Atikokan Health and Community Services
Health Privacy Policy

Atikokan Health and Community Services (AHCS) is committed to patient[1] privacy and to protecting the confidentiality of health information.

AHCS is a health information custodian (HIC) under the *Personal Health Information Protection Act, 2004* (PHIPA). AHCS is accountable and liable for compliance with PHIPA and the protection of health records. AHCS has obligations to make and keep health records under the *Public Hospitals Act, Mental Health Act, Vital Statistics Act* and under other legislation and documentation standards for regulated health professionals.

The AHCS health record contains information compiled at AHCS relating to the health history, care, treatment, assessment, examination or investigation of a patient. The health record provides a medium of communication for past, current, and future patient care.

PHIPA applies to records of "personal health information", which is a defined term. We refer to the health record in this policy – although there may be additional records of personal health information that are subject to PHIPA. For example, video surveillance recordings can be records of personal health information to which a patient could have a right of access.

"Team Members" includes AHCS staff, students, board members, volunteers, researchers, consultants, vendors and any other agents.

There are additional privacy policies that are included by reference to this Health Privacy Policy and are listed at Appendix A: AHCS's Privacy Program. All Team Members agree to abide by those policies, procedures and other materials as well.

AHCS is also subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA). Some personal information collected, used and disclosed by the hospital is subject to FIPPA and not PHIPA. AHCS is also subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) when it collects, uses, and/or discloses personal information in the course of commercial activities.

Principle 1 – Accountability for Personal Health Information

AHCS is responsible for any personal health information held.

AHCS has a Privacy Officer. The Privacy Officer is accountable for compliance with this Health Privacy Policy and compliance with PHIPA.

AHCS's commitment to privacy is demonstrated by adherence to privacy policies and procedures to protect personal health information and by educating Team Members who collect, use or disclose personal health information on AHCS's behalf about their privacy responsibilities.

[1] We have used the term "patient" throughout the policy. "Patient" (also known as client or resident) includes former patient, out-patient, former out-patient and anyone who is or has been detained in a psychiatric facility. It is possible that we hold personal health information about individuals who are not or were not officially AHCS patients and this policy would apply equally to those individuals.

Principle 2 – Identifying Purposes for Collecting Personal Health Information

We collect personal health information for purposes related to direct patient care, administration and management of programs and services, patient billing, administration and management of the health care system, research, teaching, statistical reporting, quality improvement, meeting legal obligations and as otherwise permitted or required by law.

We may collect PHI for the purposes of fundraising and marketing within the limitations detailed in PHIPA and any other relevant legislation.

When personal health information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified prior to use. Unless the new purpose is permitted or required by law, consent will be required before the information can be used for that purpose.

Principle 3 – Consent for the Collection, Use and Disclosure of Personal Health Information

In general, AHCS requires consent in order to collect, use, or disclose personal health information. However, there are some cases where AHCS may collect, use or disclose personal health information without consent as permitted or required by law.

a. Implied consent – Circle of Care – Disclosures to other health care providers for health care purposes

Patient information may be released to a patient's other health care providers for health care purposes (within the "circle of care") relying on implied consent and without requiring the express written or verbal consent of the patient as long as it is reasonable in the circumstances to believe that the patient wants the information shared with the other health care providers. No patient information will be released to other health care providers if a patient has stated they do not want the information shared (for instance, by way of the placement of a "lockbox" or "consent directive" on their health records).

A patient's request for treatment constitutes implied consent to use and disclose their personal health information for health care purposes, unless the patient expressly instructs otherwise.

