ADMINISTRATIVE
Policy and Procedure

Title:	Privacy and Confidentiality of Personal Health Information	Number:	AD-AO-030
Sponsor:	General Counsel, Legal Services	Page:	1 of 37
Approved by:	Executive Leadership Team, NSHA	Approval Date: Effective Date:	July 10, 2017 February 13, 2020
Applies To:	All Employees and Staff		

TABLE OF CONTENTS

POLICY STATEMENTS

1. In managing Personal Health Information (PHI), Nova Scotia Health Authority (NSHA) recognizes the importance of Privacy, the sensitivity of PHI in its custody and/or control, and the responsibility of all NSHA Employees and Staff (see Appendix A – Definitions) to:
   - 1.1. Balance the need to protect the Privacy and Confidentiality of all NSHA Patients, with the need to provide efficient and effective Patient care;
   - 1.2. Give the Patient an opportunity to request access to their own PHI;
   - 1.3. Collect, use, and disclose PHI effectively to support the provision of health care, research, and planning, as well as other legally authorized purposes;
   - 1.4. Use and disclose PHI only for authorized purposes, such as:
     - 1.4.1. Providing care
     - 1.4.2. Conducting Research Ethics Board (REB) approved research
     - 1.4.3. Ensuring and improving quality and standards of care
     - 1.4.4. Risk management and Patient safety purposes
     - 1.4.5. Planning and delivering programs and services.
2. The right of Patients to Privacy, and to control the collection, use, and disclosure of their PHI, within the limits of the law, is essential to care provision and the Patient-service provider relationship.
3. NSHA manages the collection, use, and disclosure of PHI as described in NSHA Privacy Statement
4. NSHA is responsible to comply with the following laws, as well as any other relevant legislation:
   - 4.1 The *Personal Health Information Act* (PHIA) which governs the management and protection of PHI within NSHA
   - 4.2 The *Personal Information and International Disclosure Protection Act* (PIIDPA) which governs the access, storage, disclosure, and transportation of PHI outside of Canada.
5. All NSHA Staff collect, use, disclose, retain, dispose, and destruct PHI only as permitted by NSHA policies and procedures, applicable legislation, and professional standards of practice.
6. The NSHA Privacy Office, which includes Zone Privacy Officers and the Provincial Privacy Manager, is the primary contact for compliance with privacy requirements, information

practices, complaints and concerns, and organizational practices and procedures in relation to PHI.

7. The NSHA Privacy Office is responsible for:
   - 7.1. Monitoring compliance with this Policy and making recommendations related to the protection of PHI
   - 7.2. Facilitating Privacy education and promoting Privacy awareness
   - 7.3. Receiving and processing Privacy related complaints in accordance with this Policy and applicable legislation
   - 7.4. Investigating breaches of Privacy and/or Confidentiality
   - 7.5. Conducting audits of electronic health systems to detect unauthorized access
   - 7.6. Assessing Privacy risks
   - 7.7. Assisting in completing and approving PIA (Privacy Impact Assessments)
   - 7.8. Processing requests for Records of User Activity.
   - 7.9. Guidance related to Release of Information
   - 7.10. Respond to inquiries about NSHA's information practices
   - 7.11. Providing consultation services to NSHA Staff regarding Privacy and Confidentiality.
8. NSHA is the legal Custodian (see Appendix A – Definitions) of all NSHA Patient PHI, including any PHI collected for the purposes of REB-approved research. Individual health care providers are **not** the Custodians of the PHI of their Patients.
9. Compliance: Any breach of this policy may result in termination of access to Patient information and/or Discipline up to and including termination of employment/placement or revocation of privileges.

PROCEDURE

1. Accountability for Personal Health Information

1.1. Employees and Staff:

1.1.1. Take all reasonable steps to protect Patient Privacy and maintain Confidentiality, including, but not limited to:

1.1.1.1. Complying with the terms of their Confidentiality Pledge and NSHA policies related to the Privacy, security, and Confidentiality of PHI

1.1.1.2. Completing annual, mandatory Privacy and Confidentiality training

1.1.1.3. Reporting Privacy breaches to their Manager/Supervisor and the Zone Privacy Officer as per NSHA's Privacy Breach Protocol Guidelines.

