

Wahnapitae First Nation

**Privacy & Security Policies and Procedures
Recommendation and Approval
Policies: Privacy: 1-20 and Security 1-9**

| | |
|---|---------------------------|
| PRIVACY 1-20 POLICIES AND PROCEDURES ADOPTED AT REGULAR CHIEF AND COUNCIL MEETING ON MAY 8, 2018 | BCM# WFN 18/19-013 |
| SECURITY 1-9 POLICIES AND PROCEDURES ADOPTED AT REGULAR CHIEF AND COUNCIL MEETING OF MAY 8, 2018 | BCM# WFN 18/19-014 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

Purpose:

To provide acknowledgement by the WFN's key leadership that the Privacy & Security program is adopted and that any privacy and security gaps identified by working through 'The Five Steps' are being addressed.

Description:

Documents that privacy and security policies and Action Plan had been officially signed off by key leadership at the WFN and is a good indicator that the WFN can leverage opportunities and access to health organization systems that require the health organization to have a robust privacy and security culture.





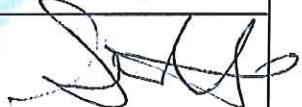
How to Use It:

Review all policies (Privacy-1-20 and Security-1-9 with key leadership and obtain their signatures to indicate that all policies are approved and adopted and or mirrored in the existing policies already in place at the health organization. **Noting that EACH policy has an approval panel at the bottom where leadership should sign/initial off.** Update this document - print off and get signatures. This overall signature document covers approval of ALL policies - attach to the hard copy of the WFN Health Department's policy set as a summary approval acknowledgement.



| TABLE OF CONTENTS – PRIVACY 1-20; SECURITY 1-9 | | |
|--|--|----------|
| Policy # | Name of Policy | Type |
| 1 | STATEMENT ON PRIVACY GUIDELINES AND PRINCIPLES | Privacy |
| 2 | (ONTARIO) – HEALTH INFORMATION CUSTODIAN ‘HIC’ RESPONSIBILITIES | Privacy |
| 3 | PRIVACY CONTACT RESPONSIBILITIES | Privacy |
| 4 | SECURITY CONTACT RESPONSIBILITIES | Privacy |
| 5 | PRIVACY POLICY FOR PERSONAL HEALTH INFORMATION ‘PHI’ | Privacy |
| 6 | DATA CLASSIFICATION FOR PERSONAL HEALTH INFORMATION ‘PHI’ POLICY | Privacy |
| 7 | RETENTION OF PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY | Privacy |
| 8 | ARCHIVING & ACCESSING PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY | Privacy |
| 9 | DESTRUCTION OF PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY | Privacy |
| 10 | DE-IDENTIFYING HEALTH INFORMATION POLICY | Privacy |
| 11 | CONSENT POLICY FOR COLLECTING, USING & DISCLOSING INFORMATION | Privacy |
| 12 | ACCURACY OF DOCUMENTATION POLICY | Privacy |
| 13 | CLIENT ACCESS AND RELEASE OF ‘PHI’ POLICY | Privacy |
| 14 | INFORMATION CORRECTIONS AND APPEALS POLICY | Privacy |
| 15 | SENDING AND RECEIVING SENSITIVE INFORMATION POLICY | Privacy |
| 16 | SOCIAL MEDIA POLICY | Privacy |
| 17 | PROGRAM AUDIT BY A THIRD-PARTY POLICY | Privacy |
| 18 | WHISTLE BLOWER PROTECTION POLICY | Privacy |
| 19 | INFORMATION DATA RESEARCH POLICY | Privacy |
| 20 | CONFIDENTIALITY AND ACCEPTABLE USE POLICY | Privacy |
| 1 | INFORMATION SECURITY POLICY | Security |
| 2 | MOBILE DEVICES POLICY | Security |
| 3 | INFORMATION TECHNOLOGY ASSET MANAGEMENT POLICY | Security |
| 4 | BUSINESS CONTINUITY MANAGEMENT PLAN POLICY | Security |
| 5 | USER ACCESS AND ACTIVITY AUDIT POLICY | Security |
| 6 | PRIVACY & SECURITY INCIDENT RESPONSE POLICY | Security |
| 7 | ORGANIZED OFFICE | Security |
| 8 | AUDIO/VIDEO SURVEILLANCE | Security |
| 9 | CLOUD-BASED DELIVERY OF SERVICES POLICY | Security |

By signing this document, signatories are certifying that the content herein is recommended as a direction for fostering a healthy privacy and security culture at the Norman Recollet Health Centre and that they will ensure that the policies, procedures and related tools are implemented and used. This includes the Privacy Policies 1-20 and Security Policies 1-9.

| Date | Document Name/ Version | Position/Title | Name | Signature |
|----------------|--|-----------------------|-------------------|---|
| April 30, 2018 | Privacy Policies 1-20 Security Policies 1-9 | Chief | Ted Roque |  |
| April 30, 2018 | Privacy Policies 1-20 Security Policies 1-9 | Counsellor | Bob Pitfield |  |
| April 30, 2018 | Privacy Policies 1-20 Security Policies 1-9 | Counsellor | Barret Dokis |  |
| April 30, 2018 | Privacy Policies 1-20 Security Policies 1-9 | Counsellor | Larry Roque |  |
| April 30, 2018 | Privacy Policies 1-20 Security Policies 1-9 | Counsellor | Samantha Corbiere |  |

Wahnapiatae First Nation

PRIVACY-1: STATEMENT ON PRIVACY GUIDELINES AND PRINCIPLES

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCN #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will publicly inform clients that privacy and security guidelines and procedures are in place and that their personal health information 'PHI' is being managed and protected. The commitment by the health organization is to:

- i. only ask for PHI that is needed for the indicated purposes;
- ii. only use or share PHI for the purposes for which it was provided, unless required to do so by law;
- iii. keep PHI only as long as required by provincial regulations and/or special territorial requirements;
- iv. be transparent about sensitive information that may be collected and managed by secure third parties;
- v. keep PHI accurate and up-to-date, allow only authorized people to see PHI;
- vi. commit that client sensitive information will be protected under provincial or territorial laws.

1.1 Statement/Poster Messaging

The health organization will assure clients and clients that privacy and security guidelines and procedures are in place by:

- i. installing posters in visible prominent areas in the health organization facility (e.g. clinics, lobby, etc.)
- ii. providing brochures to the client including when the health care services are being delivered offsite (e.g. at offsite clinics & special events, schools, client's home, etc.)

The messaging and content on the posters and in the brochures, will include statements like:

- Wahnapiatae First Nation values the trust you have placed in us. We respect your personal privacy and do our best to safeguard its confidentiality and security.
- Wahnapiatae First Nation understands the sensitivity of your personal health information. We are committed to protecting your privacy.
- When you receive care and services from Wahnapiatae First Nation, we will

- xi. Attest annually that the HIC remains compliant with the all obligations of their Privacy and Security Policies.

1.2 Inquiries and Complaints

Inquiries and complaints that are related to PHI maintained by Wahnapiatae First Nation are managed as described in Privacy-5 Privacy Policy For PHI.

If the PHI is managed by the eHealth Ontario program (e.g. access via a provincial viewer), then inquiries and complaints are processed by eHealth Ontario. A HIC must ensure that they are able to accommodate addressing Inquiries and Complaints related to the eHealth Ontario Program, whether that be addressing the Inquiry or Complaint or forwarding the Individual to eHealth Ontario within 4 working days of the inquiry or complaint, depending on the situation, and provide supporting information to eHealth Ontario within 14 calendar days to support the inquiry or complaint. All inquiries and complaints and their response must be logged, and a copy of the inquiry/complaint included in the client's health file record.

1.3 Annual self-attestation of compliance to HIC responsibilities

eHealth Ontario provides a self-attestation that HICs are required to complete each year.

1.4 North East Local Health Integration Network 'LHIN'

If the organization is an agent of the North East Local Health Integration Network 'LHIN' any suspected/actual privacy breaches must be reviewed with LHIN. This includes use or disclosure without authority; stolen information; further use or disclosure without authority; pattern of similar breaches; disciplinary action against a staff member with or without a professional designation (i.e. health college member); and or any breaches of a significant nature.

