Data Governance Framework
Privacy and Security Policy Manual

<NAME OF NATION>

Distributed on: Month DD, YYYY
Version: V1.0
Credit Statement

This document builds upon work that was conducted through the BC First Nations Panorama Implementation Project (i.e. the Privacy & Security Policy and Procedures document(s) of that project). Cowichan Tribes provided a copy of their policy documentation from that project to enable this effort to build on the good work done to date.

Warranty Disclaimer

This document and all of the information it contains are provided “as is” without warranty of any kind, whether express or implied. All implied warranties, including, without limitation, implied warranties of merchantability, fitness for a particular purpose, and non-infringement, are hereby expressly disclaimed. We do not make any warranties about the completeness, reliability and accuracy of this information. Any action you take upon the information in this document is strictly at your own risk.

Limitation of Liabilities

Under no circumstances will the Mustimuhw Information Solutions Inc. be liable to any person or business entity for any direct, indirect, special, incidental, consequential, or other damages based on any use of this document, including, without limitation, any lost profits, business interruption, or loss of programs or information, even if the Mustimuhw Information Solutions Inc. has been specifically advised of the possibility of such damages.

For more information contact Mustimuhw Information Solutions Inc. at 778-403-5473.

© Mustimuhw Information Solutions Inc. March 2015. To be freely used by First Nations and mandated and owned First Nations owned organizations, with clear acknowledgement to source.
Preface

The Data Governance Framework has been developed with the vision that “Our Nation governs and protects all Nation data and information, wherever it resides, supporting the needs of our Nation, communities, organizations, and Members, as well as the partners we collaborate with”. ¹

The Framework is a multi-faceted collection of strategy, structure, legislation, policy and related tools. It will evolve and grow in iterative cycles of expansion and refinement as our needs and capacities change and grow over time.

This document contains the Privacy and Security policies, procedures, and tools related to our management and protection of Nation data and privacy compliance.

Note: The Data Governance Framework document is the main protective blanket that provides the complete understanding of how our Nation Data is governed. This document is a supplementary portion to the Framework document – provisioned separately to make it easier to incorporate updates. The author and reader of this document is required to be familiar with the current Data Governance Framework document before applying or updating this document.

Tip: if Panorama has been implemented in your Nation this framework will supersede the P&S policy. Therefore incorporate any procedures already applied by the health center and then retire the P&S policies and implement this framework. Additionally other staff (e.g. Data Custodian(s)) or departments may have related privacy and/or security policies/procedures that need to be absorbed into this framework and subsequently retired.

¹ Data Governance Framework
Privacy Core Values

Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: none

Purpose:

Our Nation Members, customers, and Staff entrust us to be good and responsible stewards over their personal information. Nation Members, customers, and Staff have rights and require us to maintain and protect their personal information.

Additionally our Nation Members and customers expect us to share their personal information with other human and social service providers when it is required (e.g. in an emergent situation). When this information is shared between partners there is a shared expectation that the human related data is protected using the same practices, commitments and obligations.

The Personal Information Protection Act (British Columbia legislation) provides the legal authorities to protect human related information.

Outlining the rights, commitments and obligations in a policy provides transparency to all individuals and partners that we interact with; and reinforces our expectations of our Staff. Providing communication tools enhances our privacy culture which demonstrates our commitment and knowledge on the best practices to support protecting Human Related data.

Policy

When managing Human Related data the Data Governance Framework is to be imbedded in everything we do (e.g. if a principle, policy or procedure doesn’t exist or is unclear these rights, commitments, and obligations are to be used to provide guidance). Wherever Human Related data is collected from the Nation Member / customer or Staff a poster must be posted in a visible location that informs the individual of their privacy rights and provides information on how to get additional information on the subject of privacy.

Whenever Human Related data is exchanged with another party it must reflect these rights, commitments and obligations in a Data Governance and Information Sharing Information before
the data is exchanged. For further clarification refer to the Data Governance Framework policy ‘Data Sharing and/or Linking’.

All Staff must practice these rights, commitments, obligations in the course of fulfilling their roles/responsibilities.

<table>
<thead>
<tr>
<th>Privacy Values for Human Related Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rights of Nation Members, customers, and Staff</strong></td>
</tr>
<tr>
<td>• Confidentiality</td>
</tr>
<tr>
<td>• Ensuring their Human Related data is accurate</td>
</tr>
<tr>
<td>• Understanding who has access to his/her Human Related data, and for what purpose the individual required/requires access</td>
</tr>
<tr>
<td>• Understanding when their Human Related data is aggregated and summarized and for what purpose; and understand how they are protected from inference</td>
</tr>
<tr>
<td>• Understanding how long Human Related data is retained, and how it is disposed of when not required</td>
</tr>
<tr>
<td>• Understanding who their Human Related data is shared with and for what purpose prior to sharing</td>
</tr>
<tr>
<td>• Understand how their Human Related data is protected when shared</td>
</tr>
<tr>
<td>• Having these commitments and obligations built into the partnership agreements to ensure there is an appropriate balance between protecting an individual’s Human Related data and providing effective and informed human and social services using the collaborative shared service delivery models</td>
</tr>
<tr>
<td>• Ensuring we recognize and integrate the provincial and federal laws that apply to privacy such that our practices and Data Governance Framework does not conflict with these laws</td>
</tr>
<tr>
<td>• Provided information at the point of service delivery that informs the Nation Member / customer and staff of their rights and how to obtain additional information about privacy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Our Nation Staff are committed to our Nation to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure the Human Related data and the health and wellness of an individual will remain confidential; and an individual’s privacy is of the utmost importance</td>
</tr>
<tr>
<td>• Ensure that Human Related data that is aggregated and disclosed by our Nation does not have the potential to harm an individual</td>
</tr>
</tbody>
</table>

For example, a “Communicable Disease” report indicating percentage of Nation Members / customers who have a communicable disease may be acceptable; however, a “Community Disease by Age Group” report may be unacceptable, particularly if the report has a small number of people within a given age range and an individual’s identity could be inferred by the report.
| Commitment to our Partners | We recognize the value of sharing Human Related data for the purpose of assessing, planning, developing programs to support health and wellness of First Nations people in BC and Canada. We are committed to developing new partnership agreements and supporting existing partnerships that are dependent on the sharing of personal information or aggregated information providing the sharing of the information incorporates these rights, commitments and obligations, and is consistent with our Data Governance Framework. |
| Our Nation’s Obligations | • Take adequate / reasonable measures to protect client confidentiality  
• Take adequate and reasonable measures to protect Human Related data in our custody from risks such as unauthorized collection, access, use and disclosure irrespective of the form in which we store or transmit the data  
• Support our Staff with their privacy responsibilities (e.g. professional and regulatory requirements / standards and code of ethics)  
• Take adequate and reasonable measures to protect the Human Related data associated with staffing  
• Support the privacy responsibilities of our Partners; and assess any privacy risks inherited from these partnerships  
• Put into place policies and procedures that ensure researchers adhere to the core values of OCAP; and support the Tripartite Data Quality Sharing Agreement which enables Human Related data to be shared between federal/provincial/First Nation governments in adherence to the OCAP principles  
• Fulfill our privacy commitments to our Nation Members / customers, staff, our Nation, and First Nations people  
• Advocate for privacy to ensure a balance between privacy protection without disabling the shared human and social service delivery models that enables health & wellness for all First Nations and Nation customers  
• Fulfill our legal responsibilities |
Procedures

The Data Steward is required to prepare the poster (see the draft entitled ‘Privacy Rights, Commitments, Obligations’ located at the end of this document) and have it reviewed by the Data Governance Board.

Data Governance Board must approve the poster.

Upon approval the Data Steward must print and post in all locations where Human Related data is collected from a Nation Member / Customer or Staff.

The Poster is to be posted within one (1) month after approval of this policy.

On an annual basis the Data Steward must verify that the posters are in good condition and still located appropriately. If required a fresh poster is to be printed and posted accordingly. (Hint: the Data Steward should consider creating an electronic reminder task/appointment.)

If any changes are proposed it must be drafted and reviewed/approved by the Data Governance Board. Upon approval all old posters must be removed and replaced with the new poster.
Ministry of Health (eHealth) Software Conformance Standards

Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: Applicable to health data where the data is collected or disclosed using provincial eHealth technical solutions

Purpose:

The Ministry of Health publishes Software Conformance Standards to support the development, implementation, and management of the eHealth information management systems (e.g. Panorama, eViewer, Provincial Lab Information System, Provincial Diagnostic Imaging system, etc.). Volume 7 specifies the standards for Privacy and Volume 8 is for Security.

Policy

The Nation organizations that access provincial eHealth systems must be compliant with all standards that are set by the partners who provide or support these systems. If our Nation cannot meet a standard the Executive Data Steward must work to understand the barrier and work with the partner to determine the best course of action. The net result is that data governance and privacy and security must not be a barrier to empowering and qualifying our Nation health care employees to accessing the same provincial or regional health care tools/systems that are provided to our health care partners (e.g. regional Health Authorities, First Nations Health Authority, Ministry of Health, BC Center for Disease Control, Cancer Agency, etc.).

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Data Steward</td>
<td>Work collaboratively with our health care partners to support our Nation health care team to access provincial or regional tools/systems that are necessary for our Nation to access for the purpose of delivering health care services to our Members and customers. Co-approve the Conformance Standard Report(s) on behalf of the Nation; and follow-up on action plans as required.</td>
</tr>
<tr>
<td>Nation Manager</td>
<td>Identify requirements to the Data Steward. As outlined in the procedures below co-approve the Conformance Standard</td>
</tr>
</tbody>
</table>
Data Stewards
Identify and analyze requirements. As outlined in the procedures analyze and complete the Conformance Standard report and facilitate Data Governance Board review cycle; update the Data Governance Board action plan, and support the Executive Data Steward and Nation Manager on following up with the action plans. Schedule and reinitiate compliancy reviews; update the report in accordance to new versions of the standards published by the Ministry of Health.

Data Steward Subject Leads
Support the Data Steward in identifying, analyzing, and meeting the requirements.

Data Custodian
Support the Data Steward in identifying, analyzing, and meeting the requirements.

**Procedure**

The following procedure, leverages work developed under the First Nations Panorama Implementation Project, which transform the Standards into template that supports doing a compliancy review and provide a report to the Ministry of Health. Please check with FNPIP to confirm that there have been no changes in the process or template before proceeding.

The Data Steward initiates by:

1. Obtaining a copy of the FN PIP eHealth Conformance Standard template from the FNPIP team and rename it to a document title suitable for our organization and set it to version 0.

   Making a copy of version 0 and set it to version 1.

2. Reviewing each line item in the document and specify our status (e.g. compliant, partially compliant, non-compliant) and provide an understanding of the status that will support the ministry completing the review. Note, for this initial version there is no need to change the description if the status is the same as the template (notwithstanding perhaps reference to policy numbers if they differ from the FNPIP template).
For each line item that has a status of ‘partially compliant’ or ‘non-compliant’ provide a mitigation strategy and target completion date. Record these items in the Data Governance Action Plan.

Review the document with the applicable Nation Manager, Data Custodian, and any other applicable Staff that will be actively participating in the review/approval cycle. Make amendments during this review and gain consensus to set it to be ‘ready for submission to the Ministry of Health’.

Present the document to the Data Governance Board for review/approval.

3. If the Executive Data Steward and Nation Manager agree with the report they are to sign the document; if not they are to provide direction/guidance to the Data Steward who follows-up to complete the analysis until such time that signatures can be obtained.

4. Data Steward sends the document to the Health Director, Health Information Privacy, Security, and Legislation Office, Ministry of Health. The ministry will review and provide feedback if there are any concerns/questions. If there is no feedback they will approve acceptance of the report.

5. If there are action plans that need to be followed up the Data Steward must resubmit an updated signed report to the ministry every 6 months.
   a. To do so make a copy of the previous version and update the version number, update the report as per step 2 above, present the new report to the Data Governance Board and obtain signatures as outlined in step 3 above. Then resubmit to the Ministry as per step 4.

If the report is indicating full compliance the report must be reviewed annually as per step 5a.
Data Storage Assets

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards

**Purpose:**

We must have a current understanding of the locations and devices where data is stored and/or transported to ensure we manage these assets and protect them from harm. Data storage could be a building and filing cabinet, technical device such as a computer, server, cell phone, camera, etc., network devices, etc. This policy describes the methods that will be used to track the Data Storage Assets.