1.2. The Manager of Health Information Services:

1.2.1. Responds to requests made by individuals for the correction of their health records.

1.3. Access to Personal Health Information/Release of Information Staff:

1.3.1. The Access to Personal Health Information and Release of Information staff Team respond to requests to access/copy Patient's PHI.

2. Collection of Personal Health Information

2.1. NSHA only collects PHI for the purpose of:

2.1.1. Providing health care and medical treatment to Patients

2.1.2. Planning, administering, and managing internal operations (e.g. bed management)

2.1.3. Conducting quality improvement and risk management activities at NSHA

2.1.4. Meeting any legislative and regulatory requirements (e.g. *Vital Statistics Act* requirements)

2.1.5. Supporting and promoting approved research and education at NSHA

2.1.6. Receiving payment for health care provided to Patients.

2.2. NSHA must take reasonable steps to ensure that information related to NSHA's collection of PHI (i.e.: NSHA's Notice of Purpose) is readily available and likely to be seen by Patients or Substitute Decision Makers (SDM) (See Appendix A – Definitions) coming to NSHA to receive a service. Such steps may include:

2.2.1. Ensuring appropriate display of Privacy Posters in entryways, registration, and admitting areas

2.2.2. Providing information through mail-outs and Patient pamphlets

2.2.3. Posting information on NSHA's internet site.

2.3. If collecting PHI from a Patient on behalf of NSHA, Staff must explain the reasons why the information is being collected, or direct the Patient or SDM to a person who can provide this information if requested, and provide them with information on the specific uses and disclosure of the information.

2.4. Patients have the right to refuse having their PHI collected by NSHA. If this occurs, NSHA Staff involved with the individual, with support from the Privacy Office, will inform the individual of the consequences of limiting or revoking consent in the specific circumstances.

2.5. Employees and Staff must collect information directly from the Patient, or their SDM, except in the following circumstances:

2.5.1. If the individual authorizes collection of their PHI from another source

2.5.2. When it is not reasonably possible to get information from the Patient directly

2.5.3. If there is a safety concern (e.g. aggressive Patient).

3. Limiting the Collection, Use, Disclosure, and Retention of Personal Health Information

3.1. Employees and Staff should only collect, use, and/or disclose the minimum amount of PHI necessary to meet the intended purpose.

3.2. When they have approval to do so, Employees and Staff should collect, use, or disclose *non-identifiable* information (e.g. aggregate statistical information, hypothetical case examples, etc.) if the intended purpose can be achieved without collecting, using, or disclosing PHI.

3.3. For the collection, use, disclosure, and retention of PHI for research purposes, Staff must adhere to PHIA, NSHA's Research Ethics Board process, NSHA's Research Services policies, and this policy.

3.3.1. Prior to any collection, use, disclosure, and retention of PHI for research purposes, ensure Research Ethics Board approval is in place, verify the Patient's consent or obtain a waiver of the consent requirement from the Research Ethics Board and where required complete NSHA's data access process.

3.4. Refer to NSHA's Use and Disclosure of Personal Health Information Policy for guidance in using and disclosing of PHI, including how Patients may limit or restrict access to their PHI.

3.4.1. Direct questions about disclosure of PHI not addressed by the Policy to the relevant manager and/or the applicable Zone Privacy Officer.

3.5. Refer to currently approved and published policy for more information on retention of PHI.

4. Accuracy of Personal Health Information

4.1. NSHA ensures that the PHI of Patients is as accurate, complete, and as current as is necessary for the purposes for which it is to be used.

4.2. A Patient, (or their SDM), who believes there is an error or omission in their PHI may make a request to the Zone Privacy Officer to have the information corrected;

4.2.1. The Zone Privacy Officer will then review the request, consult with the applicable Health Information Manager, as appropriate, and respond to the request in writing within 30 days.

4.2.2. The Health Information Manager will contact the appropriate NSHA clinical Staff to determine if the correction can be made.

