugs.

Policy objective

2. To ensure a consistent, fair and timely response to requests for information while:

   a) protecting the privacy of any individual to whom the information may relate; and

   b) releasing information as is reasonable to achieve the objects of the Program.

GENERAL

Legislative framework

3. a) The Nova Scotia Prescription Monitoring Program is bound by the *Prescription Monitoring Act* ("*PM Act*") and its regulations and the *Freedom of Information and Protection of Privacy Act* ("*FOIPOP Act*") and its regulations.

   b) This policy is intended to provide guidance on the application of the *PM Act* and the *FOIPOP Act*.

Principles

4. With respect to personal information, this policy shall be interpreted in conjunction with the Program Information Management Principles attached as Appendix A.

Definitions

5. In this policy:

   a) “Administrator” means the agency or person designated by the Minister to administer the Program.

b) “aggregate data” is group level data that does not contain information that can be used to:

   i. identify an individual; or

   ii. identify a group of individuals which numbers five or less.

c) “authorized representative” means:

   i. a person with written authorization from the resident to act on the resident’s behalf, where the written authorization has been provided;

   ii. a person exercising power of attorney for a resident, where a certified copy of the power of attorney document has been provided;

   iii. a personal guardian appointed for the resident, where a certified copy of the order appointing the guardian has been provided;

   iv. a resident’s personal representative where the resident is deceased, for the exercise of a right or power related to the administration of the resident’s estate, and where legal documentation appointing that person as legal representative of the estate has been provided;

   v. the resident's parent(s) or guardian, if the resident is under 16 years of age or if a resident aged 16 to 18 years does not have the capacity to provide consent.

d) “Board” means the Nova Scotia Prescription Monitoring Board established by this Act.

e) “de-identified person level data” means person level data that does not contain any personal identifiers.

f) “law enforcement” means

   i. policing, including criminal-intelligence operations,

   ii. investigations that lead or could lead to a penalty or sanction being imposed, and

   iii. proceedings that lead or could lead to a penalty or sanction being imposed.

g) “Licensing Authority” means the College of Physicians and Surgeons, the College of Pharmacists, the Provincial Dental Board or the College of Registered Nurses of Nova Scotia.

h) “non-nominal data” includes aggregate data and de-identified person level data.

i) “personal information” means recorded information about an identifiable individual including:

   i. the individual's name, address or telephone number,

   ii. the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,

   iii. the individual's age, sex, sexual orientation, marital status or family status,

iv. an identifying number, symbol or other particular assigned to the individual,

v. information about the individual's health-care history, including physical or mental disability,

vi. information about the individual's educational, financial, criminal or employment history,

vii. anyone else's opinions about the individual, and

viii. the individual's personal views or opinions, except if they are about someone else.

j) “record” includes books, documents, letters, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

k) "resident" is defined as:

i. a person who is legally entitled to remain in Canada and who makes their home and is ordinarily present in Nova Scotia and has lived in Nova Scotia for a period of not less than 3 months, and for greater certainty, does not include a tourist, a transient, or a visitor who ordinarily resides outside Nova Scotia,

ii. not including a person who is prescribed monitored drugs while they are an in-patient as defined in the *Hospital Insurance Regulations* under the *Health Services and Insurance Act,* and

iii. including a person who is a visitor to Nova Scotia and has a prescription, which may be written by a physician, dentist or nurse practitioner from outside the province, for a monitored drug that is filled at a community pharmacy.

Scope

6. This policy applies to all information collected, used, or managed by:

a) the Program;

b) consultants contracted by the Program;

c) students completing internships or co-operative education work terms at the Program.

7. Any data sharing agreement signed on or after the effective date of this policy must be consistent with this policy and with the legislative framework.

8. All contractors and consultants contracted by the Program and all students completing internships or co-operative education work terms at the Program must adhere to confidentiality guidelines set by the Program.

9. All contractual obligations must be consistent with the *PM Act*, the *FOIPOP Act* and this policy.

Accountability

10. The Program Manager ("Manager") or designate is accountable:

    a) to make every reasonable effort to assist with an applicant's request for access; and

    b) to protect the privacy of personal information that is in the custody or under the control of the Program.

11. The Manager has responsibility for the ongoing monitoring and enforcement of this policy.

REQUESTS FOR INFORMATION

Access to information

12. Any member of the public is entitled to seek access to any record as prescribed by the *FOIPOP Act.*

Disclosure of personal information

12. Personal information of an individual shall only be disclosed to a third party with the individual's or their authorized representative's written consent or as authorized under the *PM Act* or *FOIPOP Act.*

Requests from individuals for personal information about themselves

13. An individual or their authorized representative shall be permitted to view or receive a copy of any personal information about the individual collected and managed by the Program unless the disclosure is exempted by the *PM Act* or the *FOIPOP Act.*

14. Prior to release of personal information to an individual, their authorized representative or a third party, the Program requires that the request for release of information be submitted by completing the form attached as Appendix B or by providing, in writing, all of the information requested in the form attached as Appendix B.