**Policy**

A Data Storage Asset is anything that supports the storage, generation, transmission, or reproduction of Nation data.

For data stored internally each Nation Manager is responsible for identifying the data asset to the Data Steward. The Data Steward will then use the Data Asset Inventory Log for referencing this detail.

The Nation Manager is responsible for:

- Ensuring the Data Storage Asset meets the needs of their department and working collaboratively with other members of the Nation to achieve these needs
- Where applicable collaboratively work on proposals for maintenance and replacement
- Maintaining a Business Continuity Plan (BCP)
- Applying the Data Governance Framework and ensuring data storage assets are protecting data from harm (i.e. inappropriate access, theft, corruption, etc.)
- Where possible in advance alert the Data Steward when changes occur; where advance notice cannot be provided the alert must be provided immediately following a change. A change can be in the form of something new, replaced, or retired.

Each Data Storage Asset:
• Must be provisioned by the Nation (i.e. no personal devices, such as cell phones, home faxes or home computers, can be utilized to transmit Nation data)
• Must be stored in a secure and/or supervised area at all times
• Must be password protected, where applicable (e.g. cell phones, laptops, desktops)
• Must have all photos, videos and other media transferred to a permanent storage location and subsequently deleted from the device (e.g. cell phone, camera) within 1-2 business days, whenever possible
• Must not be loaned to a non-staff member
• If lost or stolen must be reported verbally (i.e. not using voice mail) and in writing immediately to the Nation Manager or delegate; or if the Manager or delegate is not reachable it must be reported to a Nation Staff member who will take responsibility for following up on the matter (e.g. Data Custodian or Data Steward)
• Must be disposed of in accordance with the Privacy and Security Retention and Disposal Policies
• Must be considered within business continuity plans
• Where applicable must be backed up on a daily basis unless otherwise authorized by the Nation Manager.

For Nation data stored externally the Data Governance and Information Sharing Agreement between our Nation and the other Party must define the equivalent data storage specifications.

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Data Steward</td>
<td>Reviewing the Data Asset Inventory Log, identifying issues, and providing awareness and guidance to all Staff.</td>
</tr>
<tr>
<td>Nation Managers</td>
<td>Refer to this policy.</td>
</tr>
<tr>
<td>Data Custodian</td>
<td>Support the activity of maintaining the Data Asset Inventory Log and protection of the data; identify risks and risk mitigating recommendations to the Nation Manager and/or Data Governance Board.</td>
</tr>
</tbody>
</table>

Procedures

Each Nation Manager informs the Data Steward of changes to data assets (see above).

Each Data Steward creates/updates records in the Data Asset Inventory Log.
The Executive Data Steward/Chair includes an annual agenda item that requires the Data Governance Board to review the Data Flows and Data Asset Inventory Log. The Board reviews these logs to look for any gaps and issues and resolves these accordingly.

The Data Custodian uses the log to validate that all Data Storage Assets are accounted for and that they are being protected and monitored in accordance to the policies/procedures defined. The Data Custodian also provides guidance and recommendations to the Nation Managers and Data Governance Board as required.

The Data Asset Inventory Log must include the following data storage characteristics, such as:

- Name of Data Storage Asset
- Special characteristics/description
- Date acquired
- Anticipated use life
- Where applicable back-up arrangements and a verification indicator that identifies the arrangement either do or don’t align to the requirements as specified in the Data Asset Inventory Log
- Data sector (i.e. Corporate, Cultural, Human Related, and/or Lands and Resources) and data description
- Name of the Nation Manager accountable for the Data Storage Asset item and other Nation Managers or other parties accountable
Storage of Critical Data

Applicable To: All types of data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards

Purpose:
If a disaster or scenario occurs that causes our Nation to lose certain data it may cause a significant impact for our Nation’s ability to continue to provide programs/services, continue their business enterprises, and/or it may have a direct impact to the health and wellness of a Nation Member or customer. Consequently it is important that the data be identified and subsequently protected by making a backup copy of the mission critical data and storing the backup in a different physical location. This policy supports establishes the best practice for storing the data.

Policy
Any data that is identified on the Data Asset Inventory Log as ‘mission critical’ must be stored electronically. This includes data stored/managed internally or externally.

The electronic data storage methods may include storing the data on servers, memory sticks, and disk drives, etc. It cannot include storing data using fax machines, cell phones, or email. It may include storing the data in a database, personal computer tools such as Microsoft Excel, MS Word, etc., or scanned PDF documents, etc.

All electronic data storage methods must be backed-up automatically based on the requirements defined by the Nation Manager and noted on the Data Asset Inventory Log.

All backups must be stored in a separate physical location from the original physical location.

All backups must be recoverable. Backup recovery must be tested on an annual basis.

All backup procedures must be documented in a system management manual.
## Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation Managers</td>
<td>Ensuring all mission-critical data is stored electronically.</td>
</tr>
<tr>
<td>Data Custodian</td>
<td>• Supporting Nation Managers in storing mission critical data electronically.</td>
</tr>
<tr>
<td></td>
<td>• Managing, including testing, data backups</td>
</tr>
<tr>
<td></td>
<td>• Document backup procedures, including backup testing</td>
</tr>
</tbody>
</table>
Data Lifecycle and Disposal

Applicable To: All types of data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards

Purpose:

Data has a lifecycle whereby it has no value to our Nation, our partners, and/or our Nation Members or customers. It is important that we understand when it no longer has value and can be securely destroyed. This policy provides the specifications for the data retention requirements and the data disposal procedures.

Policy

Each data asset must be identified in the Data Asset Inventory Log.

Data retention requirements for Corporate Data:
• [to be determined during Demonstration Site implementation]

Data retention requirements for Cultural Data:
• [to be determined during Demonstration Site implementation]

Data retention requirements for Lands and Resources Data:
• [to be determined during Demonstration Site implementation]

Data retention requirements for Human Related Data:
• All data must be retained when a breach investigation is occurring and/or a court case exists.
• Data associated with a client must be retained for seven (7) years.
• Data associated with employees that is stored and/or managed by our organization must be retained for seven (7) years
• Access audit reviews must be retained for seven (7) years
• [Additional specifications to be determined during Demonstration Site implementation]
Data will be disposed of by processing the Disposal Request, Approval, and Tracking form (see Appendix). The applicable Nation Manager and Executive Data Steward must approve disposal of any type of data. Where the Executive Data Steward and Nation Manager are a single person a Data Steward must approve the disposal.

Data must be destroyed in such a way that it cannot be retrieved or reconstructed (e.g. paper records must be shredded, burned or pulped; magnetic media should be erased or physically destroyed in a safe and secure manner). Any records that need to be transferred in order to destroy them must be transferred using a secure and confidential process. A contract must be in place if another party performs the destruction. The contract must be in place before data is given to the contractor.

The data retention schedule and destruction process must be defined in the Data Governance and Information Sharing Agreement when data is stored/managed externally.

Human Related data: A copy (printed or image) of a Nation Member or customer’s data must be stored in the individuals chart and the above retention/disposal policy applies. In the circumstances where a copy does not warrant being placed in the chart it must be destroyed by placing it in a temporary secure holding location and subsequently be shredded and removed using the confidential removal procedure.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation Managers</td>
<td>Defining retention schedule requirements; approving data destruction requests; overseeing destruction procedures.</td>
</tr>
<tr>
<td>Executive Data Steward</td>
<td>Approving data destruction requests.</td>
</tr>
<tr>
<td>Data Steward</td>
<td>Approving data destruction requests if a single individual holds the role of the Nation Manager and Executive Data Steward.</td>
</tr>
</tbody>
</table>

## Consent Notification

<table>
<thead>
<tr>
<th>Applicable To:</th>
<th>All types of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Date:</td>
<td>[mmm/dd/yyyy]</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Nation Leadership</td>
</tr>
<tr>
<td>Any Related factors:</td>
<td>This policy aligns with the Ministry of Health Software Conformance Standards</td>
</tr>
</tbody>
</table>

### Purpose:

Under BC legislation individuals and their guardians must be notified of the legislative authority that governs the collection, use, and disclosure of their Human Related data and the purpose for which the Human Related data is being collected, used, and disclosed.

When delivering human and social services (e.g. health care, social services, etc.) the consent for collection, use, and disclosure of the data for BC operates primarily on an “implied consent” model. This means that those individuals who form part of a patient’s “circle of care” (e.g. specialists, referring physicians, lab technologists) can access, use, disclose, and retain patient information for the purposes of ongoing care and treatment.”

When Staff provide their Human Related data it is to support employment with our Nation and the “implied consent” model is also utilized. For example, a Staff member provides their data as part of requesting employment. It is implied that we have consent to collect and use the data for the purpose of employment; and if employed it is implied that we can continue use the data for the original purpose it was collected and it is implied that we can disclose the data where applicable to support their employment.

Implied consent must be informed. This policy provides direction on how our organization informs our clients on how we manage privacy of their Human Related data.

---

[3] BC College of Physicians Privacy Toolkit
Policy

Implied consent will be used when we are collecting, using, and disclosing identifiable Human Related data for employment purposes, or with those individuals who form part of the “circle of care” in context of receiving and delivering Nation services; or when we are legally required to do so (e.g. the legal requirement to disclose identifiable personal information relating to the public health program such as reporting reportable communicable diseases, processing employment data, etc.).

Expressed consent will be obtained when we are collecting, using, and disclosing identifiable Human Related Data outside of the “circle of care”, or for other purposes other than the purposes for which we originally collected the data (e.g. research). Consent may be received from the individual in verbally or written form. If consent is received verbally it must be recorded (i.e. data received, name of individual or guardian, if guardian provided consent include the name of the person that we are referencing, name of person who received the consent, and a description of the applicable data, and any other specifications).

Nation Members, customers, and staff must be informed about our consent model. This will be done using the following methods:

- The ‘Caring for Your Information’ poster must be posted within the locations where Human Related data is collected and the Nation Members, customers, and staff reside (e.g. reception areas, staff meeting and lunch rooms, Human Resource Manager office, doctors/nurse/social workers offices, etc.); refer to the Appendix for the poster.
- Where an individual receives services outside of our facilities (e.g. nursing care in their hospital, employment fair, etc.) the Nation staff must provide a pamphlet that supports the same outcome as the ‘Caring for Your Information’ poster. The poster is to be brought to the attention of the individual/guardian who has the option of reading it and it may be left with them if they want to retain a copy. Refer to the Appendix for the pamphlet.
- When Human Related data is collected/used over the phone a telephone script that results in the same outcome as the ‘Caring for Your Information’ must be spoken to replace the poster/pamphlet. The telephone script must ensure the Member/Customer/Guardian explicitly acknowledges that they have been informed about the purpose for the collection, use and disclosure of their data. Refer to the Appendix for the telephone script.
- The poster, pamphlet and telephone script must:
  i. Alert individuals, including guardians, of primary legislation that permits the collection, use, and disclosure/sharing of their Human Related data for the various purposes.
  ii. Must make an individual/guardian aware they have the right to expressly withhold or withdraw consent at any time

Mustimuhw Information Solutions Inc.
Data Governance Framework – Data Governance Policy Manual
iii. Must encourage any individual to submit privacy breach notifications to our Data Governance Board or the Office of the Information Privacy Commissioner

iv. Provide the contact details of the applicable Privacy Officer (i.e. Data Steward)

If an individual withholds or withdraws consent our Staff must verbally advise the individual of any/all known impacts. Our Staff must record in writing these events and store them in the individual's chart.