4.3. The requested correction will <u>not</u> be made if:

4.3.1. The Patient has not demonstrated that there is an error (i.e. that the record is incomplete, inaccurate, or out of date)

4.3.2. The Patient has not provided the information necessary to correct the record

4.3.3. The record was not originally created by NSHA and NSHA does not have sufficient knowledge, expertise, and authority to correct the record

4.3.4. The record consists of a professional opinion or observation made in good faith about the Patient

4.3.5. There are reasonable grounds to believe the request for a correction is frivolous, vexatious, or part of a pattern of conduct that amounts to an abuse of the Patient's right to have a correction made.

4.4. If determined it is appropriate to make the requested correction, the Health Information Manager:

4.4.1. Makes the correction and strikes out any incorrect information (without obliterating it)

4.4.2. Makes a notation on the record that the information is incorrect and ensures a system is in place to inform a person who accesses the record that the information in the record is incorrect, and directs the person to the correct information where it is not possible to physically correct the information in the record.

4.5. The Zone Privacy Officer will give written notice to the Patient of what has been done.

4.6. If requested by the Patient, the Zone Privacy Officer will give written notice of the requested correction, to the extent reasonably possible, to those persons to whom the custodian has disclosed the information (unless the correction has no impact on the ongoing provision of health care or other benefits to the individual).

4.7. If deemed inappropriate to make a requested correction to PHI, the health Information Manager will inform the Zone Privacy Officer.

4.8. The Zone Privacy Officer will provide the Patient with a letter outlining the reasons for the refusal, and stating that the Patient is entitled to:

4.8.1. Prepare a brief statement of disagreement, setting out the correction NSHA refused to make

4.8.2. Require NSHA attach the statement of disagreement to the records in question

4.8.3. Disclose the statement of disagreement whenever NSHA discloses information to which the statement relates

4.8.4. Require NSHA to make all reasonable efforts to disclose the statement of disagreement to any person who would have been notified, if NSHA had granted the requested correction

4.8.5. Make a complaint about the refusal to the Office of the Information and Privacy Commissioner.

4.9. If requested by the Patient, the Health Information Manager will attach the statement of disagreement to the Patient's health record.

5. Safeguards for Personal Health Information

5.1. NSHA protects PHI in all formats (paper, digital, electronic, and verbal). The safeguards vary depending on the sensitivity of the information and include physical, administrative, individual, and technological measures.
Note: measures listed below are examples, and are not an exhaustive list.

5.2. Physical Measures:

5.2.1. Store PHI in secured areas and do not leave unattended until properly secured (e.g. locked in filing cabinets/offices), ensuring PHI is accessible if required to address a health emergency

5.2.2. Place computer monitors, printers, and fax machines so as to minimize inappropriate information viewing/access

5.2.3. Do not allow PHI (originals or copies) to be removed from NSHA, except in limited authorized circumstances or as required by law

5.2.4. Do not use personal electronic devices (e.g. cell phones, tablets, etc.) to collect, disclose, or store PHI, including images/videos, photographs

5.2.5. Use only encrypted USB memory sticks to store data containing PHI for transport

5.2.6. Ensure proper storage and safekeeping of Subscriber Identity Modules (SIM) cards and other memory cards (e.g. always store memory cards used in NSHA cameras and other electronic devices in a locked cabinet when not in use)

5.2.7. Store PHI only on NSHA network drives or in the electronic medical record (EMR); PHI is not to be stored or retained on individual computer hard-drives or in email folders (Outlook or other email system)

5.2.8. Securely destroy records of PHI in consultation with Health Information Services as per Confidential Waste Management Policy

5.2.9. Consult with the Privacy Manager and/or Zone Privacy Officers regarding best practices when travelling with Patient information.

