First Nations Health Authority
Board Policy

First Nations Health Authority
Health through wellness

Name	**Privacy Policy**
Category	Information and Communication
Type	Corporate

For Board Secretariat (do not fill this in)		
Document #	**Effective**	
IAC-23-001-006		
Board Approved Date	**Verified By**	**Authorization (BoD Motion #)**
May 25, 2023	Bevan	MOTION 0523-BOD-01

1.0 Purpose

1.1 The purpose of this policy is to establish principles and guidance for managing Personal Information in the Custody or under the Control of First Nations Health Authority (FNHA).

1.2 This policy is supported by the 7 Directives and Shared Values.

2.0 Scope

2.1 This policy applies to Workers, the Board of Directors (Board) and Members.

2.2 This policy applies to Client, Worker and any other Personal Information in the Custody or under the Control of FNHA regardless of format or medium.

2.3 This policy applies to all Workplaces.

3.0 Statements

Principles

3.1 FNHA and its Workers must comply with

(a) the *Personal Information Protection Act*;

(b) health-sector-specific legislation, including but not limited to, *Medicare Protection Act*, *Public Health Act*, *Health Professions Act*, and *Pharmaceutical Services Act*; and

(c) any other applicable professional codes of ethics and standards of practice.

3.2 FNHA will demonstrate organizational accountability and responsibility for managing Personal Information in its Custody or under its Control in order to maintain trust-based relationships with Clients, Workers, healthcare partners, and business partners.

3.3 FNHA will be transparent with Clients, Workers, healthcare partners, business partners and the public regarding the management of Personal Information.

3.4 FNHA acknowledges an individual's right to their Personal Information and will assist individuals who request access to their Personal Information to the degree that providing access does not negatively impact others.

3.5 The Chief Executive Officer (CEO) will report significant Privacy Breaches to the Board, which could include breaches involving a large volume of information, many individuals' information, and/or multiple departments.

3.6 FNHA will protect Personal Information in accordance with this policy and the *Information Security* Policy Documents.

Directives

Consent for Collection, Use, and Disclosure of Personal Information

3.7 When collecting Personal Information in any format (i.e. electronic, audio/visuals, paper), Workers will consult with the Privacy Office on appropriate data management and obtain appropriate consent.

3.8 Workers must obtain consent for the collection, use, or disclosure of Personal Information about an individual unless

(a) the law authorizes the collection, use, or disclosure without the consent of the individual; or

(b) the law deems the collection, use or disclosure to be consented to by the individual.

3.9 Workers must give individuals sufficient Information on the specific purposes for collection, use, and disclosure of their Personal Information so they can make an informed decision regarding consent. Consent cannot be obtained by providing incorrect or incomplete Information.

3.10 Consent can be obtained by either express consent, implied consent, or by opting in/out:

(a) Workers can gain express consent from an individual by informing them of the reason for the use, collection and disclosure of their Personal Information and getting their consent either in writing or verbally.

(b) Workers can rely on the implied consent from an individual if FNHA's reason to collect, use or disclose their Personal Information would be obvious to a reasonable person (e.g., a Client provides health Information to Health Benefits to process a benefits claim).

(c) consent can be obtained if an individual agrees to opt-in or opt-out of providing their Personal Information for a program or service (e.g., checking a box to participate in a survey).

3.11 Workers may collect, use, and disclose Personal Information without consent from the individual or from a source other than the individual only in specific circumstances including

(a) when it is clearly in the interests of the individual and consent cannot be obtained in a timely manner;

(b) when the information is about a minor and consent is required from the minor's parent or guardian;

(c) when it is necessary for medical treatment of the individual and/or if the individual is in imminent harm and/or the individual does not have the legal capacity to give consent;

(d) the Personal Information is collected in a Public Setting or from a public source (i.e., at which the individual voluntarily appears); or

(e) the collection is required or authorized by law.

3.12 Workers may collect, use, and disclose Personal Information from, or on behalf of, another organization without consent if

(a) the individual previously consented to the collection and use of the Personal Information by the other organization; and

(b) the Personal Information is used, disclosed to or collected by FNHA solely for the purposes for which the Information was previously collected and to assist FNHA in conducting work on behalf of the other organization.

3.13 Workers will consult with the Privacy Office on any situation involving Personal Information that relies on previous consent obtained by either FNHA or an External Party where FNHA wants to use the Personal Information for a similar or secondary purpose.

3.14 Workers must respect an individual's right to withdraw consent at any time with reasonable notice, subject to any legal agreement or other restrictions.