1.5 Statistics and Reporting

The designated HIC privacy contact will be responsible for logging any privacy breaches and requests for information so that prior year statistical reports can be provided to the Information and Privacy Commissioner (IPC) of Ontario by March 1st of every year.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-2 (Ontario) – Health Information Custodian 'HIC' Responsibilities Policy:

Privacy-3 Privacy Contact Responsibilities Policy

Privacy-4 Security Contact Responsibilities Policy

3.0 POLICY - ACTION ITEMS


Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are

used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

| Privacy & Security Implementation Workbook | | |
|--|--|---------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>Attestation to Compliance</i> | <i>For ONTARIO HIC's only (but can also be leveraged by other provinces as documentation for compliance) - to provide the health organization with a template for Attestation to Compliance when the health organization is using an Ontario health record system.</i> | 1.3 |


Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-2: (ONTARIO) - HEALTH INFORMATION CUSTODIAN 'HIC' RESPONSIBILITIES

| | |
|---|-------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM#WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The Health Information Custodian, 'HIC', as defined in the *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A*, means a person or organization described in one of the paragraphs in the Act who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any. The following is mandatory for a HIC organization providing health services in the province of Ontario:

1.1 Health Information Custodian 'HIC' Responsibilities:

- i. Identify a Privacy Contact responsible for following PHIPA rules, and responding to questions, access or correction requests, and complaints;
- ii. Limiting the collection, use, and disclosure of PHI to only what is necessary to meet the purposes identified in the Privacy Notice;
- iii. Making a Privacy Notice available that describes PHI practices;
- iv. Ensure that the Privacy Notice provides the eHealth ONTARIO website and its contact information for clients, so they have a clear means of contacting eHealth. (E.G. when a client gives a consent directive (e.g. a block) relevant to another health organization/s they should be instructed to contact eHealth ONTARIO);
- v. Following steps to ensure PHI is accurate;
- vi. Maintaining physical, technical, and administrative controls to keep PHI safe and support secure disposal;
- vii. Developing a process to manage user accounts so only authorized users providing health care services or other approved activities have access to PHI;
- viii. Providing access to or correction of a client's PHI upon written client request, subject to some exceptions (PHIPA Sections 52 and 55);
- ix. Developing policies and procedures to support the collection, use, and disclosure of PHI including privacy or security breaches, record keeping and destruction; and
- x. Notifying affected individuals of privacy breaches.

- xi. Attest annually that the HIC remains compliant with the all obligations of their Privacy and Security Policies.

1.2 Inquiries and Complaints

Inquiries and complaints that are related to PHI maintained by Wahnapiatae First Nation are managed as described in Privacy-5 Privacy Policy For PHI.

If the PHI is managed by the eHealth Ontario program (e.g. access via a provincial viewer), then inquiries and complaints are processed by eHealth Ontario. A HIC must ensure that they are able to accommodate addressing Inquiries and Complaints related to the eHealth Ontario Program, whether that be addressing the Inquiry or Complaint or forwarding the Individual to eHealth Ontario within 4 working days of the inquiry or complaint, depending on the situation, and provide supporting information to eHealth Ontario within 14 calendar days to support the inquiry or complaint. All inquiries and complaints and their response must be logged, and a copy of the inquiry/complaint included in the client's health file record.

1.3 Annual self-attestation of compliance to HIC responsibilities

eHealth Ontario provides a self-attestation that HICs are required to complete each year.

1.4 North East Local Health Integration Network 'LHIN'

If the organization is an agent of the North East Local Health Integration Network 'LHIN' any suspected/actual privacy breaches must be reviewed with LHIN. This includes use or disclosure without authority; stolen information; further use or disclosure without authority; pattern of similar breaches; disciplinary action against a staff member with or without a professional designation (i.e. health college member); and or any breaches of a significant nature.

1.5 Statistics and Reporting

The designated HIC privacy contact will be responsible for logging any privacy breaches and requests for information so that prior year statistical reports can be provided to the Information and Privacy Commissioner (IPC) of Ontario by March 1st of every year.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-2 (Ontario) – Health Information Custodian 'HIC' Responsibilities Policy:

Privacy-3 Privacy Contact Responsibilities Policy

Privacy-4 Security Contact Responsibilities Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are



used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

| Privacy & Security Implementation Workbook | | |
|--|--|---------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>Attestation to Compliance</i> | <i>For ONTARIO HIC's only (but can also be leveraged by other provinces as documentation for compliance) - to provide the health organization with a template for Attestation to Compliance when the health organization is using an Ontario health record system.</i> | 1.3 |



Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-3: PRIVACY CONTACT RESPONSIBILITIES

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM# WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization shall identify and designate a privacy contact as the person responsible for ensuring that privacy policies and procedures are followed. The privacy contact's organizational job description need to reflect the responsibilities of the privacy role. The privacy contact designate for the organization will be kept current on any documentation including the privacy poster and brochures for the Wahnapiatae First Nation.

1.1 Knowledge

The privacy contact will be familiar with and remain current in:

- i. The health organization's approved privacy policies and procedures;
- ii. Applicable provincial/territorial privacy laws;
- iii. First Nation privacy laws, if applicable;
- iv. Privacy principles and guidelines;
- v. How to protect individual and community privacy in aggregate formats, such as community reports.

1.2 Key Responsibilities

The privacy contact will actively handle the following responsibilities:

- i. Help staff follow established privacy policies and procedures to ensure health organization remains compliant
- ii. Intervenes on privacy-related issues when required and is available to staff to provide advice and answer privacy related questions;
- iii. Ensures that external contractors or contacts (such as visiting healthcare professionals, I.T. vendors, students and volunteers) are informed about their privacy responsibilities and the health organization's privacy policies and procedures; Identifies privacy training, assessment tools, and awareness opportunities for staff;
- iv. Investigates and reports privacy breaches;
- v. Responds to questions from leadership and management regarding how PHI is managed, protected and disclosed.
- vi. Reviews all privacy policies and procedures on a regular basis (e.g. every 2 to 3 years) to

- confirm they remain current and complete and revises as necessary to address identified gaps;
- vii. Conducts an 'Information Privacy Assessment' every 3 to 5 years or when major change occurs to the health organization, technology, business objectives, process, identified threats, possible future threats or external events;
 - viii. Maintains a high-level view of the personal health information 'PHI' that is collected, used and disclosed by staff delivering services on behalf of the health organization and ensures appropriate authorization for access are in place;
 - ix. Conducts regular reviews (e.g. at least annually) of the purposes for collection, use and disclosure of PHI to ensure they remain appropriate or to identify new purposes;
 - x. Ensures that an evaluation of privacy impacts is completed for each new request for access to data and identified risks are addressed prior to providing the data;
 - xi. Regularly monitors user access and activity to practices and clinical data by regular audits (e.g. at least annually) to ensure access is appropriate and initiates training and/or disciplinary actions when necessary;
 - xii. Conducts scheduled audits of the consent directives to ensure that they are still appropriate.
 - xiii. Responds to client questions, complaints, access, and correction requests related to information practices;
 - xiv. Champions the health organization's privacy policies, practices, and procedures to ensure alignment with other policies that might already be in place as a result of existing community activities such as Emergency Preparedness Planning;
 - xv. Advises management and staff about how privacy policies, practices, and procedures can be consistent with applicable privacy obligations and privacy best practices;

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-3 Privacy Contact Responsibilities Policy:

Privacy-4 Security Contact Responsibilities Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook'.

| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>HO P&S Contacts</i> | <i>Provides a table to identify key individuals responsible for privacy and security at the health organization. Provides a quick reference for applicable contacts at the Provincial and Federal level for advice about your privacy and security program and for clarification on the provincial and federal laws around privacy and security.</i> | 1.0 |
| <i>P&S Job Responsibilities Review</i> | <i>Provides a tool (procedures & checklist) to determine how the primary functions associated with the Data Governance, Privacy and Security accountabilities and responsibilities are reflected in job descriptions for the P&S designates and all staff involved with Personal Health Information 'PHI' or with access to sensitive information.</i> | 1.2 |
| <i>P&S Contact Activity Checklist</i> | <i>Provides a checklist including the timing of privacy & security activities for the Privacy & Security Contacts to monitor and ensure that they are aware of their ongoing accountabilities and responsibilities.</i> | 1.2 |
| <i>Information Privacy Assessment</i> | <i>Provides an assessment tool to identify the obligations, scope and any gaps regarding privacy policies and procedures that may require the health organization to create an action item/s (Action Plan)</i> | 1.0 |
| <i>Action Plan</i> | <i>Provides a clear means of tracking action items that must be completed to demonstrate the health organization is in compliance with privacy and security protocols and laws.</i> | 1.0 |

X

Ted Roque
Chief

Wahnapitae First Nation

PRIVACY-4: SECURITY CONTACT RESPONSIBILITIES

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization shall identify and designate a security contact as the person responsible for ensuring that security policies and procedures are followed. The security contact's organizational job description need to reflect the responsibilities of the security role. The security contact designate for the organization will be kept current on any documentation including the privacy & security poster and brochures for the Wahnapitae First Nation.

1.1 Knowledge

The security contact will be familiar with and remain current in:

- i. The health organization's approved security policies and procedures;
- ii. Applicable provincial/territorial privacy laws;
- iii. First Nation security laws, if applicable;
- iv. Security principles and best practices;
- v. The health organization's security policies and procedures.