5.3. Administrative Measures:

5.3.1. Ensure PHI access is given only to those Staff (as much as possible) who need to know the information to do their job

5.3.2. Require completion of online Privacy training and signing of Confidentiality Pledge by all Staff upon hire when access to PHI is anticipated, and renew the training and Pledges on a yearly basis

5.3.3. Ensure data sharing agreements are used, where applicable

5.3.4. Complete a PIA (Privacy Impact Assessment) regarding the collection, use, or disclosure of PHI for any new – or significantly changed – program or service, which impacts the accessibility, security, or consent for the use of PHI

5.3.5. Ensure all access, disclosure, storage, or transportation of PHI outside of Canada (whether as a result of international vendor access or NSHA Staff access/storage outside of Canada) complies with the NS Personal Information International Disclosure Protection Act (PIIDPA)

5.3.5.1. Include PIIDPA compliance in vendor agreements and consult Legal Services for guidance where appropriate

5.3.5.2. Request and receive Vice-President approval for taking electronic devices (e.g. laptops; cellular phones) outside of Canada.

5.3.6. Obtain Patient consent prior to taking photographs or videos of Patients for any purpose. Use only NSHA-approved devices for any such photographs/videos

5.3.7. Ensure that Electronic Information Systems ("EIS") that house Patient information are accessible by individual passwords only (e.g. Active Directory).

5.4. Measures for Staff:

5.4.1. Do not share passwords

5.4.2. Do not look up information on yourself or family, friends, co-workers if not required for your job. The *ability* to access information does not mean one has the *authority* to access that information

5.4.3. Do not discuss PHI in public areas (elevators, lobbies, cafeterias, hallways, off-site, etc.). Do not discuss PHI in the presence of persons not entitled to such information

5.4.3.1. It is not acceptable to discuss PHI with a Patient when others may overhear unless absolutely necessary to facilitate Patient care. Where possible, verify PHI with a Patient in a manner such that others present will not see or overhear details of the PHI. **Example:** Through generic "yes" or "no" questions ("Do you still live at the same address?" "Have your prescriptions changed?")

5.4.3.2. In rare circumstances, it may be necessary to discuss PHI with a Patient in public areas in order to provide efficient and effective health care. In these circumstances, all reasonable efforts should be made to maintain Patient Privacy and Confidentiality.

5.4.4. A Patient's presence in a clinical setting often discloses information respecting the provision of specific care or treatment to that individual. To prevent the disclosure of identifiable information in such

circumstances, address Patients by first name or assigned waiting number only

5.4.5. Do not leave Patient records or other confidential information open, visible, or unattended in public places

5.4.6. Do not access, transfer, or store PHI outside of Canada unless in accordance with PIIDPA (see Procedure 5.3.5)

5.4.7. Ensure PHI is **not** used in public presentations. De-Identified Information (See Appendix A – Definitions) may be used

5.4.7.1. Removing obvious identifiers (i.e.: name, DOB, health card number, address, etc.) is not sufficient if the circumstances are such that the Patient could still be identified

5.4.7.2. **Exception**: A minimal amount of PHI may be used in presentations for NSHA internal medical/surgical rounds (educational purposes) when it is not possible to achieve the quality or educational purposes without the use of PHI, or when express consent has been obtained from the Patient or SDM.

5.5. Technological Measures:

5.5.1. Conduct routine PHI access audits by the NSHA Privacy Office as per NSHA's Auditing of PHI in Electronic Information Systems and Record of User Activity Requests Policy

5.5.2. Ensure a secure computer network/firewall to facilitate secure communication and electronic records storage

5.5.3. Ensure that mobile devices, laptops, BlackBerrys, and cellular phones are on the NSHA network and password protected

5.5.4. Use SEND for emails with PHI, or internal email addresses with nshealth.ca to email someone who has an nshealth.ca email address — see NSHA AD-AO-045 Electronic Messaging of Personal Health Information.

6. Openness about Personal Health Information Policies and Practices

6.1. The Privacy Office and the Policy Office together ensure that the NSHA Privacy and Confidentiality Policy and any associated policies or guidelines are available on the OP3 website and in hardcopy upon request.
Note: Only the digital copy of any policy is considered the original; paper copies must be discarded immediately after use.

6.2. The Privacy Office develops and maintains a Patient education pamphlet - *Your Personal Health Information and its Protection: NSHA's Privacy Statement*.
Note: The Privacy Statement is available on the NSHA public website in addition to being available for order as a Patient pamphlet.