3.15 If an individual wishes to withdraw consent for use of Personal Information previously provided to FNHA, Workers may consult with the Privacy Office for advice and instruction on how to withdraw consent. Workers must inform individuals of any implications of such withdrawal.

3.16 If an individual still wants to withdraw their consent, the Privacy Office or respective department will strive to identify and coordinate the elimination of any use of the individual's Personal Information. The Privacy Office will notify the individual if it is not possible to suspend all use of the Personal Information.

Collection, Use, Disclosure, and Retention of Personal Information

3.17 Workers must collect, use, and disclose only the type and amount of Personal Information needed to conduct FNHA business, programs, or activities on a Need to Know basis and must not collect, use, or disclose more Personal Information than is required to fulfill those purposes. The business, programs and activities include, but are not limited to:

(a) providing First Nations communities in BC with primary health care services;

(b) administering health benefits plans;

(c) research, surveillance, and program evaluation to inform development of health programs and services, and for responding to public health incidents; and

(d) establishing, managing, and terminating an employment relationship.

3.18 Workers must not collect, use, and disclose Personal Information for purposes other than those for which it was originally collected, used, or disclosed, except with the consent of the individual or as required by law.

3.19 Upon written request, individuals will be informed of the existence, use, and disclosure of their Personal Information in the Custody or under the Control of FNHA.

3.20 Workers must take all reasonable steps to ensure that the Personal Information FNHA collects, uses or discloses is as accurate, complete, and as up-to-date as reasonably possible for the purposes that are known at the time of collection, use, or disclosure.

3.21 Any inaccurate or incomplete Personal Information must be amended upon request by the individual.

3.22 If Workers use an individual's Personal Information to make a decision that directly affects the individual, Workers must retain that Information for at least one year following the decision to provide the individual a reasonable opportunity to access it.

3.23 Any Personal Information created by Workers about themselves, either by saving a file or through personal email, should not be stored either electronically on an FNHA device or in hard copy. Anything sent to FNHA or stored on an FNHA device, including personal emails containing Personal Information, could be disclosed (e.g., during legal proceedings).

3.24 Workers will destroy Records containing Personal Information in accordance with the *Records and Information Management* Policy Documents.

3.25 Requests for First Nations identifiable health and wellness Data and Information will be managed in accordance with the *Health Data and Information Governance* Policy Documents.

Worker Personal Information

3.26 Workers must collect, use, and disclose only the type and amount of Worker Personal Information that is reasonably required to conduct the following activities, including but not limited to:

(a) determine eligibility for employment, including verifying qualifications and references;

(b) establish training and development requirements;

(c) manage performance, including investigations;

(d) administer Worker pay and benefits;

(e) process work-related claims (e.g., benefits, Workers' compensation, and insurance claims);

(f) comply with requirements of funding bodies;

(g) comply with applicable laws (e.g., the *Income Tax Act* and *Employment Standards Act*); and

(h) carry out specific job duties on a Need to Know or Least Privilege basis.

3.27 In circumstances where Workers are legally permitted to collect, use, or disclose Worker Personal Information without consent, Workers must notify the Worker of such collection, use, or disclosure.

Access to Personal Information

3.28 Access to Personal Information on FNHA Information Systems will be assigned based on the practice of Least Privilege and will be managed in accordance with the *Information Security* Policy Documents.

3.29 Workers will not charge Aboriginal applicants a fee for requesting access to their Personal Information.

3.30 Workers may charge non-Aboriginal applicants a fee commensurate to the cost of processing the request to access their Personal Information (other than Worker Personal Information).

3.31 If an individual is required to pay a fee for processing an information request, Workers in coordination with the Privacy Office

(a) Must give the applicant a written estimate of the fee before providing the service, and

(b) may require the applicant to pay a deposit for all or part of the fee.

3.32 Workers must not charge fees to process access requests for Worker Personal Information.

3.33 Workers will make a reasonable effort to assist each applicant and to respond to each applicant as accurately and completely as reasonably possible.

3.34 Workers must respond to an applicant no later than 30 days (excluding holidays and Saturdays) after receiving the applicant's request, or by the end of an extended time period approved by the applicant and/or the Office of the Information and Privacy Commissioner (OIPC).

3.35 In coordination with the Privacy Office, Workers may request an extension from the OIPC under the following circumstances:

(a) the applicant does not give enough detail to enable FNHA to identify the Personal Information requested,

(b) a large amount of Personal Information is requested or must be searched and meeting the time limit would unreasonably interfere with the operations of FNHA, or

(c) more time is needed to consult with another organization or public body before FNHA is able to decide whether or not to give the applicant access to the requested information.