15. A request for information shall provide sufficient particulars to enable identification of the record requested.

Requests from individuals for personal information about a deceased person

16. In order to obtain the Program's history of a deceased person, the requestor must provide proof that they are the Executor of the individual's Last Will and Testament. A copy of the death certificate and a copy of the first page of the Last Will and Testament must be submitted with the request for information. Should no Last Will and Testament exist, the requestor would be required to apply to the Nova Scotia Supreme Court to obtain a Letter of Administration. This document can then be provided with the request for data.

Requests from prescribers or pharmacists for personal information

17. A prescriber or pharmacist shall be permitted to view or receive a copy of a resident's drug profile if it is reasonable to achieve the objects of the Program. The drug profile identifies the resident's prescriptions for drugs monitored by the Program. It includes, but is not limited to, the identification of the prescribers prescribing the drugs and the pharmacies dispensing the drugs to the resident.

18. Prior to releasing information to a prescriber or pharmacist, the Program shall verify the identity of the prescriber or pharmacist.

19. A request for information shall provide sufficient particulars to enable identification of the record requested.

Requests from a licensing body for personal information

20. A representative of a licensing authority shall be permitted to view or receive information collected and managed by the Program about a resident who has a prescription for a monitored drug or a member of that licensing authority if it is reasonable to achieve the objects of the Program.

21. Prior to the release of information to a licensing authority the Program shall require that the request be submitted in writing, by fax or e-mail and signed by the individual making the request, and that the request provides sufficient particulars to enable identification of the record requested.

Requests from law enforcement for personal information

22. Law enforcement shall be permitted to view or receive information collected and managed by the Program as is reasonable to achieve the objects of the Program.

23. Prior to the release of information to law enforcement, the Program shall require that the request be submitted in writing, by fax or e-mail, signed by the individual making the request, and that the request provide sufficient particulars to enable identification of the record requested.

Processing of subpoenas, court orders, and warrants

24. A valid subpoena, court order or warrant must be referred to the Manager or designate.

25. The required information detailed in the subpoena, court order or warrant will be released within the specified timeframe.

Requests from the Department of Health and Wellness

26. Any information provided to the Department of Health and Wellness shall be in the form of non-nominal data.

Requests for set(s) of de-identified person level information

27. The Program may release set(s) of de-identified person level data to an applicant if the Manager, in consultation with the Board, deems the request reasonable to further the objects of the Program.

28. All requests must be referred to the Manager.

29. Applications for information must be in the form attached as Appendix C.

30. The applicant must sign a confidentiality agreement.

31. Only the minimum information required to fulfill the purpose outlined by the applicant in the Request for Access form shall be considered for release.

Requests for aggregate data

32. Requests for aggregate data may be granted at the discretion of the Manager.

RELEASE OF INFORMATION

Release of non-nominal data by the Program

33. The Program may release aggregate or de-identified person level data.

Release of personal information by the Program

34. The Program may release information with respect to monitored drugs including the identification of prescribers, pharmacists and pharmacies if releasing the information is reasonable to achieve the objects of the Program.

35. The Program or its designate may release personal information with respect to a resident who has a prescription for monitored drugs, including the identification of prescribers, pharmacists and pharmacies, if releasing the information is reasonable to achieve the objects of the Program.

36. Pursuant to subsection 23(1) of the *PM Act*, if the Program has reasonable grounds to believe an offence has been committed, they must provide to the appropriate law enforcement authority all necessary information including, but not limited to,

    a) the resident's name;

    b) the resident's address;

    c) an identification of the drug or drugs in use;

    d) the number of prescriptions dispensed and the date of the dispensing; and

    e) the number of prescribers.

37. The Program may:

    a) file a complaint with a licensing authority regarding the activities of a member of that licensing authority, and

    b) shall provide the licensing authority with all relevant information,

    if the Program has reason to believe that the member may be practicing in a manner that is inconsistent with the objects of the Program.

Challenging Compliance

38. Any challenge to the Program's compliance with this policy shall be provided in writing to the Manager.

NOVA SCOTIA PRESCRIPTION MONITORING PROGRAM

SECTION II

GUIDELINES

Privacy Breach Guideline

1. This guideline provides a process for Program staff to follow when there may have been a privacy breach. The guideline will assist staff to contain the privacy breach, notify appropriate persons, document the breach and reduce the likelihood of future breaches.

Accountability

2. All Program staff are responsible for maintaining the confidentiality of any personal or sensitive information and for reporting any privacy breaches to the Manager. The Manager is responsible for monitoring compliance with these guidelines.