6.3. Patients may request a copy of, or to view, their own PHI. Refer to the Use and Disclosure of Personal Health Information Policy for procedures.

7. Privacy Concerns and Complaints

7.1. Review by NSHA's Privacy Office:

7.1.1. To challenge NSHA's compliance with this Policy and/or PHIA, or to report a concern with Privacy and Confidentiality practices, any individual may submit their concern in writing to NSHA's Privacy Office, or by completing the NSHA Privacy Complaint Form.

7.1.2. The Privacy Office oversees the procedure to receive and respond to complaints or inquiries about NSHA handling of PHI.

7.1.3. The Zone Privacy Officer ensures all complaints are reviewed and investigated, as appropriate. The Zone Privacy Officer will respond in writing to complaints within 60 days, and may advise that a further extension of up to 30 days for review is required.

7.1.4. Any Staff having knowledge of a complaint, breach of this Policy, breach of Confidentiality, or potential Privacy concern should report the issue to their Manager/Supervisor and the Zone Privacy Officer as soon as possible.

7.2. Complaint to Office of the Information and Privacy Commissioner

7.2.1. An individual may submit a complaint to the Provincial Review Officer, or request that the Provincial Review Officer conduct a review of NSHA's Privacy activities. NSHA's Zone Privacy Officer acts as the liaison for all complaints and inquiries by the Provincial Review Officer. Any inquiries received by NSHA Staff from the Provincial Review Officer should be directed to the NSHA Zone Privacy Officer.

7.3. Privacy Breaches (see Privacy Breach Protocol)

7.3.1. Privacy breaches are managed and investigated as outlined in NSHA's Privacy Breach Protocol and NSHA-AD-AO-040 Internal Auditing of Access to Personal Health Information (Pending).

7.4. Notification of Privacy Breaches

7.4.1. In the event of a suspected Privacy breach, report as soon as possible to Manager/Supervisor and Zone Privacy Officer, and file a Patient Safety Report via Safety Incident Management System (SIMS).

7.4.2. In the event of an actual Privacy breach, as determined by the Privacy Office, the Manager/Supervisor or Zone Privacy Officer notifies the affected Patient at the first reasonable opportunity, if there is a reasonable basis to believe that:

7.4.2.1. The information is stolen, lost or subject to unauthorized access, use, disclosure, copying, or modification ***and***

7.4.2.2. As a result, there is potential for harm or embarrassment to the Patient.

7.4.3. Notifying the affected Patient is not necessary if the NSHA Privacy Office determines that PHI has been stolen, lost, or subject to unauthorized access, use, disclosure, copying, or modification, ***but***

7.4.3.1. It is unlikely that a breach of the PHI has occurred (i.e. could not be accessed) ***or***

7.4.3.2. There is no potential for harm or embarrassment to the individual as a result.

7.4.4. Where it is found to be not necessary to notify a Patient, then, the Zone Privacy Officer will notify the Provincial Review Officer as soon as possible.

7.5. Compliance with this Policy

7.5.1. Any breach of this Policy may result in termination of access to Patient information and/or Discipline up to and including termination of employment/placement and/or revocation of privileges.

7.5.2. Failure to report a Privacy breach, if aware, may also result in Discipline.

7.5.3. The Zone Privacy Officer is to be notified at the earliest opportunity if PHI is lost, stolen, accessed, used, or disclosed without proper authorization.

8. Retention, Destruction, Disposal, and De-identification of Personal Health Information

8.1. Refer to currently approved and published policy for more information on retention of PHI.

8.2. Properly destroy confidential information, such as PHI, as per currently approved and published policy.

8.3. Do not place confidential information in a regular garbage bin or recycling bin.

8.4. Completely erase electronic information (e.g. deleting file and then emptying 'Recycle Bin"), as appropriate.

8.5. Consult Health Information Services, IT Security or the Zone Privacy Officer for further assistance in this area.

REFERENCES

Legislative Acts

Crown in right of Nova Scotia. (2006). *Personal Information International Disclosure Protection Act* (PIIDPA). Retrieved from http://nslegislature.ca/legc/statutes/persinfo.htm