The Data Steward provides Privacy Officer services so that an individual may make inquiries and/or report a privacy concern that is associated to our Nation or another Party. The Data Steward will facilitate and support the individual to the best of their abilities. For further details refer to the Data Governance Framework – Privacy and Security Policy ‘Privacy Breach Notification and Investigation’.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Data Steward</td>
<td>Approve posters, pamphlets, and telephone scripts.</td>
</tr>
<tr>
<td>Data Stewards</td>
<td>Develop and post approved posters, provide approved pamphlets and telephone scripts to Nation Managers; and act in the capacity of a Privacy Officer.</td>
</tr>
<tr>
<td>Nation Managers</td>
<td>Ensure Staff use the pamphlets and telephone scripts.</td>
</tr>
<tr>
<td>All Staff</td>
<td>Record events where an individual withholds/withdraws consent.</td>
</tr>
</tbody>
</table>

**Procedures**

1. In consultation with Nation Manager or delegate the Data Steward uses the appendices to create the poster, pamphlet, and telephone scripts for each operational area.
2. Data Steward provide the final drafts to the Data Governance Board.
3. Data Governance Board reviews/approves. If approval cannot be obtained guidance must be provided to Data Steward who then amends material and resubmits for review/approval.
4. Data Steward posts approved posters and provides approved pamphlets and telephone scripts to the Nation Manager.
5. Nation Manager implements the use of the pamphlets and telephone scripts.
6. On an annual basis the Data Steward verifies that the posters and pamphlets are in good condition, in suitable locations. If required print a fresh poster and/or consider relocating the poster; and confirm printed pamphlets are available for staff and clients.
Business Continuity Plan

Applicable To: All types of data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards

Purpose:

Our Nation provides vital services to our Nation Members and other customers that collectively and individually affect the health and wellness of our Nation. Therefore it is important to assess and plan for situations that may result in loss of data assets and/or the disruption of access. The purpose of this policy is to outline the mechanism that will be used to assess and plan for these losses.

Policy

The Nation Manager and applicable Data Steward is required to develop a Business Continuity Plan (BCP) that considers maintaining operations if there was a partial or full loss of data for a short, medium, and long-term period. This includes considering data that is stored/managed internally and externally. Refer to the Business Continuity Plan Form in the Appendix.

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation Manager</td>
<td>Developing and maintaining the Business Continuity Plan</td>
</tr>
<tr>
<td>Data Stewards</td>
<td>Supporting the Nation Managers but not developing the plan.</td>
</tr>
<tr>
<td>Data Governance Board</td>
<td>Review BCPs, provide guidance, identify action items, monitor action items, report risks.</td>
</tr>
</tbody>
</table>

Procedures

The Data Steward and Nation Manager present the BCP to the Data Governance Board and seek support and guidance.

The Data Governance Board is required to identify action plans to support the plan.
The BCP must include a communications plan for ensuring other departments or other Party’s that need to support the plan (e.g. planning of our facilities and facility infrastructure including areas such as hydro, water, heat, networks, staff, etc.).

If the data is stored/managed externally the specifications of the BCP must be incorporated in a Service Agreement or Data Governance and Information Sharing Agreement.

The Nation Manager and Data Steward must review the BCP every three (3) years. Any changes must be presented to the Data Governance Board. The Data Governance Board provides support and guidance and identifies any new action plans.
Request to Access Human Related Information

Applicable To: Human Related Data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

A Nation Member, customer, or Staff member may want to make an inquiry about the Human Related that is under the Stewardship of our Nation. This policy outlines who is accountable for developing and managing the procedures; and key components that must be included in the procedures.

Policy

An individual is entitled to make inquiries regarding privacy and/or request access to their data that is stored by our organization to:

• Ensure it is accurate and complete
• To understand how their information has been used
• To identify the names and organizations to which we disclosed their data

Such a request must be made in writing using the ‘Request for Access to Human Related Personal Information’ form (refer to the applicable Appendix). The person submitting the form is referred to as the ‘Submitter’.

The request must be fulfilled within 30 days. In the situation where 30 days cannot be achieved the requestor must be informed within 10 days from the original request; and the requestor must be informed as to when the information will be provided.

The request must be date stamped with the date it was received. The form must be forwarded within 24 hours to the Executive Data Steward and applicable Data Steward. If the incumbent is away for more than 3 business days the person on shift that is acting in this person’s behalf must receive the request within 5 business days.

The Executive Data Steward or delegate is responsible for ensuring the requests are processed and the information disseminated is compliant with our privacy and security policies, legislation,
and partnering with our health care partners where the information is contained within a partnering health information management system.

The response may be a copy of the information or, in the case where copies cannot be made; arrangements must be made for the individual to review the original records.

All responses must inform the individual on how to submit a Privacy Breach Notification.

Our Nation may charge a reasonable fee for such access. Where a fee is charged, a written estimate must be provided to the Submitter, which may request that a deposit for all or part of the fee be paid before the service is provided.

There are some exceptions in which personal information may not or must not be released to the Submitter. For example, data that is protected by client-solicitor privilege or that would reveal confidential business proprietary data must not required to be disclosed. Additionally, data must not be disclosed in certain situations where doing so may result in harm to an individual or someone else, or if the data is about someone else. If access is refused, we must explain to the Submitter the reasons why.

The Submitter may request a review of a response that he or she is not satisfied with within 30 working days after receiving the response.

General requests for general information may be asked / answered by any Nation Staff member providing the staff have received Data Governance Awareness training. The information conveyed must be general in nature. Specific detailed questions must be forwarded vis-à-vis the above mentioned form.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Data Steward</td>
<td>Receiving and fulfilling requests for information.</td>
</tr>
<tr>
<td>Human Related Data Steward</td>
<td>Receiving requests and supporting the Executive Data Steward in fulfilling the request.</td>
</tr>
<tr>
<td>Staff</td>
<td>Supporting individuals in making a request for information, forwarding requests to the Executive Data Steward and Data Steward, processing general requests as described in this policy, and supporting the Executive Data Steward in fulfilling the request.</td>
</tr>
</tbody>
</table>

**Procedures**

Data Governance Framework – Data Governance Policy
Procedure

The following procedures are described in three parts.

- Part one (1) describes the procedures associated with assisting an individual (i.e. client or staff member) in completing/submitting a request and initiating Part Two.
- Part two (2) is processing the request and relaying the details to the requestor.
- Part Three (3) is processing a request to correct personal information if requested to do so.

Part 1: Completing and submitting a request

1.1. A individual that is requesting access to their data must complete the form titled: Request for Release of Human Related Personal Information. This individual is referred to as the Requestor.

1.2. The request must be signed and the identity of the person verified by a member of our staff or a signed witness.

1.3. An original must be provided and retained in our records. The form cannot be emailed or faxed unless the individual is known by an Nation Staff member who can validate that the document is suitable to be received via email or fax. When the form is emailed or faxed it must be printed and a signed by the Nation Staff member who approved acceptance by fax/email.

1.4. The form is then reviewed for completeness. All mandatory information as specified on the form must be provided. If it is not provided the form is returned to the Requestor requesting the form to be completed. All optional information must be able to be deciphered by our Nation otherwise it will be considered incomplete and in this scenario dialogue must occur between our Nation and the Requestor to assist in obtaining clarification. At the point of having a clear understanding of the request the form will then be considered to be complete and submitted. This process must happen in an efficient timeframe and communications with the Requestor must be charted to demonstrate that every effort was made to support the Requestor. If the Requestor is unable to complete the request the form is marked incomplete and filed in a folder dedicated to this work and stored in a secure location.

1.5. A completed/submitted request must be processed within 30 days (refer to policy). Therefore when the request is received the original request form must be immediately date/time stamped and the name of the receiver must be recorded. This original must be immediately copied and the original filed in a folder dedicated to this work and stored in a secure location. The copy must immediately be forwarded to the Executive Data Steward and Human Related Data Steward. Return to the original document and record the date/time the name of Role acknowledged receipt of the document and return the document to the dedicated folder.
2. Part 2: Processing the request

2.1. Upon receipt of the request the following must be determined within 1-3 business days:

2.1.1. Confirm that the individual has a right to receive the records. For example, if the Requestor is not an adult (>19 years old) or someone other than the actual individual confirm that the individual has the legal authority to receive the information. (As a reference refer to page 27-30 of the Lower Mainland Information Management (LMHIM) Release of Information (ROI) Manual developed by the Fraser Health Authority, Providence Health Care, Provincial Health Centre Authority, and Vancouver Coast Health Authority dated June 2012.) If the Requestor does not have authority then consider if they have authority under another means and for this refer to the same reference document and/or seek the guidance of our organizations legal counsel. If the requestor has no authority, construct a letter of notification and attach it to the original request and re-file the document.

2.1.2. Determine if the request can be accommodated within the 30-day time limit and if not construct a letter of notification and explanation to the Requestor. Attach a copy of this letter with the original request and re-file the request.

2.1.3. If the request is from an individual determine if the effort to complete will require a fee to be charged to the Requestor (refer to policy) and if so construct a letter of notification and request the client to submit the fee before proceeding with the request. Attach a copy of this letter with the original request and re-file the request.

2.2. Identify the information assets that need to be sourced, the staff required to assist in collating the information and the dates required for the work to be collated. Communicate with the applicable staff and record this detail to prove that due diligence is being applied to meet the 30-day timeline to complete the process. Consider records that are not necessarily located in our physical location at this time (e.g. located off site; records stored in a backup system that supports electronic information management; records store in satellite offices or on laptops used off-site; etc.).

2.3. Continue to monitor and manage the collation of the information.

2.4. As the information is collated review the materials to determine the following:

2.4.1. Should any information be severed to protect the privacy of 3rd parties (e.g. staff, other clients, family/friends, etc.). Refer to page 41-44 of the above-mentioned manual.

2.4.2. Is any of the information incomplete or out-of-date? If so continue to process the request and prepare to alert the Requestor to this fact with a goal to
providing them an understanding of what is outstanding and an expected timeline as to when they can expect us to complete the request.

2.5. Compile the information. The compilation of the records must include a photocopy of paper documents that reflects a similar context as the original (e.g. if the original record is double-sided it should be photocopied double-sided. For electronic records a logical representation of the information should be presented in a report format or alternatively screen shots.

Prepare a Record Inventory sheet that enumerates the various records and the order in which they are provided in the response package. The first record should represent a cover letter document. The second record should represent the Record Inventory document. All subsequent documents should represent the name of the document and the number of pages provided. If applicable the end of the Record Inventory sheet must provide a description of the records that are not yet included and an anticipated date that this will be available.

The Record Inventory sheet must also identify how we used the record and identify whether the record was disclosed to any other parties and if so when and why if the Requestor requested this information.

2.6. Once all records are compiled and the Record Inventory Sheet is completed a letter to the requestor must be developed and signed by Data Steward. The letter must include information on how to submit a Privacy Breach Notification. The package is then fully copied and filed with the original request; and the original package is either provided to the requestor using the method of delivery defined on the original request (e.g. mail, courier, or in-person pickup). The package cannot be emailed unless it is done by scanning the package and send by email using encryption. The package cannot be fax’ed.

If the requestor has chosen to pick up the package in-person they must be informed that we will retain the package for no more than six (6) months. If they have not picked up within three (3) business days after they indicated they would pick it up the requestor will be contacted two (2) additional times to prompt them to pick up the package. This detail must be charted and filed with the original request. If a client does not pick up the package it may be securely destroyed after six (6) months.

3. Completing a request to correct personal information
3.1. Upon receiving the package the requestor may request us to correct personal information. This request must be received in writing delivered by mail, in-person, email, or fax.

3.2. Original records cannot be changed except for demographic (factual) errors.

3.3. Incomplete or incorrect records: two options are available

   Option 1: if the correction is brief and there is relative consensus between the originator of the record and the submitter a clinical note describing the correction of information can be added to the client's record.

   Option 2: if the correction is voluminous or if the originator and submitter disagree the individual can submit documents describing or discussing the correction of personal information. This marks the original record to indicate there is a dispute and enables appending an amendment/correction to the record. A correlation between the submitted document and the original record is required. This can be done in various ways depending on how the record is stored (i.e. paper or electronic). The submitted document becomes part of the permanent record and is available for future releases of information.

3.4. The submitted document must be forwarded to any parties that we disclosed the original information to in the past 12 months prior to when the correction was processed.

A requestor may contact the Office of the Information and Privacy Commission to review any aspect of our request. The contact information is:

Office of the Information and Privacy Commissioner
P.O. Box 9038
Stn. Prov. Govt.
Victoria, BC V8W 9A4
Phone: 250-387-5629
Fax: 250-387-1696
Privacy Breach Awareness

Applicable To: Human Related Data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

Our Nations’ Data Governance Framework and related policies are in place to ensure our organization has a privacy culture that demonstrates our commitment and knowledge on the best practices for protecting data, auditing these practices, and following up on any reported concerns which may or may not prove to be a privacy breach. This policy focuses on raising awareness and demonstrates our commitment to improving our privacy culture and following up on issues.