Definitions

3. In this guideline,

   a) "*Personal information*" is as defined in the Program's Privacy Policy;

   b) "*Sensitive information*" includes confidential financial information, confidential strategic advice, information subject to solicitor-client privilege, draft documents, or other information not generally available to the public.

   c) *Personal or sensitive information* may be found in:

      - electronic files on desktop or laptop computers,
      - computer discs, CDs and DVDs,
      - memory sticks and memory cards
      - paper records or files,
      - palm pilots or PDAs,
      - calendars and diaries, and
      - email and voicemail.

   d) "*Privacy breach*" means that information collected and retained by the Program is retained or disclosed in a manner that does not follow the Program's Privacy Policy. Some examples of privacy breaches may include:

      - transmission of a letter, email or fax containing personal or sensitive information to the wrong person or place;

- verbal disclosure of an individual's personal information to someone who is not authorized to know it;

- unauthorized access to a database containing personal or sensitive information;

How to deal with a privacy breach

Step 1 - Contain the privacy breach

4. Immediately identify the scope of the breach and take steps to prevent further loss or unauthorized disclosure of information, if possible. For example:

   a) If a fax was sent to the wrong number, call the recipient and ask them to destroy the document and any copies that were made.

   b) If an email was sent to the wrong person, call the recipient and ask them to destroy any email printouts that were made and delete the email.

   c) If an unauthorized person has access to a database or computer system, prevent further unauthorized access to or destruction of personal information by notifying the Technology Support Desk, who can disable accounts or change passwords and identification numbers.

   d) If a computer screen can be seen to display personal information in a public place, relocate or re-orient the computer to prevent public viewing.

   e) Where unauthorized verbal disclosure has occurred, request that the recipient of the personal or sensitive information treat it confidentially.

Step 2 - Notify appropriate persons about the privacy breach

5. All privacy breaches, including misdirected fax and email, relating to personal or sensitive information must be reported to the Manager.

6. When the privacy breach involves a crime or the loss of records or information, immediately notify the Manager who will notify all appropriate persons. The Manager is responsible for coordinating the Program's response to the breach.

Notification

7. In some cases, it may be appropriate to inform the individual whose personal information was the subject of the privacy breach. The decision to inform will be made by the Manager in consultation with appropriate individuals. Generally, notification should occur if there is risk of:

   a) harm to the individual,

   b) public disclosure of the personal information; or

   c) malicious use of the personal information.

Step 3 - Document the breach

8. When a privacy breach has or may have occurred, the Manager will document the breach in the form attached as Appendix D. Information breaches will be reported to the Board immediately.

Transmission of Confidential Information by Email and Facsimile Guideline

Purpose

9. The purpose of this guideline is to provide a framework that ensures all reasonable efforts are taken to protect the confidentiality of personal information that must be transmitted by email or fax.

Accountability

10. Individuals are responsible for maintaining the confidentiality of the information that they are transmitting. The Manager is responsible for monitoring compliance with this guideline.

Email

11. Internal email is defined as email where the sender and the recipient are both on the Administrator's email system. External email is defined as email where:

    a) the sender is on the Administrator's email system and the recipient is not, or

    b) the recipient is on the Administrator's email system and the sender is not.

12. Program staff shall not include identifiable personal information about an individual in an email sent outside the Administrator's email system.

13. If identifiable personal information about an individual must be transmitted to an external recipient, the personal information must be placed in a password protected encrypted format. If an external sender emails personal information to an internal recipient, the internal recipient shall not return or respond to the email without first password protecting and encrypting the file containing personal information.

Facsimile

14. Before sending a facsimile with personal information in it, ask the recipient to stand by the fax machine to receive the transmission if the machine is accessible by someone other than the recipient and to acknowledge receipt of the facsimile as soon as possible.

Information System Privacy and Security Guideline

Statement

15. The Prescription Monitoring Program Information System (PMPIS) recognizes the right to have personal information protected against unauthorized access or misuse. Protection of personal information is the responsibility of every user of the PMPIS.

Access to information on the PMPIS

16. No user shall be authorized to have access to the PMPIS until:

    a) a user profile is defined and set by the Manager or designate. This user profile may not be amended by any user;

    b) the user has signed an employee confidentiality agreement; and

    c) the user has been advised of their responsibility by the Manager or designate regarding the safeguarding of personal information.

Authorized versus unauthorized access

17. A user is only authorized to access information on the PMPIS in the performance of their duties related to the day-to-day operations of the Program.

18. Unauthorized access to information on the PMPIS is prohibited. Unauthorized access is defined as access to information that is not required to perform the duties of a user's job.