3.36 If the time limit is extended, Workers must inform the applicant of

(a) the reason for the extension,

(b) the time when a response from FNHA can be expected, and

(c) the rights of the applicant to contact the OIPC and request the time extension be reduced.

3.37 If access is permitted, Workers will provide each applicant with

(a) the requested Personal Information; or

(b) a reasonable opportunity to examine the Personal Information if the requested Personal Information cannot be reasonably provided.

3.38 If access is denied, Workers must inform the applicant of the

(a) reasons for the refusal and the provision(s) of the *Personal Information Protection Act* (PIPA) on which the refusal is based;

(b) contact Information for the Privacy Office which can answer the applicant's questions about the refusal; and

(c) applicant's right to ask the OIPC for a review within 30 days of being notified of the refusal.

Privacy

3.39 Workers will complete the initial privacy training within six months of onboarding.

(a) thereafter, Workers will complete the privacy refresher training annually.

3.40 Managers/Supervisors must conduct Privacy and Security Risk Assessments (PSRA) when implementing a new initiative, program, or activity involving new collection, use and disclosure of Personal Information to ensure safeguards for Personal Information are met.

3.41 Managers/Supervisors will work with the Privacy Office to complete PSRAs. The Privacy Office will collaborate with the IT Security Office as needed.

3.42 The Privacy Office will conduct regular internal reviews and audits of Personal Information holdings and controls.

3.43 The Privacy Office will advise on privacy and compliance issues as well as on matters of interpretation and application of this Policy.

3.44 The Privacy Office will review amendments to privacy legislation and make recommendations for policy changes.

3.45 When this policy changes, FNHA's confidentiality and non-disclosure agreement templates may be amended for future use.

Privacy Complaints

3.46 Workers who are concerned about FNHA's compliance with this policy or with any relevant privacy legislation are encouraged to contact the Privacy Office.

3.47 Workers will inform Clients and members of the public who are concerned about FNHA's compliance with any relevant privacy legislation that they are entitled to lodge a complaint with the Privacy Office, or directly with the OIPC.

(a) The Privacy Office will provide contact Information on FNHA's website to receive and respond to questions from Clients and the public regarding the management of Personal Information.

3.48 Workers who receive complaints regarding FNHA's handling of Personal Information will direct those complaints to the Privacy Office.

3.49 The Privacy Office will acknowledge, catalog, assess and investigate complaints.

3.50 If the Privacy Office determines a complaint will be investigated, the Privacy Office will create a written response (*Privacy Investigation Summary*) outlining the measures FNHA will take in response to the complaint, which may include a commitment to amend Policy Documents.

3.51 Once the complaint has been resolved, the Privacy Office will send a response to the complainant.

Privacy Breaches

3.52 Workers will identify, contain and report on the actual or suspected Privacy Breach (e.g., misdirected fax, email or unauthorized access to Personal Information) to their Manager/Supervisor and the Privacy Office.

3.53 The Privacy Office will outline measures to identify and contain Privacy Breaches.

3.54 The Privacy Office and the IT Security Office will work closely together on any Privacy Breaches that may involve either party.

3.55 The Privacy Office will investigate Privacy Breaches and notify the OIPC and affected individuals when legally required and may notify the OIPC and affected individuals if substantial business or personal risks are identified.

3.56 Workers in consultation with the Privacy Office will inform partners if a Privacy Breach impacts Information relating to the partnership.

3.57 The Privacy Office will report significant Privacy Breaches to the CEO, which could include breaches involving a large volume of Information, many individuals' Information, and/or multiple departments.

Compliance

3.58 Any violations of this policy may result in Disciplinary Action, up to and including termination, in accordance with the *Progressive Corrective and Disciplinary Action* Policy Documents.

Exceptions

3.59 Exceptions to this policy require approval by the CEO.

Delegation

3.60 This policy is further defined and elaborated upon through procedures. The Senior Executive responsible for Privacy has been delegated responsibility for ensuring compliance with this policy, and the development, approval, implementation and monitoring of procedures that relate to Privacy. Any new, amended or removed procedure will be reported to the CEO.

4.0 Responsibilities

4.1 Board of Directors (Board): approve the *Privacy Policy*.

4.2 Chief Executive Officer (CEO): provide overall leadership and support to Senior Executives in the oversight and management of Personal Information; report Privacy Breaches to the Board; review and approve exceptions as appropriate.

(a) Privacy Office: provide leadership, direction, and solutions for ensuring that the management of Personal Information complies with privacy legislation; work with Managers/Supervisors to complete PSRAs; respond to and investigate public inquiries and complaints; report significant Privacy Breaches to the CEO.