Policy

Nation Members, customers, and staff must be informed on how to report a potential privacy breach. This will be done using the following methods:

• Privacy Breach Notification poster must be posted within the locations where our Nation Members, customers, and staff reside (e.g. reception areas, lunch rooms, staff offices or hallways, etc.); refer to the appendix for the poster.
• Where an individual receives services outside of our facilities (e.g. nursing care in their hospital, employment fair, etc.) the Nation staff must provide a pamphlet that supports the same outcome as the Privacy Breach Notification poster; refer to the appendix for the pamphlet.
• Where an individual receives recurring services outside of our facilities (e.g. nursing care in their home the pamphlet is to be left with the individual/guardian)
• Individuals have the option of reading the poster or pamphlet; and may retain a copy if desired
• When data is collected/used over the phone an equivalent telephone script must be spoken to replace the poster/pamphlet. Refer to the appendix for the telephone script.
• The poster, pamphlet, or telephone script may be integrated with other privacy related posters, pamphlets, or telephone scripts
• The poster, pamphlet and telephone script must:
  i. Provide information on how to report a potential privacy breach to our Nation or the B.C. Office of the Information and Privacy Commissioner
  ii. Must inform the individual/guardian that reporting will not cause any harm to themselves
  iii. Provide the contact details of the applicable Privacy Officer (i.e. Data Steward) or Executive Data Steward

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Stewards</td>
<td>Draft posters, pamphlets, and telephone scripts and obtain Data Governance approval; post and maintain the quality and content of the posters.</td>
</tr>
<tr>
<td>Nation Managers</td>
<td>Implement the use of the pamphlets and telephone scripts.</td>
</tr>
</tbody>
</table>

Procedures

1. The Data Steward drafts the poster, pamphlet, or telephone script and reviews with the Nation Manager.
2. The Data Steward presents the poster, pamphlet, or telephone script to the Data Governance Board.
3. The Data Governance Board reviews and approves. If approval cannot be met the board must provide guidance. The Data Steward then updates accordingly and resubmits until approval is met.
4. Once approved the Data Steward posts the posters and distributes the pamphlet and telephone scripts to the Nation Manager.
5. The Nation Manager is responsible for implementing the use of the pamphlet and telephone scripts.
6. Annually the Data Steward reviews the poster; updates if required and seeks re-approval; and upon approval reposts accordingly. If no updates are required the Data Steward reprints/reposts if the condition of the poster that is currently posted requires a fresh copy to be posted.
**Privacy Breach Notification**

**Applicable To:** Human Related Data  
**Approval Date:** [mmm/dd/yyyy]  
**Approved By:** Nation Leadership  
**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

**Purpose:**
An individual (e.g. Nation Member, customer, guardian, Staff, member of the public, member of a Partner, privacy commissioner, etc.) or a group representing or advocating on behalf of an individual may have a privacy issue (e.g. risk, concern, complaint, incident(s) of actual or suspected unauthorized access, misuse of Human Related data, inappropriate disclosure, etc.) that needs to be reported and followed up. The item may be perceived or actual; it may pertain to himself or herself or another Party; and it may involve our Nation or another organization. It is important that our Nation supports the reporting of privacy issues. This policy provides the framework for a person/group to submit a privacy issue.

**Policy**
Every privacy issue, hereafter referred to as a ‘Privacy Breach Notification’ are to be reported to one of the 5 Data Stewards. The Data Steward is responsible for recording the issue on the Privacy Breach Notification report within three (3) business days. Once logged the Data Steward immediately notifies the Executive Data Steward and the two parties initiate the Privacy Breach Investigation described in the Data Governance Framework – Privacy and Security Policy ‘Privacy Breach Investigation’.

All Privacy Breach Notifications must be numbered sequentially, stamped with the date received, and recorded in the Privacy Breach Notification Log.

The Privacy Breach Notification Log must be stored electronically in a secure location that is only accessible to the Data Governance Board and any approved support Staff members.

If the Privacy Breach involves one or more of the Data Stewards the Privacy Breach Notification Log cannot be updated. Instead the receiver of the notification must retain the notification report in a secure location and report in writing to the Nation Leader. In this
circumstance the Nation Leader takes the lead in conducting an investigation (refer to the Data Governance Framework – Privacy and Security Policy ‘Privacy Breach Investigation’).

A Privacy Breach Notification may be an item reported by a person, an organization, or a result of conducting an audit. A privacy breach may also be linked to a privacy breach that is associated with an item reported to another Party. For example, if a person reports privacy breach to one of our Partners who in turn contact us as part of their investigation. This contact must be recorded as a Privacy Breach Notification.

Staff are informed to report Privacy Breaches vis-à-vis the following:
• Staff Data Governance Awareness Training
• Privacy Confidentiality and Acceptable Use Acknowledgement form that is signed by Staff at the start of their employment and updated annually
• Privacy Breach Poster that is posted in the staff common areas

Nation Members and customers are informed to report Privacy Breaches vis-a-vis the Consent Notification poster, pamphlet, or telephone script; or the Request for Information form and response letter.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Stewards</td>
<td>Receiving and maintaining the Privacy Breach Notification Log.</td>
</tr>
<tr>
<td>Executive Data Steward</td>
<td>Initiate Privacy Breach Investigation immediately.</td>
</tr>
<tr>
<td>Nation Leader</td>
<td>Receive Privacy Breach Notifications where they involve the Data Stewards and initiative the investigation immediately.</td>
</tr>
</tbody>
</table>
Privacy Breach Investigation

Applicable To: Human Related Data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

It is essential that our Nation review and investigate all privacy breach notifications in an objective manner so that we may respond positively and supportively to the person/group who notified us of a potential privacy breach. Furthermore our Nation must show evidence that each privacy breach notification has been investigated fairly and a conclusion has been determined. If the outcome of an investigation results in privacy being compromised our Nation must have a plan to notify the parties affected and have an action plan that remedies the issue.

Policy

A Privacy Advocacy poster (refer to applicable Appendix) must be displayed wherever Nation Members, Customers, and Staff congregate and Nation Data is collected. The poster must include the following key messages:

• Nation commitment, accuracy, and empowerment
• Individual rights to access information, ensure it is accurate and support an individual on understanding who their data has been disclosed to
• How individuals make requests for corrections to their data
• How to report suspected or actual privacy breaches

If a Privacy Breach Notification involves data managed/stored internally the notification document must be forwarded to the applicable Nation Manager(s) unless it is speculated that the Nation Manager(s) is involved in which case it must be forwarded to an applicable Nation Leader who is not likely involved.

If a Privacy Breach involves data that is managed/stored by another Party the notification document must be forwarded to the other Party as per agreements that govern the data.
Each Privacy Breach Notification initiated by our organization must have an investigation initiated within 2 business days. All investigation details will be recorded in the Privacy Breach Investigation Report. All evidence will be securely protected using industry best practices.

Investigations involving data that is managed by our organization will be led and managed by the Executive Data Steward; or if it is possible the Executive Data Steward is involved it must be led by a Nation Leader who is not likely involved or a hired 3rd party contractor. Additional support resources from our Partners and/or the Office of the Information and Privacy Commissioner may be obtained.

Each investigation will remain confidential and deemed highly sensitive information. An investigation is considered a ‘potential’ breach until such time that the investigation is complete. At a minimum each investigation must include:

- Immediate containment of the breach/violation
- Breach Awareness Notification(s)
- Contacting other departments or individuals within our organization or other organizations to assist in managing the breach
- Investigating and documenting the details, including the cause and extent
- Identifying impacts to other organizations
- Determining if a breach occurred and if so making reprimanding recommendations; identifying risks and plans to mitigate the breach in the future; and communicating the results and action plans to the applicable leaders of our organization.

Any individuals affected must be notified. This type of notification is referred to as a ‘Breach Awareness Notification’ and is required as soon as possible after the breach, and no later than three (3) business days after the breach was reported (i.e. the full investigation is not required to be completed). The Breach Awareness Notification may be delayed in order to not impede a criminal investigation if deemed necessary after contract from law enforcement authorities. The Breach Awareness Notification must be documented to ensure the appropriate information is conveyed completely and accurately. It may be made in person, by phone, or in writing.

Investigations involving data that is managed/stored by another Party will be led by the given other Party in accordance to the agreement that governs the data.

The Executive Data Steward or Nation Leader is responsible for writing the final report that reflects our Nations position on the given Privacy Breach Notification and completing any of the necessary Investigation steps identified above.

All Nation Staff are required to cooperate with anyone involved in the investigation and support the outcomes of an investigation.
During an investigation the Investigation Lead will be responsible for determining the communication(s) that will occur during the investigation. This person will also be responsible to follow-up on the outcomes of the Breach Investigation.

Failure to comply with the privacy and security policies / procedures may lead to termination of access, termination of employment, termination of contract, withdrawal of privileges, and/or be subject to applicable laws and the applicable Acceptable Use and Confidentiality agreement. A privacy breach may also result in notifying the relevant professional organization a staff/contractor may be associated with which may result in professional sanctions invoked by the given professional organization in accordance to their policies/procedures.

Approval to dispose of any evidence is made on a case by case basis and at a minimum requires the approval of the Lead Investigator and Executive Data Steward. If a single person holds these roles the Lead Investigator and Nation Leader must approve instead. In the case where external Parties are also involved in the investigation it would also require approval by the given external organizations.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Investigator (i.e. Executive Data Steward or Nation Leader)</td>
<td>Lead privacy breach investigations, engage other Parties as required, facilitator-informing individuals as described herein, approve disposition of investigation notifications and reports according to this policy; participate in investigations led by other Parties.</td>
</tr>
<tr>
<td>Data Stewards</td>
<td>Support the Lead Investigator</td>
</tr>
</tbody>
</table>

**Procedures**

The following workflow diagram is an example of how to process a privacy breach investigation.
When a Privacy Breach Notification is received the breach must be confirmed, contained, responded to and investigated. The following procedures support these activities while also assisting the Lead Investigator in determining if the breach is contained within the Nation, when and how to notify individuals and other Parties of the breach and when to collaborate with partner organizations that may be impacted by the breach.

1. **Receive Notification of Possible Breach**
   Refer to the Data Governance Framework – Privacy and Security Policy ‘Privacy Breach Notification’.

2. **Confirm Breach**
   When the Privacy Breach Notification is received the Lead Investigator may engage the Data Custodian and Nation Manager to confirm the breach. This may include some high-level investigative actions to verify the accuracy of the breach details such as:
   - Reviewing access logs (both to systems and facilities)
   - Talking with Staff members, Nation Members, or customers
   - Reviewing audit logs
   - Reviewing documentation/media

   This work needs to be done immediately and with precision however it must also be done quickly.

3. **Contain Breach**
   Once the breach has been confirmed, immediate action must be taken to contain the breach e.g.:
   - Halting unauthorized practices
   - Changing computer/facility access codes or keys
   - Recovering records
   - Ensuring no copies of data have been made or retained by the individual(s) involved in the privacy breach
   - If the data/material has been securely destroyed rather than retrieved, obtain confirmation in writing from the party responsible for the secure destruction of the data/material

4. **Conduct Preliminary Assessment**
   Once the breach has been contained, preliminary assessment activities can occur to determine the extent of the breach, impacted individuals, potential risk factors and internal communication about the breach. Preliminary assessment activities are added to and expanded throughout the breach investigation.

   a. **Designate a Breach Response Team**: Investigation Lead selects and designates a Breach Response Team and assigns a Lead:
• Appoint an individual to conduct the initial investigation and make recommendations for follow-up
• Determine if a Breach Response Team should be assembled with representatives from appropriate business areas (if the breach is determined to impact other organizations, the Breach Response Team consists of representatives from some/all Parties/Organizations)
• The Breach Response Team must include a minimum of three (3) people whereby no more than two (2) members are Data Governance Board Members

b. **Internal Notification:** Breach Response Team determines who, internally, should be aware of the incident. Internal notification should not include identifiable personal information about the person(s) under investigation or the individual(s) impacted by the breach.

c. **Report Criminal Activity:** If the breach involves theft or other criminal activity, the police must be contacted and will provide guidance for breach investigation and communication.

d. **Preserve Evidence:** When conducting preliminary analysis of risks and cause of breach, make sure the evidence is preserved appropriately. Do not destroy evidence that may be valuable in determining the cause of the breach or support you in taking corrective actions.

e. **Analyze and Document Breach Information:** The Breach Response Team analyzes and investigates breach information.