1.2 Key Responsibilities

The security contact will be actively handling the following responsibilities:

Helps staff follow security policies and procedures to ensure health organization remains compliant

- i. Intervenes on security-related issues when required and is available to staff to provide advice and answer security related questions;
- ii. Ensures that external contractors or contacts (such as visiting healthcare professionals, students and volunteers) are informed about their security responsibilities and the health organization's security policies and procedures;
- iii. Responds to security questions and complaints from clients and clients;
- iv. Reviews all security policies and procedures on a regular basis (e.g. every 2 to 3 years) to confirm they remain current and complete and revises as necessary to address identified gaps;
- v. Identifies security training, assessment tools, and awareness opportunities for staff;
- vi. Investigates and reports security breaches.
- vii. Conducts an 'Information Security Assessment' every 3 to 5 years or when major change



- occurs to the organization, technology, business objectives, process, identified threats, possible future threats or external events;
- viii. Ensures that applications and systems have appropriate security measures in place and regularly monitors to ensure that vulnerabilities are identified and resolved;
 - ix. Champions the health organization's security policies, practices, and procedures to ensure alignment with other policies that might already be in place as a result of existing community activities such as Emergency Preparedness Planning;
 - x. Advises management and staff about how security policies, practices, and procedures can be improved and consistent with best practices;
 - xi. Ensures that an evaluation of security impacts is completed for each new request for access to data and identified risks are addressed prior to providing the data.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-4 Security Contact Responsibilities Policy:

Privacy-3 Privacy Contact Responsibilities Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>HO P&S Contacts</i> | <i>Identifies key individuals responsible for privacy and security at the health organization. Provides a quick reference for applicable contacts at the Provincial and Federal level for advice about your privacy and security program and for clarification on the provincial and federal laws around privacy and security.</i> | 1.0 |

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>P&S Job Responsibilities Review</i> | <i>A tool (procedures & checklist) to determine how the primary functions associated with the Data Governance, Privacy and Security accountabilities and responsibilities are reflected in job descriptions for the P&S designates and all staff involved with Personal Health Information 'PHI' or with access to sensitive information.</i> | 1.2 |
| <i>P&S Contact Activity Checklist</i> | <i>Privacy & security checklist including the timing of activities for the Privacy & Security Contacts to monitor and ensure that they are aware of their ongoing accountabilities and responsibilities.</i> | 1.2 |
| <i>Information Security Assessment</i> | <i>The Security Assessment identifies the obligations, scope and any gaps regarding privacy policies and procedures that may require the health organization to create an action item/s.</i> | 1.0 |

X

Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-5: PRIVACY POLICY FOR PERSONAL HEALTH INFORMATION 'PHI'

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization shall ensure that privacy and security guidelines and procedures are in place to manage and protect the client's personal health information 'PHI' that is being collected and used as part of the delivery of health care services. This includes managing a client's wishes as closely as possible if the client gives a consent directive to not allow access to staff or health care provider/s at the organization, as long as it poses no significant risk to the client and/or to others.

This policy supports 'Privacy-1 Statement on Privacy Guidelines and Principles' on how the health organization manages personal health information 'PHI'. Each of the following sections provides details of the policy and the guidelines and principles for the health organization.

1.1 Responsibility for Personal Health Information 'PHI'

The **Health Director** has been designated as the Privacy Contact and is the person responsible for the protection of PHI as described in this policy.

1.2 Identifying Purposes for Which PHI is Collected

The health organization collects PHI only for purposes related to the delivery of health care services as outlined in Privacy-1 Statement on Privacy Guidelines and Principles (poster) that is made available to the public. If other publicly viewed or accessible means are available, the poster is also shared on the health organization website or in brochures that are distributed. The health organization will review this Privacy Statement annually to ensure it is up-to-date.

If PHI that has been collected is needed for a purpose not previously identified, client consent will be obtained unless the new purpose is permitted or required by law and only used for that reason and for the time required.

1.3 Images or Print-outs of PHI

If PHI has been printed out to use for a particular purpose including if a consent directive has been overridden for the purposes of client safety - the print out must not be saved for a later date; it must not be used beyond the particular purpose and time frame after which it must be securely destroyed or marked with the date and purpose on the print out (noting that it is void after the specific timeframe for which it was used).



1.4 Consent for the Collection, Use, and Disclosure of Personal Health Information

The health organization collects PHI directly from the client or from a person acting on the client's behalf.

i. Implied Consent

When a client seeks health care services from a health organization, there is implied consent to collect and use the sensitive information to deliver the care - **unless specifically instructed not to do so by the client** to:

- a. Maintain contact with them about their health care;
- b. Provide ongoing care;
- c. Share and gather information with other health care service providers at other organizations in the client's circle of care (e.g. copies of health records, medication information, lab test results which includes viewing information on electronic record systems/databases/eMRs/cEMRs; noting that when staff discloses personal health information to other health care providers, staff is required to tell those providers when the client's information is inaccurate or incomplete, including when the missing information could affect the client's health care).
- d. Identify and provide the most appropriate health care services and benefits based on eligibility;
- e. Help manage and improve health organization internal health systems planning operations, performance and quality, including sending anonymous client satisfaction surveys that do not have any personal identifiable information that could lead back to the client;
- f. Conduct research (as permitted by law and approved by an appropriate research governing body that do not have any personal identifiable information that could lead back to the client);
- g. To deliver teaching and education;
- h. To provide information as required by law (e.g. court order) if not doing so may cause harm to the client or another person including a minor.

ii. Express Consent

The health organization needs to ask the client for their express consent to collect, keep, use and share information if it is required for a purpose not noted above or as required by law.

iii. Without Consent

Under certain circumstances as permitted by law (e.g. if the health care provider believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious or bodily harm to a person or group of persons, the decision to access a health file can be made without consent of the client, or if the client has given a consent directive to block access to their information.

iv. Withdrawing Consent

A client can withdraw their consent at any time in writing. The health organization is required to provide the client with an appropriate form to fill out and sign to authorize the withdrawal of consent, which is then forwarded to the health organization's privacy contact and filed in the client's health record. The withdrawal cannot apply to past collection, use, or disclosure.

The health organization's privacy contact is responsible to inform staff and those providers within the client's circle-of-care that consent is being withdrawn.

Individuals who may override a withdrawal of consent on a health file include:



- The client or substitute decision maker: An 'Authorization to Disclose Personal Health Information Form' must be completed. This form will be forwarded to the Privacy Contact and kept on file. The privacy contact will ensure that staff and those within the client's circle-of-care are made aware of consent being reinstated and that the reinstatement is documented in the client's health file.
- A health care provider: When a health file for which consent has been withdrawn is accessed by a health care provider, the health care provider is required to notify the privacy contact and client at the first reasonable opportunity and must document the reason for the override in the client's health file.

1.5 Accessing PHI

The health organization ensures that only those people who need to see personal records are allowed to look at them. In addition, the information is protected through administrative policies, specific contracts (such as information sharing agreements 'ISAs' with external agencies), and by adopting appropriate safeguards and security measures.

A client may ask to see the personal information that the health organization has on record about them and if they feel that any information is incorrect or incomplete, can request that it be updated accordingly.

1.6 Limiting Collection of PHI

- The health organization should limit the amount and type of PHI collected to only what is necessary for the **purposes identified in the Privacy Notice**. PHI may include name, date of birth, address, health history, record of visits to a health care provider, and the services received.
- Occasionally, PHI may be collected from other sources if consent has been obtained or if permitted by law.

1.7 Limiting Use, Disclosure, and Retention of PHI

- The health organization will limit use, disclosure and retention of PHI to only what is necessary for the **purposes identified in the Privacy Notice**. Only those individuals that need to use PHI for direct care or administrative purposes are allowed to access client records. Every employee, contractor, student and volunteer signs a confidentiality and acceptable use acknowledgement to protect PHI within the control of the organization. Where appropriate, Information Sharing Agreements 'ISA' with third parties are created when PHI is involved.
- PHI is stored according to the retention, access and transfer of medical records policy of the provincial/territorial College of Physicians and Surgeons, or any information sharing agreements, whichever is the longer period.
- PHI is securely and permanently destroyed following the retention period.

1.8 Accuracy of PHI

Employees, contractors, students and volunteers ('staff') will keep PHI as accurate, complete, and up-to-date as possible for the purposes for which it was collected. All client information is recorded following the documentation standards and guidelines of the provincial/territorial bodies, e.g. College of Nurses.

Clients may request a change to their health file by contacting the Privacy Contact.

1.9 Safeguards for PHI

- The health organization has established safeguards for the PHI in their custody or control. These

safeguards include:

- Physical measures (such as locked filing cabinets);
 - Access policies (such as allowing access to a member of the health team on a least-privilege, need-to-know basis);
 - Technological measures (such as the use of passwords, encryption, and audits);
 - Confidentiality acknowledgements;
 - Contracts containing privacy requirements (e.g., data sharing agreement); and
 - Privacy training.
- ii. All staff, contractors, students, and volunteers are required to follow the safeguards. Failure to follow these safeguards may result in disciplinary actions, up to and including termination of employment.

1.10 Openness about Health Information Privacy and Security Practices

- i. The health information privacy and security practices for PHI are described in the Privacy Notice (poster). The Privacy Notice is posted for public information.

1.11 Client Access to Personal Health information

- i. Clients may request access to their PHI by completing and submitting a request. The health organization should respond to such requests within 30 business days as required by law.