4.3 Senior Executive responsible for Information Management and Information Technology (IMIT): provide resources to support compliance.

(a) IT Security Office: work closely with the Privacy Office to manage Privacy Breaches that may impact either party; collaborate with the Privacy Office on PSRAs as needed.

4.4 Senior Executives: provide resources to support compliance within their departments.

(a) Managers/Supervisors: communicate expectations and ensure Workers are trained and comply with this policy.

(b) Workers: manage Personal Information in accordance with the *Privacy* Policy Documents.

5.0 Definitions

Aboriginal: First nations, Métis, and Inuit.

Client(s): an individual, resident, family, or community that receives direct care or accesses health and wellness services delivered by the organization and has the ability to decide and define the programs and services that will best support their health and well-being. Services enable each individual to become well-informed and best able to make decisions as it relates to their personal and collective health.

Control: having the authority and responsibility to decide what other parties do with Information or Data under their Custody, even though that Information or Data is not necessarily owned or possessed by FNHA.

Custody: having physical possession and Control of Information or Data, but not necessarily ownership.

Disciplinary Action(s): a process for dealing with job-related behaviour that does not meet expected and communicated performance standards, including non-compliance with Policy Documents.

External Party(ies): any FNHA business partner entity or other non-FNHA entity.

Information: Data organized and analyzed in a structured manner that provides context.

Information Management Services (IMS): a team within Information Management and Information Technology (IMIT) that is responsible for managing organizational Records and Information, regardless of medium or form, and providing related services.

Information System(s): a discrete set of Information resources organized for the Collection, processing, maintenance, use, sharing, dissemination, or disposition of Information. Information systems also include specialized systems such as industrial/process control systems, telephone switching and private branch exchange systems, and environmental control systems.

Least Privilege: the practice requiring that Workers be granted the most restrictive set of privileges, permissions, or lowest clearance needed to perform their work.

Manager(s)/Supervisor(s): a person working in a position authorized by FNHA to oversee and direct Workers' day-to-day job duties.

Need to Know: a principle where Workers may only access Data required for the performance of their respective duties.

Personal Information: information that can identify an individual (whether alone or in combination with other information) or that is about an identifiable individual. Personal information includes Worker personal information but does not include their business contact or work product information.

Policy Document(s): all existing documents within a policy set, including the Board-approved policy that provides principles and guidance and delegates authority to the CEO; consistent with approved policy, any procedures approved by Senior Executives that outline specific steps to be followed.

Privacy Breach(es): the loss of, unauthorized access to, or unauthorized disclosure of Personal Information resulting from a breach of an organization's security safeguards.

Public Setting(s): a location to which the public has access and is open to public view, with exception to areas specifically marked off for privacy. This includes public parks, sidewalks, parking lots, and lobbies.

Record(s): Information, regardless of medium or form, created, received, and maintained by an organization or person as evidence of its operations for Business Purposes, legal obligations, or both, that has value requiring its retention for a specific period of time.

Senior Executive(s): includes the Chief Executive Officer, Chief Officers, and Vice Presidents.

Worker(s): includes individuals employed or contracted with FNHA while engaged in a FNHA work activity; specifically, employees (union, non-union; permanent, term, casual; full-time, part-time); people working at FNHA through an Interchange Agreement; people paid via third-party agencies (temporary workers); contractors; consultants; trainees; students; volunteers.

Worker Personal Information: Personal Information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between FNHA and that individual, but does not include Personal Information that is not about an individual's employment.

6.0 Mandatory Compliance Documents

Employment Standards Act (British Columbia)

Health Professions Act (British Columbia)

Income Tax Act (Canada)

Medicare Protection Act (Canada)

Personal Information Protection Act (British Columbia)

Pharmaceutical Services Act (British Columbia)

Public Health Act (British Columbia)

7.0 Rescind and Interpretation Statements

7.1 With the approval of this policy, older versions are considered to be replaced and/or rescinded and are no longer in effect.

7.2 Where interpretation is required regarding the relationship between Policy Documents, the CEO has sole discretion to provide the interpretation.

8.0 Summary of Changes

Replaces	Dated	Key Changes to Previous Version
IAC-19-001-005 IAC-20-DIR-007-002	May 2, 2019 March 3, 2020	• Combined Personal Information Privacy Policy and Executive Directive. • Removed duplications. • Added clarification around the collection of personal information in various formats (i.e., electronic recording) and obtaining consent. • Technical edits.

9.0 Attachments

None.