Notifications and all other activities associated to the breach investigation must be documented. See the **Privacy Breach Template** for an example.

**Follow the guidelines below when conducting the preliminary investigation:**

i. Consider what information has been breached
   • Consider the sensitivity of the information (e.g. health information, financial account numbers, government issued identification etc.)
   • Determine if the information can be used for fraudulent or harmful purposes

ii. Analyze the cause and extent of the breach
   • Cause of the breach
   • Risk of ongoing or further exposure of the information
   • Extent of unauthorized collection, use or disclose, including number of likely recipients and risk of further access, use or disclosure, including in mass media or online
   • Determine if information was stolen and, if so, if it was the target of theft
   • Is the information encrypted or protected
   • Has the information been recovered
iii. Determine individuals affected and potential harm from the breach
   • Who received the information (an accidental breach/mistake or intended breach)
   • Is there a relationship between the unauthorized recipients and the data subject?
   • Identify potential harm to the individuals that may result from the breach
     • Security risk
     • Identity theft/fraud
     • Loss of business/employment
     • Hurt, humiliation, damage to reputation or relationships

iv. Identify potential harm to the organization as a result of the breach
   • Loss of trust in public body or organization
   • Loss of assets
   • Financial exposure
   • Loss of contracts/business

v. Identify potential harm to the public as a result of the breach
   • Risk to public health
   • Risk to public safety

5. Breach Contained Within the Nation?
   It is imperative to determine if the breach is contained within the Nation or if it impacts other Nations/Parties/customers. The impact to others may result from the person(s) under investigation being employed by/affiliated with another Nation or organization or from the breach occurring through the use of an computer-based system used by ourselves and our Partners.

   a. Is the unauthorized recipient(s) of information employed by the Nation?
   b. Is the unauthorized recipient of information on contract with the Nation and/or work for any other organizations? (If yes, breach is not contained within the Nation)
   c. Are any other organizations impacted by the breach? (If yes, breach is not contained within the Nation)

Note that if a breach is not contained within the Nation, affected Parties and/or the Office of the Information and Privacy Officer must be contacted for support. All further activities regarding the breach will be done in conjunction with and with support from these other...
Parties.

6. **Conduct Risk Assessment**
   Continue with analysis of breach and document additional investigation activities and risk assessment findings.

7. **Partner Organization Impacted?**
   Determine if the breach directly impacts Partner Organizations (e.g. Regional Health Authority (RHA), Ministry of Health, Ministry of Children and Families, etc.), and/or if the breach involves an computer-based system that is shared between our Nation and our Partners.

8. **Contact Partner Organization Privacy Officer for Breach Support**
   If the breach affects a Partner Organization, contact the Partner Organization(s) Privacy Officer for Breach Management support to collaborate on and align response activities for the breach and/or follow the arrangements set out in the support or data governance and information sharing agreements.

9. **OIPC Reportable?**
   For internally managed/stored data determine if the breach should be reported to the B.C. Office of Information Privacy Commissioner. Refer to the Checklist for Notifying the Office of the Information and Privacy Commissioner (OIPC) below:

### CHECKLIST FOR NOTIFYING THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER (OIPC)

Consider the following factors when determining if the Office of the Information and Privacy Commissioner should be notified of the breach.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>The breach involves Human Related data and it is sensitive</td>
</tr>
<tr>
<td>☐</td>
<td>There is a risk of identity theft or other harm including pain and suffering or loss of reputation</td>
</tr>
<tr>
<td>☐</td>
<td>A large number of people are affected by the breach</td>
</tr>
<tr>
<td>☐</td>
<td>The information has not been fully recovered</td>
</tr>
<tr>
<td>☐</td>
<td>The breach is the result of a systemic problem or a similar breach has</td>
</tr>
</tbody>
</table>
To report this breach to the OIPC, fax a copy of the following documents to the OIPC (250-387-1696):

i. Checklist for Notifying the Office of the OIPC
ii. FNHSO Breach Reporting Form,
iii. Breach Notification Letter(s) sent to impacted individual(s)
iv. Any additional information you determine the OIPC should be aware of.

If notification to the OIPC is required and the breach involves an eHealth system, you must also provide a copy of the report to eHealth Operations Privacy Services and Health Information Privacy, Security and Legislation (HIPSL). In addition, HIPSL has the responsibility to notify the Office of the Chief Information Officer (OCIO) of all OIPC reportable events.

10. Notify Impacted Individuals/ Communities?
Assess the need to notify individuals/communities impacted by breach. If the breach impacts partner organizations, notification assessments and messaging shall be jointly undertaken by all impacted organizations.

a. Will notification avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed?
b. Do legislation or contractual obligations require notification
c. Is there a risk of identity theft, fraud, physical harm, hurt, humiliation, damage to reputation, loss of business or employment?
d. Has law enforcement been contacted and have they requested delayed notification in order not to impede a criminal investigation?

11. Send Notification to Impacted Individuals/Communities
a. If notification is required, it should occur as soon as possible following the breach.
   • Direct notification (via phone, letter or in person) is preferred.
   • Indirect notification (via websites, posted notices and media) should only occur where direct notification could cause further harm, is cost prohibitive or contact information is lacking.
b. Notification should include the following (Refer to **Breach Notification Letter Template** for a sample):
   - Date of breach
   - Description of breach
   - Description of information inappropriately collected, used or disclosed
   - Steps taken so far to reduce or control harm
   - Future steps planned to prevent further privacy breaches
   - Steps the individual can take (e.g. how to change PHN, DL number etc.)
   - Privacy Commissioner contact information (for concerns, complaints)
   - Contact information for Nation Privacy Officer (i.e. Executive Data Steward)

c. Determine if other organizations should be contacted (note that personal information should not be shared with these entities unless required)
   - Professional or regulatory bodies
   - Technology suppliers (if breach was due to a technical failure or could be mitigated through technical fixes)

12. **Coordinate Disciplinary Action**
   Determine if disciplinary action is required regarding the person(s) under investigation for the breach
   - Deprovision user(s) from internal and/or eHealth systems (the Data Steward is responsible for initiating de-provisioning of users from all internal and eHealth systems)
   - Suspension/Termination of employment/contract
   - Removal of facility access

13. **Develop and Implement Remediation/Prevention Strategy**
   Determine actions to remediate impacts from breach and develop strategies to prevent future privacy breaches
   a. Review investigative findings and develop prevention strategies
   b. Monitor prevention strategies
# NATION BREACH REPORTING FORM

**Date of Report:**

## 1. FNHSO CONTACT INFORMATION

<table>
<thead>
<tr>
<th>FNHSO Name</th>
<th>Contact Name (Data Steward)</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------</td>
<td>-----------------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Street Address</th>
<th>City</th>
<th>Prov</th>
<th>Postal Code</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone</th>
<th>Fax</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## 2. RISK EVALUATION

### 2.1 INCIDENT DESCRIPTION

Describe the nature of the breach and its cause

<table>
<thead>
<tr>
<th>Date incident occurred</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date incident discovered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location of incident</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
### 2.2 PERSONAL INFORMATION INVOLVED

Describe the personal information involved (e.g. name, address, SIN, medical) Do NOT include identifiable personal information

### 2.3 SAFEGUARDS

Describe physical safeguards (locks, alarm systems etc.)

Describe technical safeguards

- Encryption
- Password
- Other:

Describe organizational security measures (security clearances, policies, role-based access, training programs, contractual...
## 2.4 HARM FROM THE BREACH

| Identify the type of harm that may result from the breach | ☐ Identity theft  
(most likely when the breach includes loss of SIN, credit card numbers, driver’s licence numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud)  
☐ Risk of physical harm  
(when the loss of information places any individual at risk of physical harm, stalking or harassment)  
☐ Hurt, humiliation, damage to reputation  
(associated with the loss of information such as mental health records, medical records, disciplinary records)  
☐ Loss of business or employment opportunities  
(usually as a result of damage to reputation to an individual)  
☐ Breach of contractual obligations  
(contractual provisions may require notification of third parties in the case of a data loss or privacy breach)  
☐ Future breaches due to similar technical failures  
(notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)  
☐ Failure to meet professional standards or certification standards  
(notification may be required to professional regulatory body or certification authority)  
☐ Other (specify) |

## 3. NOTIFICATION

<p>| Has your Privacy Officer | |</p>
<table>
<thead>
<tr>
<th><strong>been notified?</strong></th>
<th>☐ Yes: Who was notified and when?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>☐ No: When will your Privacy Officer be notified?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Have the police or other authorities and organizations been notified?</strong></th>
<th>☐ Yes: Who was notified and when?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>☐ No: Will they be notified and if so when?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Have affected individuals been notified</strong></th>
<th>☐ Yes: How were they notified?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How many individuals were notified?</td>
</tr>
<tr>
<td></td>
<td>When were they notified?</td>
</tr>
<tr>
<td></td>
<td>☐ No: Describe why affected individuals have not been notified</td>
</tr>
</tbody>
</table>
What information was included in the notification?

- Date of breach
- Description of breach
- Description of information inappropriately accessed, collected, used or disclosed
- Risk(s) to individual(s) caused by the breach
- Steps taken so far to control or reduce harm
- Future steps planned to prevent further privacy breaches
- Steps individuals can take to reduce the harm
- Privacy Commissioner contact information
- Organization contact information for further assistance

### 4. PREVENTION

**Describe the immediate steps taken to contain and reduce the harm of the breach** (e.g. changed locks, changed access codes, deprovisioned users)

**Describe the long-term strategies to correct the situation** (e.g. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security)
BREACH NOTIFICATION LETTER TEMPLATE

Insert into NATION Letterhead (include full name and address)

[Date]

[Client Name]
[Address Line 1]
[Address Line 2]
[City, Province, Postal Code]

Re: Personal [Health] Information of [Name of Client]

Dear [insert name]

On [date], [name of responsible organization] became aware of a breach of [your] personal health information accessed via [indicate how information was accessed]. We [have identified/estimate] the date of information breach to be [date]. OR [The duration of information exposure was (include date range and time range)]. OR [We are unable to determine the date of the breach occurrence.] We are notifying affected individuals in as timely a manner as possible. [It was necessary to delay notification because of the protected nature of the forensic investigation.] Incident investigation [is/is not] complete at this time.

The incident involving personal health information was [loss/theft/other] [state the circumstances]. [Examples: theft of a laptop containing files of 5,326 individuals from the trunk of a car OR exposure of personal health information on the (name of organization) Web site OR misplacement of five boxes, 250 paper medical records, during transit to a vendor destruction site]. The unsecured information includes [list the types of information involved: part/complete health records dated between (state date range), full name, date of birth, home address, account number, diagnosis, types of treatment information, disability code, name other information types].

[Name of responsible organization] [has/have taken OR will soon take] these steps to protect your, and others’ personal information from further harm or similar circumstances: [Choose from or customize these examples or add your own]:

• Initiated a forensics security investigation

• Filed a police report on [date]; Initiated a criminal investigation
• Sanctio\n\ned five employees/physician by suspension/termination of employment/medical staff
privileges
• Address operational or technology updates or changes triggered by the incident to improve
confidentiality, such as strengthening technology safeguards or administrative policies and/procedures
• Other
\n[Name of responsible organization] sincerely apologizes for the inconvenience and concern this
incident causes you. Your information privacy is very important to us and we will continue to
do everything we can to correct this situation and fortify our operational protections for you
and others.

You may contact us with questions and concerns in the following ways: [by calling our Privacy
Officer at (XXX) XXX-XXXX between the hours of X a.m. and X p.m., 24 hours or Monday to
Friday; sending an e-mail message to xxxx@xxxx.org; addressing a letter to our postal address].