1.12 Questions or Concerns about <insert health organization name> PHI Practices

- i. Questions or complaints about the health organization's PHI practices should be sent to the designated privacy contact and/or the applicable Office of the Privacy Commissioner. Contact information should be provided in the Privacy Notice that is posted for public view.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-5 Privacy Policy for Personal Health Information:

Privacy-1 Statement on Privacy Guidelines and Principles

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':



| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| Withdrawal of Consent template | <i>Provides a tool to document withdrawal of consent by a client.</i> | 1.4 iv. |
| Authorization to Disclose | <i>Provides a means to document a health organization's client consenting to allow disclosure of personal health information 'PHI'.</i> | 1.4 iv. |
| Statement of Disagreement template | <i>Provides a template to use when clients want to contest the decision by the health organization to refuse a requested correction by the client to change their personal health information.</i> | 1.5, 1.8 |
| ISA Guiding Principles | <i>Provides a minimum set of items that should be included in an Information Sharing Agreement 'ISA' in place with another organization.</i> | 1.7 i. |
| Provincial PHI Retention | <i>Provides a quick reference to the provincial retention policies for personal health information 'PHI' / or patient record retention.</i> | 1.7 ii. |
| Poster Templates | <i>Poster design that the health organization can leverage (add logo and health organization name)</i> | 1.10 |
| Request to Access PHI | <i>A tool to help the community members with their request to access their personal health information 'PHI' that can be completed with health organization staff.</i> | 1.11 |

X



Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-6: DATA CLASSIFICATION FOR PERSONAL HEALTH INFORMATION 'PHI' POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

All information assets maintained by the health organization must be classified into one of three levels of sensitivity: Low, Medium or High (e.g. in regard to personal health information 'PHI') to determine its specific sensitivity classification. This classification guides the appropriate management of the information.

1.1 Information Asset Classification

When assigning a classification, consider the potential impacts if the information were disclosed to an unauthorized person(s) and/or organization(s), was lost, or corrupted.

The following table provides a reference to support the classification assessment. It is based on sensitivity classifications consistent with industry best practices.

| Types of Information | Sensitivity Classification |
|--|---|
| Client personal health information | High |
| Aggregated health information | High |
| Client general contact information | Medium |
| Health promotion / education materials / bulletins | Low sensitivity unless it is linked to client health information. If it is linked to a client, it is 'high' |

1.2 Information Storage

Information with the same sensitivity classification must be stored together. In situations where information with different sensitivity classifications is stored in the same location, then the safeguards, assessment and monitoring procedures, and related action plans must be aligned with the highest level of sensitivity classification.

1.3 Sensitivity Classification Examples of Data

The following table describes each level of classification with examples of the data that may be associated with each classification and the privacy and security safeguards that should be in place.



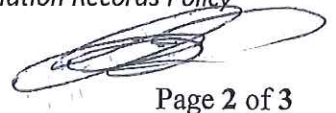
| Sensitivity Classification | Examples of data | Privacy and security safeguards examples |
|--|--|---|
| <p>Low</p> <p>Inappropriate access could cause very little or no injury/harm, such as minor embarrassment</p> | <p>First, middle, and last name of an individual, age and gender</p> <p>For example, perhaps the individual considers their middle name an embarrassment. If disclosed would not likely cause injury/harm but may cause minor embarrassment</p> | <p>Generally, no need to have any safeguards in place.</p> |
| <p>Medium</p> <p>Inappropriate access could cause personal injury or harm, such as identity theft</p> | <p>First, middle, and last name of an individual, age and gender combined with the individual's SIN#, birth date, home address phone number, or personal cell phone number</p> <p>A minimum of five of these pieces of information provide positive identification of the individual</p> | <p>Limited access for authorized staff that requires access to complete their job duties (e.g. staff that provide health care services or support health care programs).</p> <p>Safeguard examples:</p> <ul style="list-style-type: none"> • Locked filing cabinet with policies and procedures for managing locks/keys and establishing audit controls, • Information management system controlled by unique UserID, password, and user access audit policies and procedures. |
| <p>High</p> <p>Inappropriate access could cause extremely serious personal injury or harm, such as suicide, social hardship, loss of employment causing economic hardship, negative impact to personal relationships, illness or increased health risks should the individual decline to seek access to health care services for fear of inappropriate disclosure of information</p> | <p>Client's health file</p> | <p>Limited access for authorized staff using privacy principles of 'need-to-know' and 'least privilege'.</p> <p>Disclosed to other health care providers based on their need to support the health care needs of the client or to protect the health of a population (e.g. preventing or managing communicable diseases).</p> <p>Safeguard examples:</p> <ol style="list-style-type: none"> i. Same as above with audit review procedures supported by a robust privacy and security program that includes an assessment and monitoring process. |

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - It is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-6 Data Classification for Personal Health Information:

Privacy-7 Retention of Personal Health Information Records

Privacy-8 Archiving & Accessing Personal Health Information Records Policy



Privacy-9 Destruction of Personal Health Information Records Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|---------|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>No additional tools currently available</i> | | |
| | | |

X

Ted Roque
Chief

Wahnapiṭae First Nation

PRIVACY-7: RETENTION OF PERSONAL HEALTH INFORMATION 'PHI' RECORDS POLICY

| | |
|--|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTED AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will retain and store all client health files as per the required minimum provincial/territorial retention periods and/or longer as determined by the organization for any special categories of files. All files will be held in a secure location accessible only to authorized people as part of their job duties and role.

1.1 Viewing Client Files

The health organization will consider if a client's file should be stored in one place (i.e. including charts from all health departments – mental health, nursing, NP, COHI, groups etc.) and ensure that only authorized people have access to the files. The health organization will need to ensure that staff are protected from viewing unnecessary information that is not part of their job duties and role.

- Restricted: only those individuals that have approved access to the records have access to them;
- Controlled: the integrity of the records is maintained (e.g. no one can modify a record or group of records and no one can add record(s));
- Tracked: there is a clear audit trail that shows: who accessed the records, which records they accessed, verification to ensure that the records were not modified in any way, and the date and time when records were removed and when they were returned to the archive.

1.2 Time Period

The health organization will need to keep active client files in a secure location and as inactive clients' health files reach the retention period based on the health organization's records retention schedule, arrangements must be made to either store the health files off site, microfilm them, burn them onto a CD, or other electronic form, or destroy them.

Regardless of what process is chosen all appropriate documentation must take place.

1.3 Relocation of Health Files

Should health files need to be removed from the premises either for storage, or processing, secure arrangements must be made for the transportation. For example, engaging a reputable vendor that is aware of the sensitivity of the information and has protocols in place for secure handling.

2.0 ADDITIONAL REFERENCES



All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-7 Retention of Personal Health Information Records Policy:

Privacy-6 Data Classification for Personal Health Information Policy

Privacy-8 Archiving Personal Health Records Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| Provincial PHI Retention | <i>Provides a quick reference to the provincial retention policies for personal health information 'PHI' / or patient record retention.</i> | 1.0 |

X

Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-8: ARCHIVING & ACCESSING PERSONAL HEALTH INFORMATION 'PHI' RECORDS POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCN #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will manage and archive all client health files, both paper and electronic, that are accessed infrequently and store them in a secure location. The specific period of time that deems the records eligible for archiving will be defined by the organization as well as ensuring compliance with the applicable privacy laws on record keeping and archiving. A log of the archived health files will be maintained with a copy of the log kept at the archive location and retained at the health organization facility (if these are two different locations).

1.1 Access and Reviewing Health Files

On a periodic basis as defined by the health organization (e.g. annually or bi-annually), a review will be conducted of all health files, both paper and electronic, to identify those records that may be archived if they have been deemed inactive (e.g. 2-3 years after the most recent recorded activity). The person reviewing the files must be authorized to view PHI as part of their job duties and roles and could be the privacy contact or their designate. The data held about a client should have a sensitivity classification assigned that will help determine who at the health organization may view the file.

The privacy contact and health organization leadership should consider the best strategy of how personal health information, both paper and electronic, is grouped together for a specific client as this will influence storage location, and if the client's data is needed how it will be retrieved.

1.2 Archiving General Guidelines

The health files that are archived will be:

- i. Clearly marked to identify the contents (e.g. include the individual's full legal name (if known) or their alternate name, date of birth and any additional key identifiers to assist in maintaining a clear match between the information contained in the health file and the appropriate individual);
- ii. Stored with records of similar sensitivity level (e.g. records of high sensitivity must not be stored in the same file cabinet or file cabinet drawer or electronic media with records of low sensitivity);
- iii. Retained for the required time period and disposed of appropriately at the end of the retention period. There may be special considerations defined by the health organization to keep records longer than the required time period and those should be marked 'Do Not Destroy'. For example, health records for clients that relate to Residential School inquiries/files may need to be retained indefinitely;



- iv. Records that are subsequently removed from the archives must be returned in a reasonable time (e.g. same business day) or as soon as feasible after that. Those that cannot be returned on the same business day must be stored in a manner appropriate for the sensitivity classification of the information contained in the records.