Nova Scotia Department of Health and Wellness. (2013). *Personal Health Information Act* (PHIA). Retrieved from http://novascotia.ca/dhw/phia/

RELATED DOCUMENTS

NSHA RS-RE-001 Research Ethics Board process

NSHA Research Services

Policies

N/A

Forms

Privacy Impact Assessment

Records of User Activity

Confidentiality Pledge

Privacy Complaint Form

Privacy Breach Protocol

Brochures

Your Personal Health Information and its Protection: NSHA's Privacy Statement

Other

NSHA Privacy Statement

Appendices

Appendix A – Definitions

* * *

Appendix A - Definitions

Agent: Individuals authorized by NSHA to act for or on behalf of NSHA with respect to PHI.

Capacity: The ability to understand information that is relevant to the making of a decision related to the collection, use, or disclosure of PHI, and the ability to appreciate the reasonably foreseeable consequences of a decision or lack of a decision.

Circle of Care: Commonly used to describe information sharing practices among the members of a Patient's healthcare team for the purpose of providing ongoing care. The term "Circle of Care" does not appear in PHIA, but is used to refer to all regulated health professionals and other "Custodians" defined under PHIA. Information can be shared within the "Circle of Care" on the basis of the patient's "Knowledgeable Implied Consent".

Note: The "Circle of Care" does not include people or organizations that are not defined as "Custodians" under PHIA (express documented verbal or written Patient consent is required to share information with non-Custodians).

Confidentiality: The obligation of an individual, organization, or Custodian to protect the PHI entrusted to it and not to misuse or wrongfully disclose it.

Consent: Must be voluntary, knowledgeable, and relate to the specific collection, use, and/or disclosure of the individual's PHI. If the patient/client does not have Capacity (as defined above), then Consent must be obtained from the Substitute Decision Maker.

Consent can be *express* or *implied*. Express consent is given either verbally or in writing. Implied consent is consent that can reasonably be inferred from the actions of the Patient or their SDM, if applicable. See definition of Knowledgeable Implied Consent below.

Custodian: An individual or organization listed in the *Personal Health Information Act* and its regulations including, but not limited to:

- A regulated health professional in private practice;
- NSHA/IWK;
- The Review Board under the *Involuntary Psychiatric Treatment Act*

- A pharmacy licensed in Nova Scotia;
- A continuing care facility licensed by the Minister under the *Homes for Special Care Act* or a continuing care facility approved by the Minister; and
- Any entity as defined in the PHIA Regulations.

De-Identified Information: Information that has had all identifiers removed that:

- Identify the individual, or
- Where it is reasonably foreseeable in the circumstances, could be utilized, either alone or with other information, to identify the individual.

Discipline: A process between a manager and Employee to address an employee's failure to adhere to policies or standards of performance, conduct or behaviour. This process can include verbal or written warnings, suspension and/or termination of employment.

Employee: A person working at NSHA whose salary and compensation are provided by NSHA.

Knowledgeable Implied Consent A type of consent that (in certain circumstances) permits healthcare providers to collect, use, and disclose a Patient's PHI, without obtaining express consent from the Patient.
For example, information can be shared among members of the Patient's treating health care team (the "Circle of Care") on the basis of Knowledgeable Implied Consent.

You can rely on Knowledgeable Implied Consent if it is reasonable in the circumstances to believe the Patient (or their SDM) knows: (a) the purpose of the collection, use, or disclosure of the Patient's PHI, and (b) that they have the right to withhold consent. In order to rely on Knowledgeable Implied Consent, NSHA and its Staff must take steps to make Patients and SDMs aware of NSHA's information practices. This is done through posters and pamphlets that explain why PHI is collected, used, and disclosed, and/or discussing NSHA's information practices with Patients/SDMs, and answering questions they may have (or directing them to someone who can answer these questions).

Patient In NSHA, the term Patient means all individuals including clients, residents and members of the public who receive or have requested health care or services from NSHA and its health care providers.