[If deemed appropriate, you may need to include other organization/MOH Contact details with an
explanation]

You may also contact the Office of the Information and Privacy Commissioner; sending an e-mail message
to info@oipc.bc.ca; by phone 1-800-663-7867 or (250) 387-5629; or addressing a letter to the postal
address, Office of the Information and Privacy Commissioner for British Columbia, PO Box 9038, Stn.
Prov. Govt., Victoria, BC, V8W 9A4

Sincerely,
[Contact name from FNHSO]
[Contact information from FNHSO]
Access to Data

**Applicable To:** All Data

**Approval Date:** [mmm/dd/yyyy]

**Approved By:** Nation Leadership

**Any Related factors:** This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

**Purpose:**

Access to data is a primary privacy and security control that must be managed and adhered to in order to ensure data adequately protected from unauthorized access as well as loss and theft. This policy provides direction on who is accountable for the granting/revoking access and auditing access.

**Policy**

Corporate data may be accessed:

• For the purpose of displaying, printing, and/or distributing data to provide or facilitate authorized corporate activities that support our Nation

• By a professional or support Staff involved in processing corporate activities

• In accordance to the roles and responsibilities described in the individual's job description or contract; or as delegated in writing by an authorized Nation Staff member

Cultural data may be accessed:

• For the purpose of displaying, printing, and/or distributing data to provide or facilitate cultural services

• By a professional or support Staff involved in delivering cultural services

• In accordance to the roles and responsibilities described in the individual's job description or contract; or as delegated in writing by an authorized Nation Staff member

Land and Resource data may be accessed:

• For the purpose of displaying, printing, and/or distributing data to manage, support and protect our Nation land and resources

• By a professional or support Staff involved in managing our Nation land and resources

• In accordance to the roles and responsibilities described in the individual's job description or contract; or as delegated in writing by an authorized Nation Staff member
Mustimuhw Information Solutions Inc.

Data Governance Framework – Data Governance Policy Manual

Human Related data may be accessed:
• For the purpose of displaying, printing and/or distributing data to provide or facilitate Nation Member and customer services provided by our Nation (e.g. health care, social services, housing, etc.) or for the purpose of facilitating employment by our Nation
• By a professional or support Staff involved in facilitating delivery of an authorized Nation human or social (e.g. clinical care, treatment of patient, program evaluation, surveillance, or to support human and social services and programs) or Nation employment service
• In accordance to the roles and responsibilities described in the individual's job description or contract; or as delegated in writing by an authorized Nation Staff member

Authorized Nation Staff members can access data:
• If they are in a profession governed by a professional organization and has credentials in good standing with the respective organization.
• When hired has been checked to verify the accuracy and completeness of their personal data, education, professional qualifications, employment data and references.
• When hired has criminal records check where necessary at the discretion of the Human Resources Manager or Nation Manager in context of role the Staff member will be assigned
• After receiving Data Governance and Privacy Awareness training and signing the Confidentiality and Acceptable Use Acknowledgement form
• A signed declaration that there are no convictions for criminal offences for which a pardon has not been granted
• Using the privacy principle of ‘need to know and least privilege’
• The Access Request/Approval form is complete, accurate and aligns with the Staff members roles and responsibilities as described in their job description or delegated by an authorized Nation Staff member (delegation must be in written form)
• Providing they are employed by our Nation

Access to all data and related facilities or tools that access the data will be conducted as per the privacy and security policies.

Where applicable each staff member that is assigned a unique user identifier (i.e. User ID) must not share the User ID with any other person. Other approved access methods (e.g. keys, key codes, etc.) must not be shared with unauthorized Staff members or any other individual with the prior permission of the Nation Manager.

The Data Custodian is accountable for development and maintenance of the procedures associated with granting and revoking access. These procedures must be documented and reviewed/approved by the applicable Nation Manager and Data Governance Board. The Data Custodian is accountable for ensuring the procedures are implemented and being adhered to.
At a minimum the procedures must include:

- The use of standard forms to process Data Access Requests
- Acknowledgement by the Staff member or Supervisor that they have received Data Governance and Privacy training and signed the Confidentiality and Acceptable Use form
- The requestor must be the Staff member or the supervisor who is most closely responsible for the functional duties of the Staff that is needing access to the data (preferably the latter when possible)
- The Data Access requestor must be a different person from the individual who approves the request (e.g. supervisor requests access on behalf of the Staff member or the Staff member requests and the Nation Manager approves the request)
- The approver must use the principles of ‘need to know’ and ‘least privileges’ as a means for approving access
- Once approved the Access Administrator must provision access and provide the access too(s) (i.e. keys, UserIDs/passwords, etc.) to the Staff member directly; and the Staff member must sign acknowledgement that they have received the access tool(s)
- The procedures must provide an audit trail for providing access
- Access must be reviewed/re-approved every three (3) years
- Any errors or omissions reported using the Privacy Breach Notification form
- Periodic review of inactive access activity and verification the user still requires access
- Treat access for Staff (employees or contractors) and Visitors (e.g. external providers supporting Nation Staff, consultants, general visitors) equally

The Data Custodian must verify that the hiring/contracting process includes verifying the prospective Staff member’s data (i.e. personal data, education, professional qualifications, employment background and references, professional accreditation is in good standing, where applicable criminal record checks are cleared etc.) are accurate. This may be verified by showing evidence in a policy/procedure and validating with Nation Leaders that the policy/procedures are being applied; or by doing period random audits of Staff records/charts. Note: the former is preferred.

When a Staff member is terminated from their employment the Nation Manager must inform the Data Custodian immediately and the access tools must be decommissioned as follows:

- Keys returned
- Key codes updated and redistributed to authorized Staff
- UserIDs inactivated

When a Staff member changes their role and/or responsibilities a review of their Access must be conducted and revalidated. This must be documented using the standard Data Access procedures.
It is the responsibility of Nation Managers to ensure Staff maintain the conditions of employment and report any privacy risks to the Data Steward and/or Data Custodian.

For Staff who require a criminal record check to be conducted as part of their initial employment the Nation Manager must arrange for an updated criminal record check to be done every five (5) years. Any privacy concerns resulting from the criminal record check must be reported using the Privacy Breach Notification form.

Although Staff are granted access to a data set (e.g. a set of files or a computer-based system) they must only access the records as/when needed to perform their duties. This is referred to as the principle of ‘need to know’. The Data Steward and Data Custodian must develop and implement audit procedures that demonstrate our Staff are accessing records based on the ‘need to know’ principle. These procedures must be reviewed/approved by the Data Governance Board. Nation Managers and Staff must support the audit procedures. Any issues arising from the audit must be reported as a Privacy Breach Notification.

Additionally Staff are granted access only when they need access. Therefore if they are granted access but do not access the data the access requirement must be reviewed by the Nation Manager and access retained or removed accordingly. The Data Steward and Data Custodian must develop procedures to monitor inactive access activity. The Data Steward monitors inactive activity and initiates re-approval requests.

Any Staff members who have access to data at the time this policy is implemented will be cross-checked to align to this policy. The cross-checking must be documented. This activity must be completed within one(1) year of implementation of this policy. The Data Steward must initiate this work.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Data Steward    | • Co-develop and implement access audit procedures, identify issues and raise Privacy Breach Notifications as required.  
                 | • Initiate the work of cross-checking current Staff to make sure they align with this policy and the access procedures. |
| Data Custodian  | • Develop and implement Data Access Request procedures.  
                 | • Co-develop and implement access audit procedures, identify issues and raise Privacy Breach Notifications as required. |
| Nation Managers | Collaborate with the Data Steward and Data Custodian to develop and implement Data Access procedures and Data Access Audit procedures. |
Outside Canada – Storage and/or Access

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

Accessing and/or storing Human Related data outside of Canada must be done under special circumstances and in accordance to the legislative authorities. Additionally our Corporate, Cultural and Land and Resource data is considered confidential and our Nation requires the same level of consideration as Human Related data. This policy addresses storing/accessing data outside Canada.

Policy

Storing Nation data outside Canada is prohibited.

Accessing Nation data when residing outside of Canada is prohibited unless prior approval has been obtained from the Executive Data Steward.

Before approval can be provided the legislative authority to grant access must be reviewed and documented as part of authorizing access.

The Data Custodian must incorporate this policy in the Data Access Request procedures.

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Data Steward</td>
<td>Review and approve requests accordingly.</td>
</tr>
<tr>
<td>Data Custodian</td>
<td>Incorporate policy into Data Access Request procedures.</td>
</tr>
</tbody>
</table>
Remote and Wireless Access

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:
Accessing sensitive or personal information using wireless functionality is risky if the remote access functionality is not configured and designed to provide a secure and auditable environment. This policy outlines the requirements associated with enabling wireless access. It also defines who is accountable for granting/revoking access, establishing procedures, and auditing access.

Policy

Wireless networks that are used to access Nation Data must be approved by Data Governance Board and Data Custodian. The approval process must demonstrate that the network is secure. This can be done using a 3rd party assessment or using the skills of our technical staff providing they have proven skills and knowledge in assessing security risks.

Wireless access is limited to authorized Nation Staff.

Wireless networks must protect wireless connections from unauthorized access or misuse. The BC Government IM/IT Architecture and Standards Manual is required to be used and is available at http://www.cio.gov.bc.ca/cio/standards/standards_manual.page

Any other methods for accessing data remotely must be reviewed/approved by the Data Governance Board.

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Stewards</td>
<td>Integrate request and approval using wireless into the Data Access Procedures; and obtain review/approval by the Data Governance Board.</td>
</tr>
</tbody>
</table>
Remote access to data stored and managed by another Party must be approved prior to accessing the data. Approval must consider the service or data governance and information sharing agreements. In other words although a Staff member may be approved to access data using our wireless access capabilities the approval is limited to data stored internally and does not extended to data stored/managed by our Partners. Additional general approval would need to be obtained to access data stored/managed by our Partners.

A Wireless Access Request/Approval form must be used to facilitate a Staff member having approval to the wireless access functionality. The Data Custodian is responsible to develop and integrate these procedures into the Data Access Procedures.

The Wireless Access functionality must have:

• Stringent technical controls that meet industry best practices and support the approvals from our health care partners (e.g. VPN, firewall rules, data and transmission encryption, etc.).
• Device hardening (e.g. removing unused services, hard drive encryption, antivirus, personal firewalls, etc.)
• Audit and monitoring processes during the remote access sessions
• Ability to revoke access immediately once access is no longer required
• Ability to suspend a user’s access temporarily or permanently
• Multi-factor authentication that complies with the BC government cryptographic standards
Data Governance Framework – Data Governance Policy Manual

Privacy and Terms of Employment

Applicable To:
All data

Approval Date:
[mmm/dd/yyyy]

Approved By:
Nation Leadership

Any Related factors:
This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

All staff that has the potential to access Nation data is responsibility to protect the data as part of their employment. This policy outlines how this responsibility is enabled.

Policy

All Staff must agree to the following privacy related terms and conditions of employment:
• Agree to the verification of their identity
• Agree to provide proof if their legal name changes
• The willingness to sign Confidentiality and Acceptable Use agreements as required to access personal information.
• Agree to following the obligations set out in the Confidentiality and Acceptable Use Agreement
• Agree to reaffirm their obligations on a regular basis

The Confidentiality and Acceptable Use Agreement must be retained in accordance to the record retention schedule.

The Confidentiality and Acceptable Use Agreement must include the following:
• Agreement to surviving the termination of employment.
• Agreement to participate in privacy and security awareness training.
• Affirming the staff is aware and agrees to follow the privacy legislation, their professional obligations, and our privacy and security policies and procedures when they are working on behalf of our organization regardless of whether they are doing so on or off our premises.
• Agreement to only access personal information in support of their role and responsibilities at the given time. This includes not accessing their own personal information or anyone else’s personal information (including family and/or friends) unless required to do so in accordance to the role and responsibility they are fulfilling on behalf of our organization (e.g. providing health care services (direct or indirect) to the individual, and/or in support of
delivering Health Centre on behalf of our community or health care partners (e.g. population health, surveillance, program management).