1.3 Electronic Archiving

The health organization should define specific protocols for archiving and storing digital or electronic health records as part of their overall Information Technology work flow. There are a variety of options, ranging from secure on-site tiered storage within a storage area network (SAN) to off-site storage by a secure and approved cloud service provider.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-8 Archiving & Accessing Personal Health Information Records Policy:

Privacy-6 Data Classification for PHI Policy

Privacy-7 Retention of PHI Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>P&S Health File Archive Log</i> | <i>Tool to help track the health organization's management of archived records - both paper-based and digital.</i> | 1.0 |

X

Ted Roque
Chief

Wahnapitae First Nation

PRIVACY-9: DESTRUCTION OF PERSONAL HEALTH INFORMATION 'PHI' RECORDS POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

Personal health information 'PHI' held beyond the required retention period, can be safely and securely destroyed by the health organization if required. On a regular basis (e.g. annually), health files, that have exceeded the retention period would be flagged for destruction by the health organization privacy contact or their designate with a log of the destroyed health files kept. This policy is applicable to both paper and digital/electronic files.

1.1 Determining which files can be destroyed

The retention period set by the health organization's privacy contact or applicable retention laws will determine which files can potentially be destroyed. There may be a client/community expectation that needs to be considered for certain types of files to be retained indefinitely. For example, client files that have a Residential School aspect may require that the health organization retain those types of files indefinitely.

1.2 Key Guidelines for destroying files

The health organization's privacy contact or their designate will ensure the following guidelines are followed when files are destroyed:

- i. privacy and confidentiality are maintained when health files are destroyed - only those individuals authorized to view the files handle the process;
- ii. only health files held beyond the legally required retention period are eligible to be destroyed;
- iii. health files destroyed at any particular time can be easily identified in a recorded log for potential audit or reference;
- iv. the destruction method must be secure, for example using a cross cut shredder for paper records so that the record cannot be reconstructed, and a formatted full delete is conducted if electronic/digital records.
- v. Any concerns or deviations during the destruction process will be immediately reported to the health organization's privacy contact.

2.0 ADDITIONAL REFERENCES



All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-9 Destruction of Personal Health Information Records Policy:

Privacy-6 Data Classification for PHI Policy

Privacy-7 Retention of PHI Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>P&S Destruction Log</i> | <i>Provides a tool to track the paper-based personal health information held beyond the required retention period that will be safely and securely destroyed.</i> | 1.0 |

X

Ted Roque
Chief

Wahnapi'tae First Nation

PRIVACY-10: DE-IDENTIFYING HEALTH INFORMATION POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will ensure that information collected and subsequently used or disclosed as part of health care reporting or other secondary allowable uses is de-identified as much as possible so that it would not be possible to identify an individual based on the personal health information 'PHI' or sensitive information that is being viewed.

1.1 Personal Health Information

The health organization will adhere to the following two principles around collecting information from a client:

- i. Will not collect, use or disclose information if **other information** (such as de-identified information) would serve the purpose and is available;
- ii. Will not collect, use or disclose information **more than is necessary** for the purpose of delivering health care services.

These two principles apply in every situation even if the client consents. The health organization has a responsibility to limit the collection of PHI as much as possible. When including the information to support reporting or other allowable secondary uses, the goal is to protect the individual's privacy by preventing direct identification or linking information in a way that would break the client's privacy.

1.2 Identifiable Information Description

Identifiable information is information that lets you identify an individual based on the PHI you have about their health or health care. This includes when information could be used either alone or with other information to identify an individual.

Personal information is identifiable information about a person in oral or written form that relates to:

- their physical or mental health;
- the health care provided to them;
- payments or eligibility for health care coverage;
- the donation of body parts or substances;
- is the individual's health card number; or
- Identification of an individual's substitute decision-maker.

In some cases, information from different sources can be combined to identify an individual. For example, in a small community, information about a client's health condition may be combined with the



date that a blood test was done, and this might be enough information to identify the client.

1.3 De-identify Case Example

An example of when the health organization may want to de-identify information is when creating reports to support program funding initiatives so that the data in the report does not inadvertently reveal a client's identity.

1.4 De-identify Strategy Mitigates Risk

De-identifying or limiting the collection of sensitive information can reduce the costs associated with using and archiving data, by reducing the privacy risks associated with inadvertent release (i.e., a data breach) and the consequences of a breach. Having an approach in place for firstly limiting collection and then de-identifying information that is on a client's file is a good strategy for mitigating privacy risks for the health organization.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-10 De-Identifying Personal Health Information Policy:

Privacy-12 Accuracy of Documentation Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>De-identifying PHI</i> | <i>Provides health organization with language that can help explain to staff why de-identifying PHI as much as possible is the goal to mitigate risks around privacy & security.</i> | 1.0 |

X

Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-11: CONSENT POLICY FOR COLLECTING, USING & DISCLOSING INFORMATION

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will follow provincial/territorial consent laws to determine and support decisions for obtaining consents for the collection, use and disclosure of sensitive information including personal health information 'PHI' for clients. The decisions of a substitute decision maker (including a Public Guardian or Trustee) will be accommodated where appropriate and will accommodate the ability to override consent when allowable by law and circumstance. This consent policy applies to adults, minors and infants as outlined applicable laws.

Consent may be provided either as implied consent or express consent. When necessary the health organization privacy contact or designate will seek further guidance from the health organization's legal counsel, or the provincial office of the privacy commissioner if the kind of consent needed for a particular situation is unclear.

1.1 Types of Consent: Express versus Implied Consent

In most cases where staff is required by law to obtain the client's consent, the consent may either be express (written or oral) or implied. However, there are a few circumstances where the consent cannot be implied, and staff must obtain express consent. There are also some use and disclosure situations when additional client consent is not required.

- i. **Implied Consent** occurs when it is assumed that an individual has given consent to the collection, use or disclosure of his/her PHI for the delivery of health care service or treatment. For example, several nurses may share PHI when each is involved in providing care to the client. Each provider in the "circle of care" is relying on implied consent.
- ii. **Express Consent** occurs when the individual is specifically asked for their consent before any collection, use or disclosure of PHI takes place. Express Consent can be obtained in writing or verbally. For example, express consent is required for a family doctor to provide PHI to a life insurance company.

When obtaining a client's express consent, it is important that it be documented. This could be a written consent signed by the client, or a staff member recording the fact that the client gave oral consent. Staff must also follow any standards for documentation of their professional college, other licensing body or the health organization.

1.2 Steps in Consent Management



The health organization will follow these general steps when managing situations that involve client consent for using and disclosing sensitive information:

- i. Check to see that this is a situation in which consent is involved, which means that there is a collection, use or disclosure of PHI;
- ii. Understand the elements of valid consent and what type of consent needs to be obtained, if any (copies of relevant laws should be available for health organization staff to reference);
- iii. Identify who needs to give consent, and ensure the person is capable of giving consent;
- iv. When further questions or concerns arise, further guidance from the health organization privacy contact, health director and potentially applicable provincial Office of Public Guardian and Trustee will be sought and documented.

1.3 When is Consent Required?

Consent is only required when dealing with Personal Health Information 'PHI' and is not meant as consent to allow the actual delivery of health care services to the client. PHI is identifying information about an individual in oral or recorded form, if the information is:

- About the physical or mental health of the individual, including information that consists of the health history of the individual's family;
- About the provision of health care to the individual, including the identification of a person as a provider of health care to the individual;
- Is a plan of service for the individual;
- About payments or eligibility for health care in respect of the individual;
- About the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;
- Is the individual's health number; or
- Identifies an individual's substitute decision-maker.

1.4 What is Consent?

Consent is the permission that a person gives for the collection, use or disclosure of his/her PHI. To be valid, the consent:

- Must be from the individual (or from the appropriate substitute decision-maker, if there is one);
- Must be knowledgeable (which can also be achieved by posting a notice of the health organization's information practices);
- Related to the PHI; and
- Must not be obtained through deception or coercion.

1.5 Who will give the consent?

- i. A capable person has the right to make his/her own decisions about the collection, use and disclosure of PHI.
- ii. If a client has a substitute decision-maker entitled to make decisions under the appropriate provincial/territorial law, this person automatically becomes the substitute decision-maker for information decisions related to the client's PHI.
- iii. If a client does not have a substitute decision-maker for treatment and is incapable of making decisions about the collection, use or disclosure of his/her PHI, staff must turn to the list of

substitute decision-makers identified in provincial/territorial privacy law.

- iv. Documentation of all information regarding the obtaining of all client's consent whether it is verbal, understood, implied or written is crucial.
- v. Clients should understand that they can give a 'consent directive' which may be that they choose not to give consent or block access to PHI to specific individuals, or if given, they can withdraw consent at any time.

1.6 When consent can be overridden?

If a client has blocked access to PHI through a consent directive, this can be overridden by a health organization provider, if the client has given express consent to the individual prior to them overriding their consent directive; OR there is a risk of bodily harm to themselves or bodily harm to other individuals.

This consent override must be documented in the client's health file. The health organization's privacy contact should verify that the override access was appropriate and whether it is necessary to report the override to the provincial office of Privacy Commissioner.

The privacy contact or their designate should also conduct scheduled audits of the consent directives in the health files to ensure that they are still relevant.