Audit and Monitoring

19. An "access log" is a report that details information related to a selected user's access to Program information.

20. The Manager or designate may audit any user's access to the system at any time without notice or warning.

21. The Manager or designate will be accountable for the review of access logs and other PMPIS privacy issues.

Confidentiality

22. Confidentiality is defined as the obligation of one person to preserve the privacy of another's personal information.

23. Nothing in this policy diminishes the existing confidentiality obligations on users of the PMPIS as defined in legislation, their employee contracts, confidentiality agreements with their employer and the code of conduct or regulating legislation of their profession.

Change in user employment status

24. When appropriate, the Manager shall modify a user's access when a user's employment status changes.

NOVA SCOTIA PRESCRIPTION MONITORING PROGRAM

SECTION III

APPENDICES

APPENDIX A

Information Management Principles

Balance

1. In the management of personal information the Program shall balance the:

   a) individual's right to keep his/her personal information private; and

   b) benefits to Nova Scotians derived from the promotion of appropriate use of monitored drugs and the reduction of the abuse or misuse of monitored drugs.

Accountability

2. The Program is accountable for the management of all information under its control, including the responsibility to have policies for the management of the information.

Identifying Purposes

3. The Program shall identify the purposes for which it collects personal information at or before the time that the information is collected.

Consent

4. The Program shall collect, use, and disclose personal information based on the principle of informed consent, unless otherwise permitted or required by law.

Limiting Collection, Use, Disclosure and Retention

5. The Program shall collect, use, disclose and retain personal information in the most limited manner and with the highest degree of anonymity that is reasonable in the circumstances.

Accuracy

6. The Program shall ensure that personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards

7. The Program shall protect personal information with security safeguards appropriate to the sensitivity of the information.

Openness

8. The Program shall make available to individuals specific information about its policies and practices relating to the management of information.

Individual Access

9. The Program shall support the individual's right to access their personal health information and the right to challenge the accuracy of that information.

Challenging Compliance

10. The Program shall provide a process for an individual to challenge the Program's compliance with this policy.

APPENDIX B

NOVA SCOTIA
PRESCRIPTION MONITORING PROGRAM

P.O. Box 2200, Halifax, Nova Scotia, B3J 3C6
Phone: (902) 496-7123 Fax: (902) 481-3157

To: Nova Scotia Prescription Monitoring Program
P.O. Box 2200
Halifax, NS
B3J 3C6

I, _____, authorize the Nova Scotia Prescription Monitoring Program to release to _____ (*insert either name of individual or designated recipient)* any and all information from my prescription records at the Nova Scotia Prescription Monitoring Program which relate to any professional services I am receiving or have received between the period of _____ to _____.

_____
Individual's Name (Print)

_____
Street

_____
City Postal Code

_____
Individual's Health Card Number

_____
Date of Birth

_____
Individual's Signature

_____
Date

APPENDIX C

Requests for Access to Set(s) of NS PMP De-identified Person Level Information

Please complete the following questions:

1. **Organization:**

2. **Request/Project:**

3. **Legislative Authority:**

4. **Date:**

5. **Contact Person (s)**

   Position:

   Address (if different from Organization):

   Phone #: **Fax #:**

   Email address

6. **Information Requested** (list in detail the specific information requested)

7. **Purpose for Requesting the Information** (provide the purpose for requesting the specific information and attach supporting material, if available, referent to your mandate)

8. **Method of data access** (e.g. paper report provided by Nova Scotia Prescription Monitoring Program, data file)

9. Data Linkages (if applicable, please explain rationale for linkages)

10. Estimated Time Period for Need of Data (specify the time: one year, five years, etc. that this data will be used for, or how often this data has to be forwarded to your organization)

11. List of all persons who will have access to the data (include names and positions within the organization).

12. Security Arrangements (e.g. where the data will be stored, security of premises, personnel access to area).

13. Retention and Disposal of Data (e.g. your retention schedule and way of disposing of the data)

For Nova Scotia Prescription Monitoring Program Use Only

Comments:

Recommendation:

Consulted with:

Reviewed by: _____
Manager, Nova Scotia Prescription Monitoring Program

Approved by: _____ Date: _____
Prescription Monitoring Program Board

APPENDIX D

Information Breach Reporting Form

---

1. Breach of (check one):

❍ Personal Information
❍ Sensitive Information
❍ Both

2. Documented by:

3. Date and time of breach:

4. Breach reported by:

5. Person responsible for breach:

6. Details of breach:

7. If personal information was involved in breach, please provide details:

9. Location of breach:

10. Notifications to individuals: (include name and date):

11. Notes of discussions:

12. Contact with Client:

13. Follow-up:

14. Signatures

Completed by	**Date**
Employee responsible for breach	**Date**
Manager	**Date**

TO BE COMPLETED BY ADMINISTRATOR, INFORMATION ACCESS AND PRIVACY

Outcome:

Date Closed:

Signature Date