- Agreement to share personal information in accordance to our Information Sharing policy.
- Agreement that the Staff Accounts (e.g. User Id(s) and password(s)) are considered to be an electronic signature and all activity linked to these accounts is considered to be performed by the given staff member. Therefore the account access details will not be shared with anyone; and password management will be performed in accordance to the applicable policy.
- Agreement that the records accessed by the Staff Accounts are recorded in an audit log and used for the purpose of auditing compliancy with this agreement and the privacy and security policies.
- Agreement to inform our organization if they are aware of any potential privacy and/or security incident and will report them in accordance to the applicable policy and procedures.
- If applicable agreement to advise our organization if they are/aren’t currently in good standing with their respective professional organization; and to advise our organization if this standing changes.
- Acknowledgement that failure to comply with this agreement and/or the privacy and security policies/procedures can lead to disciplinary action, which may include termination of access, withdrawal of privileges, termination of employment, professional sanctions, and/or legal action.

The delegated Data Stewards develop the Confidentiality and Acceptable Use Agreement form and presents it to the Data Governance Board who reviews/approves. If approval cannot be obtained the board must provide guidance and the form is updated and reviewed until such time it is approved.

The Data Steward that delivers the Data Governance and Awareness Training is responsible to facilitate the Confidentiality and Acceptable Use Agreement. Refer to the Data Governance Framework – Data Governance Policy – Awareness and Training.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Governance Board</td>
<td>Approve the Confidentiality and Acceptable Use Form</td>
</tr>
<tr>
<td>Staff involved in hiring</td>
<td>Ensure this policy is applied</td>
</tr>
<tr>
<td>Staff</td>
<td></td>
</tr>
<tr>
<td>Data Steward</td>
<td>Develop the Confidentiality and Acceptable Use form and put forward for approval</td>
</tr>
</tbody>
</table>
Handling Sensitive Information

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

Human Related data, sensitive data, and important data that is recorded on paper or electronically on devices such as a memory stick or displaying on a monitor requires controls to ensure it is protected from unauthorized access and/or theft or loss. This policy provides guidance to protecting this type of media under varying circumstances.

Policy

Personal/Sensitive/Important information that is stored or produced via electronic media (e.g. memory stick, displaying on monitors, printers, faxes, etc.) or recorded on paper will be protected using the following controls:

• Must be marked ‘Confidential’ or retained in a ‘confidential’ folder, and wherever possible the material should include:
  • Date and time the information was produced/recorded
  • Identify who recorded the information or in the case of extracting the information from an information management system record who extracted the information (e.g. name, User ID, and where necessary the Role).
  • In the case of extracting the information from an information management system record the name of the system.

• Information retained in our secure physical locations and not in use must be stored in designated locations (e.g. secure filing cabinets, secure desk drawers, etc.) defined by the Data Custodian. This includes clearing desks from all personal/sensitive/important information at the end of each business day; and for long-durations of absence within a day when the information is not being used (e.g. lunch, coffee breaks, attending meetings, etc.). It also includes clearing printers immediately; and clearing faxes on regular intervals.

• Information retained in our secure physical locations and in use must be kept confidential to the best of our ability. This includes,
• Positioning monitors to prevent unauthorized viewing of personal/sensitive/important information. Where a monitor cannot be situated to fully prevent unauthorized viewing other tools can be used to limit or minimize the risk (e.g. screen blockers, etc.).
• Locating printers and facsimiles within a secure perimeter and situating them in a manner that prevents unauthorized access.
• Information stored on a memory stick must be protected by a password and encrypted.
• Information taken out of our secure physical locations for the purpose of delivering/managing health care services must be stored in a folder/container that identifies it as belonging to our organization and must remain in the presence of an authorized employee or contractor of our organization (i.e. information cannot be left in an automobile or home office without the presence of an authorized provider).
• Information that must be transported to a physical location for the purpose of another organization receiving the information in context of delivering/managing health care services (e.g. a lab, physician office, a Regional Health Authority, etc.) must be transported by an authorized employee or contractor; or A secure/confidential provider who is bonded and has security clearance to deliver the item. A transported item must be:
  i. Verified that disclosure of the information is authorized
  ii. Marked ‘Confidential’
  iii. Stored in a container marked ‘Confidential’ and contain the correct name/address of the sender and receiver
  iv. Be tracked while in transit from our destination to the recipient
  v. Monitored to confirm its receipt

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Custodian</td>
<td>Assign secure designated locations for storing data</td>
</tr>
</tbody>
</table>
Protection of Physical Locations

Applicable To: All data storage locations
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

Personal, sensitive, or important information is contained within physical locations and/or is made accessible from physical locations. This policy outlines the safeguards that protect and secure the physical locations.

Policy

The physical location of each data asset must be protected against unauthorized access therefore the Data Custodian must complete a Physical Location Profile document for each location where data is stored. Once completed the document must be reviewed/approved by the Data Governance Board. Where approval cannot be obtained the Board must provide guidance and the Data Custodian must update accordingly and resubmit for review/approval. The Data Governance Board must provide recommendations and monitor action plans if required.

The Data Custodian must review/update the profile documents every five (5) years and subsequently seeks Data Governance Board approval.

The profile document must include the following:

- A description and diagram of the physical space that shows the physical access points (e.g. doors, windows, rooms, closets, attic doors, crawl space doors, etc.) and a description of any key vulnerabilities (e.g. wood floor accessible by a crawl space that has no access controls) [note: this diagram may be an integrated diagram that also shows other key items described in the privacy and security policies/procedures]
- A description of any enhanced features that currently protect the physical space (e.g. fire doors, sprinkler system, bars on windows, etc.)
- A description of what controls access to each of the access points (e.g. locked doors, alarm system, locked filing cabinets, access control boxes, windows, etc.)
• A description of how each of the controls is:
  • Managed
  • Authorized
    • Monitored – i.e. proactive monitoring (alarms, alerts, etc.) and reactive (regular review of audit logs, etc.); and testing
  • Identification of where the records are located that show:
    • Who has access
    • When access was provided
    • Who authorized access
    • When access was removed

• Access risks and recommendations
• A link to the Data Governance Framework document and the Privacy Breach Notification and Investigation procedures as/when unauthorized access occurs and is identified in the course of managing access
• The name of the author, reviewers, and approvers
• The version and version control log that describes the changes made to a given version of the document
• The status of the document (i.e. draft; approved; implemented)

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Custodian</td>
<td>Develop and maintain the Protection of Physical Location</td>
</tr>
<tr>
<td>Data Governance Board</td>
<td>Review/approve the profile documents; and monitor action plans.</td>
</tr>
</tbody>
</table>
Mobile Data Management

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

Staff may need to be mobile when performing their responsibilities in support of our Nation. During these sessions Nation data may be collected, used and/or disclosed. This policy outlines the guidelines that must be used when Nation Staff are mobile.

Policy

It is acceptable to collect, use and/or disclose Nation data outside of our secure locations when services are being delivered. The privacy legislation and the applicable data governance and privacy and security policies must be applied and adhered to.

If a Staff member is not involved in delivery of the service and are within the range of hearing or reading the data it is incumbent on our Staff to facilitate the creation of an environment where the data can be shared comfortably. Alternatively those that should not be hearing or seeing the data must be requested to leave the environment such that the data can remain private. It is recognized that if the situation is emergent this may not be possible therefore this policy is applied at the discretion of our Staff however every effort must be made to protect Nation data.
Network Management

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

The purpose of this policy is to provide guidance on the management and support of our computing network, including the hardware, software, management tools, and access procedures.

Policy

The network services that our organization is dependent on and is used to access, store, or manage Nation data is required to comply with the following:

• Documented roles and responsibilities for managing the network
• Documented business requirements, for example, number of users, hours of operation, tolerance for outages, physical location specifications, speed, services such as shared network, Virtual Private Network (VPN), remote access, user groups (e.g. employees, contractors, guests, technical support, authentication, etc.)
• Documented design and configuration and how access is protected including physical and logical access controls
• Each user must be uniquely authenticated
• Each user must be capable to prove its identity using a digital certificate that complies with industry best practice Cryptographic Standards - the BC Government Cryptographic Standards must be used by any user requiring access to the provincial Electronic Health Record information management systems, therefore standards will be used for our network unless another standard is deemed better and is approved by the BC Government
• All information exchanges with health care partners must be able to verify the integrity of the data being transmitted/exchanged
• Any transactions where users are applying the electronic equivalent of a handwritten signature must:
  o Allow users to apply a digital signature that satisfies the requirements under the provincial legislation
• A set of documented procedures that describe:
• Backup and recovery details
• Disaster planning details
• How issues are managed
• How changes are reviewed, approved, and implemented
• The technical support team access requirements and how these will be enabled/disabled in the standard operational setting
• How user access to the network will be enabled/disabled in the standard operational setting
• The audit records that track all accesses (e.g. technical support team and users) and the monitoring process
• Link to the Privacy Breach Notification and Investigation policies/procedures
• How access is disabled for one user, many users, or all users in the event of a potential or confirmed privacy and security breach
• Linkages to the Business Continuity Plan
• Support services associated with providing/maintaining the network must be defined by a documented Service Level Agreement (SLA) which, at a minimum, must include the following:
  • A definition of the privacy and security roles/responsibilities of the service provider and their employees/contractors
  • Agreement to comply with our privacy and security policies as an addendum to the SLA
  • If remote access for supporting the network is required it must be done using secure methods that enable access for the specific incident. Furthermore remote access cannot be used from outside of Canada
  • A set of documented procedures that describe:
    o The service level requirements
    o How technical issues will be communicated and managed
    o How changes will be communicated and managed, including authorization for making changes that are specific to our network
    o How access to the network will be enabled/disabled and monitored
    o How potential privacy and security breaches/incidents will be managed and investigated, including retention of any evidence that may be linked to the event(s)
    o How changes to procedures will be managed/approved
    o How compliancy to our privacy and security policies will be assessed

The Nation Manager that is accountable for establishing and managing the network is responsible to adhere to this policy and provide recommendations to update it.
### Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable Nation Manager</td>
<td>Adhere to the policy and make recommendations for any changes.</td>
</tr>
</tbody>
</table>
User ID and Password Management

Applicable To: All computer-based systems containing Nation data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

To ensure access to electronic information and resources (e.g. computers, printers, servers, applications, etc.) is effectively managed we must authenticate a user’s access by issuing unique identifiers (e.g. User ID) and passwords to effectively protect Nation data.

Policy

The Data Steward must validate that the procedure for hiring staff requires our Staff’s identity to be verified using industry best practices (e.g. two pieces of I.D. match the legal name on the Staff’s employment application and employment record.)

Each Staff member requiring a User ID must be assigned a unique user identifier (i.e. User ID) must not share the User ID with any other person. Other approved access methods (e.g. keys, key codes, etc.) must not be shared with unauthorized users.

User ID and passwords must be distributed using secure methods which may include person-to-person, via email or voice mail that simulates person-to-person such that only the intended person can receive the User ID or Password. The User ID and password must be transmitted in two different transactions.

Supplemental credentials (e.g. a series of questions/answers) used for the purposes of password reset or authenticating Help Desk requests are not to be used to subsequently grant additional access or privileges. In other words all additional access requests or privileges must be approved and processed as per the access policy. When supplemental credentials are used they must be stored in a protected format.

At a minimum a password is managed using the following practices:
• Passwords are not displayed on screen or on printed material
• Passwords are not transmitted in clear text
• Temporary passwords issued to users must be changed on first use
Data Governance Framework – Data Governance Policy Manual

- When a new password is processed the password specifications (see below) and guidelines of this policy must be verified before the change is processed
- Users set their own passwords
- Regular user password change must be set up preferably managed systematically, i.e., user passwords will expire after a predetermined number of days
- Passwords are required to be changed regularly and more frequently for users with special access privileges
- Re-use of passwords is restricted (e.g. cannot be used again within a set period or set number of changes)
- After three consecutive failed logon attempts the account must be locked out
- Passwords must be comprised of the following specifications ¹
  - Contain a minimum of 8 characters;
  - Contain characters from three of the following categories:
    - English upper case characters (A to Z),
    - English lower case characters (a to z),
    - Numerals (0 to 9), and,
    - Non-alphanumeric keyboard symbols (e.g., ! $ # %); and,
  - Not contain the user name or any proper names of the user.
- Passwords must be encrypted using industry best practices – the BC Government cryptographic and data handling standards are to be used:
  - when data is being transmitted electronically
  - when it is at rest (e.g. in a database)
- Employees or contractors cannot view or decrypt passwords
- Sign-on procedures cannot store authentication details as clear text in automated routines
- Password management and passwords themselves must comply with industry best practices – the BC Government password standards will be used (refer to unless a better standard is obtained and approved by Data Custodian.