1.7 How capacity of a person to give consent is determined.

There will be times when healthcare staff require a clinical decision regarding the ability (or capacity) of a client to give informed consent about their treatment or the collection, use or disclosure of their PHI because there is a doubt that the client is capable of giving consent. Such situations may include when the client has a mental disability or memory impairment, or when the client is a minor child.

If a client's capacity is in question, their capacity should be reviewed by a health professional within the health organization and the results of the assessment recorded in the client's file.

The general rule to follow when obtaining consent is the client's:

- i. ability to understand the information that is relevant to making a decision about the collection, use, or disclosure of PHI; and
- ii. ability to appreciate the probable results ("reasonably foreseeable consequences") of giving or not giving, withholding, or withdrawing the consent.

1.8 Consent on behalf of an incapable person

The following substitute decision-makers have the right to give, withhold, or withdraw consent on behalf of an incapable person:

- i. The individual's guardian of the person or guardian of property (if the guardian has authority to make a decision on behalf of the individual);
- ii. The individual's attorney for personal care or attorney for property (if the attorney has authority to make a decision on behalf of the individual);
- iii. The individual's representative appointed by a consent and capacity board (if the representative has authority to give the consent);
- iv. The individual's spouse or partner;
- v. A child or parent of the individual (unless the parent has only a right of access (visits) to the individual).

- vi. A representative from an organization that is legally mandated to protect children and youth from abuse and neglect (e.g. Children's Aid Society) or other person who is lawfully entitled to give or refuse consent in the place of the parent;
- vii. A parent of the individual with only a right of access to the individual;
- viii. A brother or sister of the individual; and
- ix. Any other relative of the individual.

The Public Guardian and Trustee have discretion to act as the substitute decision-maker only if no one in the list above can fulfil this role.

In a customary care situation, the customary care-giver would be able to provide consent based on their role as a substitute decision-maker under one of the categories in the above list.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-11 Consent for Collecting, Using and Disclosing Information Policy:

Privacy-5 Privacy Policy for PHI

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| Capacity to Provide Consent | <i>Provides a guide/ template to determine if the situation warrants that consent capacity should be determined.</i> | 1.6 |
| Consent Guidelines | <i>Provides examples of consent and to use as a reference when your staff has questions around consent when dealing with personal health information 'PHI'</i> | 1.3 |
| Client PHI Consent | <i>Provides a template to use when a client needs to give their written express consent. This</i> | 1.8 ii. |

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| | <i>includes when the provider/health organization sees a compelling need to override an existing consent directive that is in place and it's appropriate in the circumstance to seek the patient's consent to override the consent directive temporarily.</i> | |

X

Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-12: ACCURACY OF DOCUMENTATION POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will record and maintain accurate and complete documentation in the client's health file that includes and recognizes important personal health information and clinical data to ensure client safety and to provide the ability to communicate to other health care practitioners in the client's circle of care – as well as the client or their representative - as a means of ensuring continuity of assessment and care.

1.1 A client's right to accurate records

All clients seeking health care at the health organization have the right to expect that the health care practitioners and health organization staff are keeping adequate and accurate records related to their health care as an integral part of services provided to clients. Professional clinical standards and regulations along with provincial/territorial laws require that accurate and complete documentation is maintained on charting, reports, certificates and electronic health care records relating to examinations or treatments that were required by the clients or their representatives.

1.2 An accurate and reliable history of care

The client's health file demonstrates accountability for the care given by the health organization and must be kept accurate to:

- i. Answer questions or concerns about the care that was given to the client.
- ii. Determine quality improvement tools to monitor established indicators of the structure, process and outcomes of care and as risk management tools.
- iii. Compile statistical data on client visits and workload at the health organization in order to facilitate capacity and need for staff resources.

1.3 Best Practices to ensure accuracy

The health organization health care providers and staff will use the following principles to ensure accuracy of client information held in their files:

- i. That documentation is done in a timely fashion, is complete, factual and in the client's own words;
- ii. Include data that supports the assessment of conclusions including plans, implementation and evaluation.
- iii. Do not write judgmental statements in a client's health file. Avoid assigning blame, questioning



the competency of another health care provider's assessments and care plan or correcting the health care provider within the content of the client's chart.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-12 Accuracy of Documentation Policy:

Privacy-20 Confidentiality & Acceptable Use Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>Information Accuracy Checklist</i> | <i>Provides a CHECKLIST of how to ensure all sensitive information including personal health information is kept accurate.</i> | 1.0i |

X

Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-13: CLIENT ACCESS AND RELEASE OF 'PHI' POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization shall grant a client access to their own personal health information 'PHI' held by the organization, in accordance with provincial/territorial laws provided that evidence of appropriate documentation and identification is given. If another health organization/s is responsible for the information, the client will be redirected to that organization. The privacy contact or designate will be responsible for handling all requests by clients to review or access their health file and retain a record of the request. This access will be granted in the presence of authorized staff with the appropriate expertise to ensure that both the integrity of the information is maintained, vetting for third-party information is done, as well as to provide clear explanations of medical terminology and health procedures to make the PHI information that is being accessed meaningful to the client. The written or verbal request will be documented in the client's health file.

1.1 Client's right to access not absolute

In the absence of a law, the health organization will have policies and procedures in place to address specific types of PHI requests. Client access includes the right to inspect and to request a copy of the contents of their own health file. However, the Canadian Health Information Management Association 'CHIMA' supports the position that this right to access is not absolute. Under very specific circumstances, when a health care provider can demonstrate sufficient reason for concern, such as harm to the physical or mental health of the client or others, the individual's right may be overridden. In such case of denied access, a mechanism for appeal will be offered to the client.

1.2 Routine and non-routine requests for access and release of PHI

In addition to reviewing PHI with the client, documentation about personal health information 'PHI', including program attendance will be released directly to the client (capable adult or mature minor) requesting it. This may include forwarding a report to a third party at the request of the client.

Routine requests for documentation applies to reports that do not include third party information and include, but are not limited to: immunization records, lab results, and attendance at a health organization clinic or organized program. Routine requests will be processed by frontline staff in the health organization. If it is unclear whether the applicant is authorized to receive the information, the request must be escalated to the privacy contact or their designate to process as a non-routine request.

All other requests for information must be escalated to the privacy contact or their designate and responded to following the rules outlined in applicable release of health information laws.

1.3 Requests on behalf of clients



Requests from providers in the client's circle-of-care, or as permitted by law (e.g. in the form of a subpoena, summons, warrant, police, acting on behalf of a coroner, etc.) to access a client's health file will be dealt with in accordance with the current privacy and release of health information laws. Health privacy laws and regulations must be consulted when deciding to provide access to personal health information. For example, provisions precluding disclosure of information should be applied even when the client has consented to the disclosure. Particular care should be taken when granting access to PHI of a minor or a person who is not mentally competent. Certain provincial/territorial laws recognize the concept of individuals authorized to exercise rights on the behalf of others.

1.4 Client requested corrections

The client may disagree with information collected about them. The client must not be allowed the opportunity to alter, deface or remove any collected information. However, the individual should be permitted to amend the existing information, with a written, signed and dated statement detailing any personal comments. Amendments at the request of the client should be handled as an addendum to the health file, without change to the original entry and should be identified as such.

1.5 Distinguishing type of correction requested by client

The health organization must provide guidelines establishing the difference between erroneous information, for example, an incorrect date of birth and also information that is disputed by the client, for example, documented observations made by the health care provider with which the client does not agree. The means by which errors and disputes are addressed must also be defined by the health organization, in accordance with provincial/territorial laws and standards of practice.

1.6 Timeframe and cost for requests

The standard timeframe for responding to non-routine requests is within 30 working days. Should this time frame not be achievable the privacy contact will provide the client with a written notice of extension that explains when a response will be provided and why the extension is required. An extension cannot exceed an additional 30 days. Typically, a health organization will not charge a fee associated with client requests for information, except for reasonable service fee for time spent if the request has some complexity.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-13 Client Access and Release of PHI Policy:

Privacy-11 Consent Policy for Collecting, Using & Disclosing Information

Privacy-14 Information Corrections and Appeals

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>Request to Access PHI</i> | <i>Provides health organization clients with a means to request timely access to routine and non-routine verification and documents; to provide the health organization's staff with a tool to help the community members with their request to access their personal health information 'PHI'.</i> | 1.0 |
| <i>PHI Access Request LOG</i> | <i>Provides health organization with a LOG to track requests for PHI information from patients or their authorized representative.</i> | 1.0 |

X

Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-14: INFORMATION CORRECTIONS AND APPEALS POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will manage an open and fair process whereby clients or their substitute decision-maker can appeal decisions made about the collection, use and disclosure of their personal health information 'PHI' which includes requests for corrections to their records that have been refused by the health organization.

1.1 Form of the appeal

The appeal should ideally be in writing but may be given verbally. If the appeal is given verbally, it must be transcribed by the receiving staff member and signed by the client/substitute decision-maker. A copy of the appeal whether oral or written must be placed into the client's health file.