Who can be in the "circle of care" includes (among others providing direct patient care if authorized by PHIPA):

Within AHCS:

- Interprofessional health providers (Physician, Nurse Practitioner, Registered Nurse, Registered Practical Nurse, Personal Support Worker, Physiotherapist, Occupational Therapist, Kinesiologist, Dietitian, Pharmacist, Pharmacist Technician, Laboratory Technician, Diagnostic Imaging, Social Worker)
- Medical students and residents and nursing or other interdisciplinary health care students

Outside of AHCS: (among others)

- Other hospitals
- Primary care and specialists: doctors' offices, Family Health Teams, Nurse Practitioner-Led Clinics,

birth centres
- Regulated health professionals or social workers and social service workers in solo or group practice
- Ambulance and paramedics
- Pharmacies
- Laboratories
- Long-term care homes and retirement homes
- Home and community care service providers
- Indigenous health service providers and Aboriginal Health Access Centres
- A centre, program or service for community health or mental health whose primary purpose is the provision of health care
- Supportive housing
- Public health
- Rainy River District Ontario Health Team

Sharing within the circle of care includes through shared electronic health systems such as the Meditech EMR (Atikokan General Hospital), PS Suites (Atikokan Family Health Team), TREAT (Atikokan Community Counseling), Ontario Laboratory Information Systems (OLIS), Connecting Ontario, and local, regional and provincial programs.

For clarity – the following groups are NOT in the circle of care and AHCS does not share personal health information about patients with them relying on implied consent. That does not mean AHCS never discloses to these individuals and groups - but AHCS only does so with express consent or as otherwise permitted or required by law to disclose:
- Children's Aid Society
- Police
- Landlords
- Employers
- Spiritual leaders/healers
- Insurance companies
- Teachers and schools (however, psychologists, social workers, nurses, psychiatrists, speech-language pathologists, occupational therapists, physiotherapists, or audiologists affiliated with schools may be in the circle of care if they are providing health care)

b. Implied consent – affiliation

If a patient tells AHCS about their religious or other organizational affiliation, AHCS may give their name and location to someone from that religious or other organization who may offer to provide support, such as spiritual care, unless the patient says not to.

c. Implied consent – general health status and location

AHCS may share general information about a patient, such as the fact that the individual is a patient in AHCS, their location and general health status, with others, including friends and family and the general

public, unless the patient tell us not to. At the first reasonable opportunity after admission, AHCS explains to patients that this information will be disclosed unless they object.

d. Express consent

Patients may also provide a verbal or written consent if they wish for AHCS to release their information.

See "*Disclosure and Release of Patient Information Policy*".

We note that PHIPA does not apply to "aboriginal midwives" or "aboriginal healers" who are providing "traditional" services in "aboriginal communities"[2]. The provincial laws do not have jurisdiction over these providers. We consider these providers to be vital members of our care community. When we share information with these providers, we do so with the express permission of patients.

e. No Consent

There are certain activities for which consent is not required to collect, use or disclose personal health information. These activities are permitted or required by law. For example, AHCS does not need consent from patients to (this is not an exhaustive list):

- Contact a relative if a patient is incapacitated
- Prevent serious harm to patients or others when necessary
- Plan, administer and manage internal operations, programs and services
- Do financial reporting and get payment for the services provided
- Engage in quality improvement, error management, and risk management activities
- Participate in the analysis, administration and management of the health care system
- Engage in some research projects (subject to certain rules, such as obtaining Research Ethics Board (REB) Centre for Health Care Ethics, Lakehead University approval and having research contracts)
- Teach, train and educate Team Members and others
- Compile statistics for internal or mandatory external reporting
- Respond to legal proceedings
- Comply with mandatory reporting obligations including reporting certain diseases to public health authorities or if we suspect certain types of abuse

A list of mandatory reporting obligations is found in our "*Disclosure and Release of Patient Information Policy*".

f. Withholding or Withdrawal of Consent

If consent is sought, a patient may choose not to give consent ("withholding consent"). If consent is given, a patient may withdraw consent at any time, but the withdrawal cannot be retrospective. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

g. Lockbox – Consent Directive

PHIPA gives patients the opportunity to restrict access to any personal health information or their entire health record by their health care providers within AHCS or by external health care providers. Although the term "lockbox" is not found in PHIPA, lockbox is commonly used to refer to a patient's ability to withdraw or withhold consent for the use or disclosure of their personal health information for health care purposes. See the "*Lockbox Policy*" for details of how the lockbox works.

Principle 4 – Limiting Collection of Personal Health Information

AHCS limits the amount and type of personal health information collected to that which is necessary to fulfill the purposes identified. Information is collected directly from the patient, unless the law permits or requires collection from third parties. For example, from time to time AHCS may need to collect information from family members, other health care providers or police in order to get timely, accurate

[2] This is the language included in section 3(4) of PHIPA.

or complete information.