After three (3) failed login attempts for a User Id/password the system must:
- Lock the account and require administrator intervention whereby the administrator is a different individual from the individual who requires the User ID to be ‘unlocked’; or

¹ As per the BC Government Information Security Policy extracted June 15, 2012:
http://www.cio.gov.bc.ca/local/cio/index.page
• Lock the account for 15 minutes and then allow further three logon attempts at which point after the 2nd series of three attempts if it results in the account being locked it would require administrator intervention

• An administrator cannot unlock or change his/her own User Account (i.e. User ID, password, unlock password, change access privileges)

The Data Custodian must ensure all systems adhere to this policy/procedure and report anomalies to the Data Governance Board. The Data Governance Board must review anomalies, approve deviations, provide recommendations and monitor action plans.

**Roles and Responsibilities**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Custodian</td>
<td>Ensure systems meet this policy</td>
</tr>
<tr>
<td>Data Governance Board</td>
<td>Review policy deviations, provide recommendations, and monitor action plans.</td>
</tr>
</tbody>
</table>
Clean Desk

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors: This policy aligns with the Ministry of Health Software Conformance Standards; and BC privacy legislation

Purpose:

Nation data is often accessed and reviewed in personal office space assigned by our nation. This policy outlines the requirements associated with ensuring Nation data is protected when offices are unstaffed for any period of time, when meeting occurs within the office, etc.

Policy

When leaving the office desk for a period of time and/or at the end of the business day, the desk must be clean with workstations locked, all mobile devices (i.e. cell phones, cameras, laptops) locked and secured, and paper records containing Nation data stored in a locked location.

When meetings or discussions occur in a location where Nation data exists and the data is not part of the meeting/discussion it must be kept confidential using the best logical process determined by the Staff member. This may include turning a paper over, closing a file, filing the information, logging out of a computer system, locking a computer monitor screen, walking out of the space and securing the data perhaps behind a locked door, etc. All Staff are responsible for ensuring these practices are applied.
Network Management

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors:

Purpose:
To be developed during Demonstration Site Implementation

Policy
To be developed during Demonstration Site Implementation
Other Security Related Policies

Applicable To: All data
Approval Date: [mmm/dd/yyyy]
Approved By: Nation Leadership
Any Related factors:

Purpose:
To be developed during Demonstration Site Implementation

Policy
To be developed during Demonstration Site Implementation

Document Versioning

The following table describes how this document evolved to become the current version.

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Change Reference</th>
<th>Reviewed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 31 2015</td>
<td>Mustimuhw Information Solutions Inc.</td>
<td>V0 (Template)</td>
<td>Initial template document</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Appendices
The following appendices are provided in this section of the document:

Privacy Advocate - Poster
Caring For Your Information - Poster
Caring For Your Information - Pamphlet
Caring For Your Information – Telephone Script
Request for Human Related Personal Information
Disposal Request, Approval, and Tracking Form
Privacy Rights, Commitments, Obligations – Poster
Our Executive Data Steward is here to advocate your privacy rights and support you in any questions, requests, complaints that you may have regarding privacy of your human related personal information.

Inquires/Questions/Access
You have the right to:
• Ensure your personal information that we hold and protect is accurate
• Understand how your information has been used
• Know the names and organizations to which your personal information has been disclosed

To make any of the above requests, please contact a member of our Data Governance Board who will guide you through submitting a “Client Request for Access to Personal Information”. The Steward will review our policy with you and assist with fulfilling your request.

Privacy Breach Notification & Investigations
<insert Nation and Community names> has a policy and process for you to raise any privacy issues you may have and investigate.

You have the right to raise privacy issues, including:
• Any risks or concerns that you see regarding the privacy of your personal information
• Any privacy complaints you wish to make regarding the handling of your personal information
• Reporting an actual or suspected breach of your privacy or misuse of your personal information; or suspected breach or misuse of someone else’s personal information

To raise any of the above privacy issues, please contact a member of our Data Governance Board who will review our policy with you and assist in facilitating and reporting back as per the formal investigation process.

Commitment to Accuracy
We are committed to ensuring personal and health information will remain confidential.

Commitment to Accuracy
We are committed to ensuring your personal health information is accurate.

We are committed to empowering you to understanding your rights regarding the protection of your personal health information.

FOR FURTHER INFORMATION CONTACT
DATA GOVERNANCE OFFICE AT:
PHONE: <insert>
Email: <insert>
Postal address: <insert>
<insert name of Nation and Community/Communities> understands the sensitivity of your human related personal information. We are committed to protecting your privacy.

When you receive care and services from our Nation, we will collect, use and share your human related personal information for these reasons:

- To identify and keep in contact with you in context
- To provide ongoing care
- To support the provision of care by wellness partners
- To help us plan, monitor and improve our care and services to you
- To understand your eligibility for benefits and services
- Where relevant to support billing to medical services
- To analyze, manage and health and wellness and monitor the overall health of the people
- As required by law (e.g. court order, reportable conditions)

We do this under, and in accordance with, the Personal Information Protection Act (PIPA) and other applicable legislation.

Understanding Implied Consent

<FNHSO> operates under an “implied client consent model”. This means by receiving our care services we have your implied consent for information to be shared as required with those within your “circle of care” for the purpose of your ongoing care and/or treatment (e.g. other care providers, specialists, lab technologists, etc.).

Understanding Expressed Consent

Expressed consent (verbal or written) will be obtained if/when we are collecting, using, and disclosing personal information outside of the “circle of care”, or for secondary purposes outside of those listed to the left (for example, research, teaching/education).

You are entitled to enquire about privacy and to request access to your human related personal information; to do so please ask to contact the our Data Steward/Privacy Officer.
understands the sensitivity of your human related personal information. We are committed to protecting your privacy.

Commitment to Privacy
We are committed to ensuring human related personal information will remain confidential

Commitment to Accuracy
We are committed to ensuring your human related information is accurate

Committed to Empowerment
We are committed to empowering you to understanding your rights regarding the protection of your human related personal information

When you receive care and services from us, we will collect, use and share your human related personal information for these reasons:

- To identify and keep in contact with you in context
- To provide ongoing care
- To support the provision of care by wellness partners
- To help us plan, monitor and improve our care and services to you
- To understand your eligibility for benefits and services
- Where relevant to support billing to medical services
- To analyze, manage and health and wellness and monitor the overall health of the people
- As required by law (e.g. court order, reportable conditions)

- We do this under, and in accordance with, the Personal Information Protection Act (PIPA) and other applicable legislation.

Understanding Implied Consent
<FNHSO> operates under an “implied client consent model”. This means by receiving our care services we have your implied consent for information to be shared as required with those within your “circle of care” for the purpose of your ongoing care and/or treatment (e.g. other care providers, specialists, lab technologists, etc.).

Understanding Expressed Consent
Expressed consent (verbal or written) will be obtained if/when we are collecting, using, and disclosing personal information outside of the “circle of care”, or for secondary purposes outside of those listed to the left (for example, research, teaching/education).

You are entitled to enquire about privacy and to request access to your human related personal information; to do so please ask to contact the our Data Steward/Privacy Officer.

FOR FURTHER INFORMATION CONTACT DATA GOVERNANCE OFFICE AT:

PHONE: <insert>
Email: <insert>
Postal address: <insert>
Caring For Your Information: Telephone Script

There may be occasions when it is necessary for you to collect human related information from a Member/Customer/Guardian by telephone. The following telephone script ensures that the individual explicitly acknowledges that they have been informed about the purpose for the collection, use and disclosure of their human related personal information. Prior to using the script be sure to confirm the identity of the individual and confirm the reason for speaking with the Member/Customer/Guardian. If the individual does not acknowledge the understanding or disagrees with the purposes for collecting their human related personal information do not proceed to collect the data.

FNHSO Telephone Privacy Script:

During this call I may need to collect and record your personal information to verify your identity and provide services.

Your information may be shared with other providers who also provide you with related services.

Your information will be protected under the strict privacy and security standards followed by our Nation and in accordance to BC’s Personal Information Protection Act and other applicable legislation.

Do you feel comfortable sharing your personal information or do you have any questions about how it is collected, used or disclosed?

• If you wish to have more information, I can have our Data Steward/Privacy Officer give you a call or you can contact them by calling <insert phone number, and email>.
Request for Human Related Personal Information

Section A-Requestor
Name: _______________________________________________  Birth Date: ______________
   Last name  First name  Initial  MMM/DD/YYYY

Band ID#:________________ or, Other Unique Personal Identifier: ______________

Primary Address: __________________________________________
   Apt #, Address, City, Province/Territory, Postal Code

Section B-Request
Please provide the following:
☐ A copy of the following records that contain my personal information: (describe the specific records)
   Use the back of this request form to identify any additional records.

☐ A copy of all records containing my personal information
☐ An understanding of why my personal information records are used
☐ An understanding of whether my personal information records were disclosed and if so who they were disclosed to and when they were disclosed

Once the records are compiled please arrange for delivery using the following method:
☐ I will pick up the records therefore please contact me at: ________________________________
☐ I will arrange for a courier to pick up the records therefore please contact me at: ________________________________
☐ Mail the records to: ____________________________________________

Section C-Recipientship Details (to be completed by )

Request received date: ________________________________ (note, this date is based on the form being completed)

Received via: ________________________________ (mail, in-person, email, or fax)

Identity of requestor validated by: ________________________________ (name of staff member who validated the identity of the requestor; if received by email or fax the validation must be supported by an authorized party)

Notes: (used to track details – refer to the Privacy and Security Policy and Procedures manual)
Disposal Request, Approval, and Tracking Form

Section A-Request for Records Disposal

Requestor Name: ____________________________________________  Department ______________________
  Last name  First name  Initial

Record Type: ____________________ Contains Human Related Data?: ______  If Yes, Client or Staff?: ______
  (Electronic file, paper, etc.)  Yes / No  Client / Staff

Data Classification __________  Method of Disposal: __________  Requested Disposal Date: __________
  High/Med/Low  (Shred, delete, erase, etc. mmm-dd-yyyy

Section B-Approval for Records Disposal

By approving this request for records disposal, we hereby acknowledge that we do so in accordance with
the Nation Data Governance Policy and Privacy and Security Policies and Procedures, and applicable legislation.

Approved  Approved by:

  Name of Manager/Supervisor  Signature  Date

Secondary Approver:

  Name of Executive Data Steward  Signature  Date

Denied  Denied by:

  Name of Manager/Supervisor  Signature  Date

Denied Reason: ____________________________________________________________

Section C-Record of Disposal

Having received approval (Section B) for disposal of records (Section A), the undersigned hereby validates that the records have been disposed of, including the date and method of disposal.

Date of Disposal: ________________  Disposal Method: ________________
  mmm-dd-yyyy  (Shred, Delete, Erase, etc.)

Disposed of by: ___________________________  Signature: ___________________________
  Print Name  Signature


Privacy Rights, Commitments, Obligations

[insert name] clients have a right to:

• Confidentiality
• Ensuring their personal information is accurate
• Understanding who has access to their personal information and for what purpose
• Understanding how their personal information is retained
• Understanding how and when their personal information is shared
• Ensuring that we recognize and follow relevant legislation regarding protection of personal information

[insert name] staff have a commitment to our clients to:

• Ensure our operations and practices embody and recognize the client privacy rights above
• Ensure any aggregation of information or reporting does not identify an individual (either directly or by inference)
• Know and follow our Privacy & Security policies and processes

[insert name] recognizes privacy protection can co-exist with the collaborative human and social service programs that enables health and wellness for our people. Our privacy policies and practices formalize our commitment to both client privacy and the need for continuity of care within the “circle of care”.

[insert name] recognizes the value of sharing information for the purpose of assessing, planning, and developing First Nations human and social service programs, and will do so in ways that are consistent and in accordance with our Data Governance Framework and privacy and security policies.

[insert name] is committed to supporting staff in understanding and following our Privacy commitments and practices. This will include policy orientation for new staff, and annual privacy training for all staff. Clear roles and responsibilities for privacy protection within the organization will be maintained.