1.2 Appeal Process

If a client/substitute decision maker is denied the right to access or correct personal information or disputes a decision made concerning the collection, use and/or disclosure of his/her personal health information, a formal appeal may be made to the health organization's authorized staff (e.g. nurse, community care coordinator). If the authorized staff receiving the complaint is the person who made the original decision or has been involved in the matter under appeal, the appeal shall be transferred to another appropriate health professional for review. The client/substitute decision-maker will be notified of the transfer and the transfer will be noted in the client's health file. The most appropriate staff member will deal with the appeal in accordance with this policy.

The appeal will be reviewed, and the reviewing staff member will examine the situation, collect any necessary information from all available sources and prepare a report of the findings.

- i. The reviewing staff member will share the findings with the client/substitute decision-maker in writing. A copy of the findings and any redress will be included in the client's health file.
- ii. If the appeal is substantiated in whole or in part, the reviewing staff member will outline to the client/substitute decision-maker any steps that will be taken.
- iii. If the appeal is not substantiated the reviewing staff member will advise the client/substitute decision-maker of the right to appeal to the privacy contact and the right to access the office of the Information and Privacy Commissioner at any time. A copy of the investigating staff member's report will be provided to the health organization's privacy contact.
- iv. Should the client decide to appeal to the health organization privacy contact, all investigative documentation and reports will be forwarded to the privacy contact. The privacy contact will



proceed in accordance with the appeal process as outlined above. The decision of the privacy contact shall be final on behalf of the health organization; however, the Privacy Contact will advise the client/substitute decision-maker of the right of access to the office of the Information and Privacy Commissioner.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-13 Client Access and Release of PHI Policy:

Privacy-11 Consent Policy for Collecting, Using & Disclosing Information

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>Provincial Legislation</i> | <i>Provides a quick reference to your provincial legislation and whom you can contact for help.</i> | 1.2 iii. |
| <i>Statement of Disagreement</i> | <i>Provides the health organization with a template to use when clients want to contest the decision by the health organization to refuse a requested correction by the client to change their personal health information.</i> | 1.0 |


 Ted Roque
 Chief

Wahnapiatae First Nation

PRIVACY-15: SENDING AND RECEIVING SENSITIVE INFORMATION POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will take the utmost care to protect personal health information 'PHI' when sending, receiving and handling sensitive information about a client by any means which may include electronic methods like emailing, faxing, texting as well as paper-based methods like internal health organization mail and external mail via Canada Post and any courier services utilized by the health organization. The health organization will commit to choosing the lowest risk method for sending and receiving client sensitive information.

1.1 EMAILING / TEXTING

The health organization's email /mobile phone systems (unsecured service or secured [encrypted service]) are utilized to improve service to clients and partners, enhance internal communications, and reduce paperwork. Email system users will follow all relevant policies and protocols to ensure that confidentiality of client information is maintained. All staff will ensure that when Emailing (or texting) about, or to a client, that personal health information is not contained within the actual body of the email or text. Unsecured emails or texts are not an appropriate substitute for in-person appointments or over-the-telephone communication. Texting may be used by health organization staff depending on the context of the community being served. Email/texting privacy and security risks will be mitigated by the following protocols:

- i. Use extreme caution to ensure that the correct email address is used for the recipient(s).
- ii. Personal email accounts may not be used to support delivery of any health organization programs or services unless specifically authorized in advance.
- iii. Email messages must contain professional and appropriate language at all times.
- iv. Chain messages should be deleted immediately without sending on to others.
- v. Save email messages as directed by authorized support personnel.
- vi. Never use a client's full name within the body of the email and even using initials should be avoided if possible as in smaller communities the clients identify could be ascertained by the combination of the information in the email and their initials.
- vii. Use the client's health file number (if available) to identify them. If a client does not have a health file number, a combination of their initials and date of birth could be used with caution exercised so that the information details are put in a separate email or attached in a document that is password protected.
- viii. Use general language without any client identifiable information in the body of the email and attach a word or excel document that is password protected (encrypted) – once sent following up with a phone call to the receiver to provide them with the password so they can open up the attachment,



- or provide a separate email containing only the password.
- ix. With the approval of health organization management staff email can be used to share information regarding a client on a 'need to know' basis. The client's health file number (if available) will be used to identify them. Such email must be clearly marked "Confidential."
 - x. Should a staff member not know the client's health file number they must contact their clinical support staff to obtain the correct number.
 - xi. Any message or file sent via email must have the user's name and contact information attached.
 - xii. Any message or file sent via email must have a Confidentiality Statement at the bottom of the email.
 - xiii. Health organization staff should use only organizational issued mobile devices, if possible, that employ safeguards like passwords. If using a personal device, use only Canadian cell plan providers like Telus, Rogers or Bell to ensure any data transmitted is stored inside Canada.
 - xiv. Verify the identity of the intended recipient when texting them for the first time.
 - xv. Treat texts as temporary communications (similar to phone calls) and document any significant texts in the client's file.

1.2 FAXING

Sending and receiving PHI by fax increases the risk that it will fall into the wrong hands, so care must be taken by all health organization staff when choosing fax as a method of transmission. For example, a wrong fax number could accidentally be dialed, sending information to the wrong person or if a receiving fax machine is unattended, PHI may be viewed by unauthorized individuals at the health organization. Keep in mind the following general guidelines to mitigate risks:

- i. Staff should consider whether a fax is the best way of sending confidential information. Is it possible to send the information via courier or another method of secure file transfer?
- ii. Ideally, any fax machine used to send or receive PHI should be kept in a closed area to prevent unauthorized persons from seeing the documents.
- iii. Don't leave confidential documents unattended. Consider making a clinical person responsible for the fax machine. Otherwise, clinical staff should send their own faxes to limit the chances that others will see PHI. Ideally, staff should arrange a time to receive faxes containing PHI, so they can be at the machine when the fax arrives.
- iv. If possible, set up the fax machine to require the receiver to enter a password before the document will be printed. This ensures that only the intended receiver can retrieve the document.
- v. If a client asks for his or her PHI to be faxed elsewhere, explain how faxing PHI can result in accidental disclosure or interception.

1.3 PAPER MAIL

When confidential client information is to be mailed externally from the health organization or when it is received at the health organization to be distributed through the health organizational internal mail system, the information should be safeguarded in every possible way.

The health organization may want to consider the following procedures for handling paper mail.

- i. A copy of the information to be mailed is to be put into an sealed envelope with the recipient's name clearly documented on the outside of the envelope and CONFIDENTIAL is to be written or stamped on the envelope. This envelope is then to be put in a second envelope that has the recipient's name and complete mailing address on it. The outgoing mail logbook is to be completed.
- ii. If mail is received at the health organization, it should be recorded as received in a secure log and delivered to the recipient as soon as possible. If it is marked 'confidential' it should remain unopened.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-15 Sending & Receiving Sensitive Information Policy:

Privacy-20 Confidentiality and Acceptable Use Policy

Security-1 Information Security Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|---|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| Sending/Receiving PHI | <i>Provides further information for some of the methods of transmission that may be used for sending/receiving personal health information about a client.</i> | 1.2 |
| Confidential & Acceptable Use Acknowledgement template | <i>Provides a template to leverage - for contractors, students and volunteers (i.e. deemed as 'staff') working with the health organization - to read, acknowledge and sign to ensure all sensitive information held is protected.</i> | 2.0 |


Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-16: SOCIAL MEDIA POLICY

| | |
|--|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF AMENDMENT AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will ensure that employees, contractors, students and volunteers ('staff') separate their personal activities and use of all publicly accessible social media hosted for or by the organization so that they do not conflict with or could reasonably be seen to reflect negatively on the professional image of the organization and/or its staff.

1.1 **Organization social media** - Social media in context to this policy means publicly-accessible social media that includes, but is not limited to: program websites, health organization email, staff personal websites, email, text messages, blog posts, Twitter and Facebook. In some situations, it may be necessary to use some form of social media as a means of communicating with a client or to initiate programs on behalf of the health organization, in which case the following guideline is recommended:

- Set up the account following a naming convention (e.g. a nurse practitioner would be "HO -NP") that is separate from the service providers personal account. Also ensure the privacy settings are high, no posts can be made on their page, and friend lists are hidden.

1.2 **Staff personal social media** - The following guidelines should be followed by the organization's service providers who are active on their own personal social media accounts to protect the reputation of the health organization and the trust of the community being served:

- i. Never accept a request from a client or program participant in that person's chats, blogs or social networking groups; or accept a "friend" or similar request from a client or program participant;
- ii. Never use photos, logos or images of the health organization, its clients, employees, contractors, students, volunteers or programs;
- iii. Never discuss the health organization operations, decisions or activities in chat rooms, on blogs or social networking sites; and/or,
- iv. Never make derogatory, negative or defamatory statements about the health organization clients, employees, contractors, students, volunteers or others accessing the health organization or its services.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-16 Social Media Policy:



Media Policy:

Privacy-20 Confidentiality and Acceptable Use Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| Confidential & Acceptable Use template | <i>Provides a template to leverage - for contractors, students and volunteers (i.e. deemed as 'staff') working with the health organization - to read, acknowledge and sign to ensure all sensitive information held is protected.</i> | 2.0 |



Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-17: PROGRAM AUDIT BY A THIRD-PARTY POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will comply with authorized requests to conduct an audit of specific programs or services for the purposes of accreditation, to review an accreditation, or to comply with the audit requirements of established agreements. This includes chart reviews/audits for health service providers including those with professional designations. The authorized individual that is to conduct the audit or review must not remove any records of sensitive information from the health organization's premises.