Personal health information may only be collected within the limits of each Team Member's role. Team Members should not initiate their own projects to collect new personal health information from any source without being authorized by AHCS.

Principle 5 – Limiting Use, Disclosure and Retention of Personal Health Information

a. Use

Personal health information is not used for purposes other than those for which it was collected, except with the consent of the patient or as permitted or required by law.

Personal health information may only be used within the limits of each Team Member's role. Team Members may not read, look at, receive or otherwise use personal health information unless they have a legitimate "need to know" as part of their position. If a Team Member is in doubt whether an activity to use personal health information is part of their position – they should ask their supervisor or the Privacy Officer. For example, looking at health records out of personal curiosity or a self-initiated education project without being assigned to those patients and without specific authorization for an approved educational exercise is not permitted.

b. Disclosure

Personal health information is not disclosed for purposes other than those for which it was collected, except with the consent of the patient or as permitted or required by law.

Personal health information may only be disclosed within the limits of each Team Member's role. Team Members may not share, talk about, send to or otherwise disclose personal health information to anyone else unless that activity is an authorized part of their position. If a Team Member is in doubt whether an activity to disclose personal health information is part of their position – they should ask supervisor or the Privacy Officer.

c. Retention

Health records are retained as required by law and professional regulations and to fulfill AHCS's purposes for collecting personal health information. See the *"Retention Policy"*.

AHCS follows the *Public Hospitals Act* and Hospital Management Regulation guidelines for retaining health records. In some cases, AHCS keeps records for longer than this minimum period as recommended by the Ontario Hospital Association's Records Retention Toolkit.

Personal health information that is no longer required to fulfill the identified purposes is destroyed, erased, or made anonymous safely and securely. See *"Safeguards Guidelines for Personal Health Information"*.

Principle 6 – Accuracy of Personal Health Information

AHCS takes reasonable steps to ensure that personal health information held is as accurate, complete, and up to date as is necessary to minimize the possibility that inappropriate information may be used to make a decision about a patient.

Principle 7 – Safeguards for Personal Health Information

AHCS has safeguards for the personal health information, which include:

- Physical safeguards (such as confidential shredding bins, locked filing cabinets and rooms, clean desks);
- Organizational safeguards (such as permitting access to personal health information by Team Members on a "need-to-know" basis only); and
- Technological safeguards (such as the use of passwords, encryption, audits, and secure disposal).

AHCS takes steps to ensure that the personal health information is protected against theft, loss and unauthorized use or disclosure. See *"Safeguards Guidelines for Personal Health Information"*.

AHCS requires anyone who collects, uses or discloses personal health information on AHCS's behalf to be aware of the importance of maintaining the confidentiality of personal health information. This is done through the signing of confidentiality agreements, privacy training, and contractual means. As a condition of employment, all new AHCS employees/agents must sign a PHIPA Compliance Agreement. All AHCS employees are required to re-sign the PHIPA Compliance Agreement annually and participate in ongoing privacy education. See *"Mandatory Privacy and Security Training Policy."*

Care is used in the disposal or destruction of personal health information, to prevent unauthorized parties from gaining access to the information.

Principle 8 – Openness about Personal Health Information

Information about AHCS policies and practices relating to the management of personal health information is available to the public, including:

- Contact information for the Privacy Officer, to whom complaints or inquiries can be made;
- The process for obtaining access to personal health information, and making requests for its correction;
- A description of the types of personal health information, including a general account of AHCS's uses and disclosures; and
- A description of how a patient may make a complaint to the Privacy Officer or to the Information and Privacy Commissioner of Ontario.

AHCS posts privacy information on its website.

Principle 9 – Patient Access to Personal Health Information

Patients may make written requests to have access to their records of personal health information, in accordance with the *"Patient Records Access and Correction Policy"*.

AHCS will respond to a patient's request for access within reasonable timelines and costs to the patient, as governed by law. AHCS takes reasonable steps to ensure that requested information is made available in a format that is understandable.