Personal Health Information (PHI)

Identifying information about a Patient (i.e. information that identifies or could reasonably be used to identify an individual either alone or with other information), whether living or deceased, and in both recorded and unrecorded forms, if the information relates to:

- The physical or mental health of the Patient, including information that consists of the health history of the individual's family,
- The application, assessment, eligibility and provision of health care to the Patient, including the identification of a person as a provider of health care to the individual, payments, or eligibility for health care in respect of the individual,
- The donation by the Patient of any body part or bodily substance of the individual, or information that is derived from the testing or examination of any such body part or bodily substance,
- The individual's registration information, including the individual's health-card number, or
- Identification of an individual's Substitute Decision Maker.

Personal Information International Disclosure Protection Act (PIIDPA):

Nova Scotia legislation that governs the access, storage, disclosure and transportation of personal information outside of Canada, including PHI.

Privacy:

An individual's right to determine when, how, and to what extent they share PHI about themselves with others.

Privacy Breach:

Inappropriate or unauthorized access, collection, use, disclosure, copying, modification, retention, or disposal of PHI. Privacy Breaches may be accidental or intentional. Examples include, but are not limited to:

- Loss and theft of PHI;
- Faxing PHI to the wrong fax number; and
- Viewing PHI without a work-related reason, even though the PHI was not shared with others, etc.

Research Ethics Board (REB):

A REB has the authority and resources to review research protocols that will be conducted within an organization. It reviews

	all projects involving Patients, Staff, resources, and data and gives approval before the research can begin.
Security:	The measures taken to protect PHI from unauthorized or unintentional loss, theft, access, use, modification or disclosure.
Staff:	Any Employee, physician, volunteer, learner, board member, contractor, contract worker, franchise employee, foundation employee and any other individual performing work activities within the Nova Scotia Health Authority.
Substitute Decision Maker (SDM)	For the purpose of PHIA, an SDM may give or refuse consent to the collection, use and disclosure of PHI on the behalf of an individual who lacks the capacity to make the decision. The SDM of an individual shall be chosen from the following descending order: (a) a person who is authorized by or required by law to act on behalf of the individual; (b) the individual's guardian appointed by a court of competent jurisdiction; (c) the spouse of the individual; (d) an adult child of the individual; (e) a parent of the individual; (f) a person who stands in loco parentis to the individual; (g) an adult sibling of the individual; (h) a grandparent of the individual; (i) an adult grandchild of the individual; (j) an adult aunt or uncle of the individual; (k) an adult niece or nephew of the individual; (l) any other adult next of kin of the individual; (m) the Public Trustee.

District Health Authority Policies Being Replaced

AVDHA 120.037 Privacy

AVDHA 140.092 Confidentiality

CBDHA 3-001 Confidentiality

CBDHA 3-010 NShIS Privacy & Security

CBDHA 3-012 Information Protection and Handling a Privacy Breach

CDHA 30-100 Privacy and Confidentiality of Personal Health Information

CEHHA 106-003 Information Protection and Handling a Privacy Breach

CEHHA 106-005 Privacy & Confidentiality of Personal Health Information

CEHHA 106-009 Privacy Impact Assessments

CEHHA 116-028 Privacy & Confidentiality

CEHHA 404-414 Confidentiality of Patient Information

CEHHA 405-107 Confidentiality of Health Information

CHA 101-001 Privacy

CHA 227-001 Confidentiality and Privacy

CHA 228-030 Confidentiality of Patient Information

GASHA 3-30 Confidentiality

GASHA 3-35 Privacy

GASHA 10-31 NShIS Privacy and Security

PCHA 2-c-10 Confidentiality

PCHA 1-p-40 Privacy of Personal Health Information

SSDHA AD-110-901 Protection and Management of Personal Health Information

SSDHA AD-110-902 Privacy Breach

SWNDHA 205.0 Confidentiality

SWNDHA 206.0 Privacy of Information

Version History

Major Revisions (e.g. Standard 4 year review)	Minor Revisions (e.g. spelling correction, wording changes, etc.)
New 2017-07-10	
Revised: Feb. 13, 2020	