Patients have a right to ask for their records to be corrected if they can demonstrate that the records AHCS holds are inaccurate or incomplete in some way for the purposes for which AHCS holds that information. In some cases, instead of making a correction, AHCS may offer a patient an opportunity to append a statement of disagreement to their file.

AHCS may not be able to provide access to all the personal health information about a patient. Exceptions to the right of access requirement will be in accordance with law. Examples may include information that could reasonably be expected to result in a risk of serious harm or the information is subject to legal privilege.

Principle 10 – Challenging Compliance with Privacy Policies and Practices

Any person may ask questions or challenge AHCS's compliance with this policy or with PHIPA by contacting the Privacy Officer:

AHCS Privacy Officer
120 Dorothy Street
Atikokan, Ontario P0T 1C0
P (807) 597-4215 | F (807) 597-1210 | privacy@aghospital.on.ca

AHCS receives and responds to complaints or inquiries about policies and practices relating to the handling of personal health information. AHCS will inform patients who make inquiries or lodge complaints of other available complaint procedures, which may include applicable regulatory colleges.

AHCS investigates all complaints. If a complaint is found to be justified, AHCS will take appropriate measures to respond.

The Information and Privacy Commissioner of Ontario oversees compliance with privacy rules and PHIPA. Any individual can make an inquiry or complaint directly to the Information and Privacy Commissioner of Ontario by writing to or calling:

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 Canada
Phone: 1 (800) 387-0073
www.ipc.on.ca

Appendix A – AHCS's Privacy Program
Supporting Privacy Policies/Procedures/Documents

The following policies and documents are incorporated into the Health Privacy Policy:
**To be determined: Date to be updated as reviewed and published.*

Policy and Document Name	Last Updated
Public Health Privacy Notice	Feb 2025
Health Privacy Breach Procedures	*TBD
Consent, Substitute Decision-Making for Privacy Decisions and Deceased Persons Records Policy Appendix A: Attestation of Estate Trustee or Estate Administrator Appendix B: Sharing Health Information with a Caregiver Form Appendix C: Patient Consent for Voicemail Communication	*TBD
Patient Records Access and Correction Policy	*TBD
Disclosure and Release of Patient Information Policy Appendix A: Consent for Disclosure of Personal Health Information Form Appendix B: Mandatory Disclosures	*TBD
Communicating with Police Policy	*TBD
Fees for Release of Health Information under PHIPA	*TBD
Lockbox Policy Appendix A: Patient Lockbox Information Brochure Appendix B: Patient Lockbox Request Form	*TBD
Safeguards Guidelines for Personal Health Information, including Restricted Access to Personal Health Information (no snooping) Accounts and Passwords Physical Security On-Site Sending Patient Information Electronic Mail – refers to separate policy Texting Facsimile (Faxes) – refers to separate policy Social Media Telephone Mail Virtual Care Documentation Administrative Safeguards for Virtual Care Working from Home or Other Remote Sites Devices Technology Remote Workspaces Filing Patient Information Destroying Patient Information Third Party Vendors Logging and Auditing in Electronic Medical Record Logging Audits Inquiry of Unauthorized or Questionable Activity Breach of Privacy Safeguards	*TBD

Electronic Mail of Patient Information Policy Appendix A: Patient Consent and Release for Email Appendix B: Email Disclaimer Message Appendix C: Automatic Response Email	*TBD
Transmission of Personal Health Information via Facsimile Policy	*TBD
Mandatory Privacy and Security Training Policy Appendix A: PHIPA Compliance Agreement	*TBD
Video Surveillance Policy	*TBD
Retention and Destruction Policy	*TBD
Health Privacy Inquiries and Complaints Policy Appendix A: Privacy Complaint Form Appendix B: Privacy Breach/Complaint Intake Form Appendix C: Privacy Complaint Investigation Report	*TBD
Use of Personal Health Information for Education, Quality Assurance and Research Appendix A: Research Request Fee Schedule for Health Information Management Appendix B: Electronic Medical Record (EMR) and Documentation Requirements Appendix C: Request for Use of Personal Health Information for Research, Education and Quality Assurance Form	*TBD