- 1.1 The individuals authorized to conduct the audit or review must sign the health organization's confidentiality and acceptable use acknowledgement and the privacy contact or their designate will confirm that individuals performing the audit or review have been authorized to complete it.
- 1.2 Any personal health information 'PHI' must be provided as de-identified information to protect the data being viewed. (Refer to the Privacy-10 'De-identifying Personal Health Information Policy'). Include the minimum amount of sensitive information required to support the audit or review.
- 1.3 Maintain a master list that maps the identified client health file to the de-identified client information. This provides the ability for staff to look up the client health file should questions be raised by the individuals conducting the audit or review or additional client details are required to support the audit or review.
- 1.4 The privacy contact or their designate will review the terms of the planned audit or review to confirm that it explains the purpose and process for the audit or review and is in alignment with an agreement that requires it.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-17 Program Audit By a Third-Party Policy:

Privacy-20 Confidentiality and Acceptable Use Policy

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document



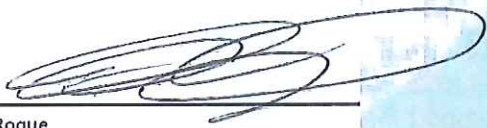
'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|---|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| Confidential & Acceptable Use template | <i>To provide the health organization with a means to ensure all sensitive information is protected by all employees, contractors, students and volunteers (i.e. deemed as 'staff') to acknowledge and sign the Confidentiality & Acceptable Use Acknowledgement document.</i> | 2.0 |

X



Ted Roque
Chief

Wahnapiatae First Nation

PRIVACY-18: WHISTLE BLOWER PROTECTION POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will ensure that clients, providers, staff, contracted resources and volunteers are encouraged to report possible privacy breaches (e.g. actual or suspected unauthorized access, activity, misuse of data or inappropriate disclosure of data, etc.) and provide reassurance that the individual reporting it will not experience any negative repercussions or retaliation.

- 1.1 The health organization will not dismiss, suspend, demote, discipline, harass, withdraw services, cancel contracts, withhold pay, reduce pay or hours, withdraw benefits, deny overtime or promotion or otherwise disadvantage anyone acting in good faith who reports a possible privacy breach which may or may not be malicious.
- 1.2 A person (i.e. complainant) who has reasonable grounds to believe that retaliation has occurred, must file a retaliation complaint either orally or in writing to the health organization's privacy contact within a reasonable time following the retaliatory action (e.g. within 30 days).
- 1.3 A complaint of retaliation must allege that the complainant engaged in activity protected by the whistle blower provisions (such as reporting possible inappropriate access), the organization knew about or suspected that activity, the organization subjected the complainant to an adverse action or threatened such action, and the protected activity motivated or contributed to the adverse action.
- 1.4 The privacy contact will interview the complainant to determine the need for an investigation into the complaint of retaliation. It is very important that a complainant respond to such contact. If a complainant is unresponsive, the retaliation complaint investigation cannot proceed, and the retaliation complaint will be dismissed. The privacy contact will work with the complainant, management and staff involved in the retaliation complaint investigation to ensure there is a fair and equitable discussion of the complaint and the response to it. If evidence supports the individual's claim of discrimination or retaliation, the privacy contact will work with management and staff to ensure that appropriate restitution occurs.
- 1.5 Complaints cannot be filed anonymously. The identity of the complainant must be provided as part of the retaliation complaint investigation activities. However, the retaliation complaint investigation must be documented, and details only disclosed as/when necessary to support the investigation and its outcomes.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-18 Whistler Blower Protection Policy:

Security-7 Incident Response Policy


3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| Incident Reporting Template | <i>Provides a template to record any privacy incidents either revealed by the proactive Privacy Access Audit process and or any privacy and security incident that needs to be documented – can be leveraged by a 'whistle blower' to report an suspected incident or breach.</i> | 1.2 |


Ted Roque
Chief

Wahnapitae First Nation

PRIVACY-19: INFORMATION DATA RESEARCH POLICY

| | |
|---|--------------------|
| ADOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

POLICY

The health organization will manage all research requests involving personal health information 'PHI' that are received in writing and have them reviewed by the organization's privacy contact and the individuals in the health organization that have oversight of the source of the data being requested. Use of any information for research that would involve the identification of any individual client will not be permitted without the written, informed, and express consent of each individual involved.

- 1.1 **Individual identifiable data:** if written informed consent is provided from each individual involved in the research request, the health organization's privacy contact or their designate will ensure that the individual or their authorized representative fully understands and agrees to the nature of the research and all uses of the data.
- 1.2 **De-identified individual data:** research can occur without client consent provided the data is truly de-identified and inference cannot occur. For example, data that includes age groups within a small population may make it possible to infer the identities of the individuals in the given age group.
- 1.3 **First Nation Community information:** research cannot occur on identifiable or de-identifiable individual or summarized data where a First Nation community then becomes identifiable without the express permission of the First Nation community. This is to ensure that ethical and culturally competent health research involving First Nation people is maintained.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-19 Information Data Research Policy:

Privacy-1.1 Consent Policy for Collecting, Using & Disclosing Information




3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document 'Privacy & Security Implementation Workbook' ('Workbook') that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization's 'Action Plan' also housed in the 'Workbook':

| Privacy & Security Implementation Workbook | | |
|--|---|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| <i>Consent Guidelines</i> | <i>Provides examples of consent and to use as a reference when your staff has questions around consent when dealing with personal health information 'PHI'.</i> | 1.0 |
| <i>Client PHI Consent Template</i> | <i>Provides a template to use when a client needs to give their written express consent.</i> | 1.0 |


Ted Roque
Chief



Wahnapi'tae First Nation

PRIVACY-20: CONFIDENTIALITY AND ACCEPTABLE USE POLICY

| | |
|---|--------------------|
| ASOPTED BY BAND COUNCIL MOTION | BCM #WFN 18/19-013 |
| DATE OF ADOPTION AT CHIEF AND COUNCIL MEETING | MAY 8, 2018 |
| APPROVAL REVIEW AND REVISION DATES: | Every 3 years |

1.0 POLICY

The health organization will ensure that all employees, contractors, students and volunteers (staff) read, understand and sign a 'Confidentiality and Acceptable Use Acknowledgement' that obligates them to adhere to all organization policies that safeguard personal health information 'PHI' and uphold the reputation and trust of the health organization in the community at large.

The document shall be completed for each person prior to them using the health organization's information and technical assets such as computer software and devices (email system, network, Internet/Intranet access) used when delivering programs and services on behalf of the health organization. The signed document will be completed and filed and should be renewed annually at the minimum. Staff who violate this policy and/or use the health organization's information and electronic assets for improper purposes will be subject to disciplinary action, up to and including dismissal.

- 1.1 **Personal Responsibility** - The health organization management recognizes that many employees, contractors, students and volunteers need access to an email system, a network connection, Internet/Intranet access, and computer software and devices while working on behalf of the organization - and will provide this access to the user - that has acknowledged their responsibilities for provisioning this access.

The Confidentiality and Acceptable Use Acknowledgement document that is signed by all users substantially covers all privacy and security aspects that need to be formally acknowledged as follows:

- i. Privacy and security awareness training has been received;
- ii. Understanding that accessing only information required for job duties is allowed;
- iii. Accessing the user's own personal information including family and friends without proper authorization is not permitted;
- iv. Accuracy and completeness in collecting and recording data is always maintained;
- v. Userid and Password constitutes a personal 'signature';
- vi. Use of the health organization's network and internet is a privilege, not a right;
- vii. Only software authorized by the organization should be used.
- viii. If a health professional, applicable regulatory body credentials will be maintained;
- ix. There are banned activities when using health organization electronic services like downloading unauthorized software, making, sending or forwarding defamatory, offensive or harassing



statements, etc.

- 1.2 **Reporting misuse or possible privacy and security breaches** – Each person when accepting an account and password for any electronic device or service agrees to follow all policies regarding their use including a commitment to report any misuse or policy violation(s) to their supervisor or the health organization’s privacy contact or their designate.
- 1.3 **Reasonable personal use** - Employees, contractors, students and volunteers will be permitted ‘reasonable personal use’ provided the personal use is fairly minimal. For example, employees are permitted to send personal emails, or to access their bank account online.
- 1.4 **Information ownership** - All information created, sent, or received using the health organization’s electronic services is the property of the health organization. Users should have no expectation of privacy regarding this information. The health organization reserves the right to access, read, review, monitor, or copy all messages and files on its computer systems at any time and without notice. When deemed necessary, the health organization reserves the right to disclose text or images to law enforcement agencies or other third parties without the user’s consent.
- 1.5 **Information security** – Security-1 ‘Information Security’ policy includes additional information regarding the security obligations of employees, contractors, students and volunteers ‘users’ have, specific to information and electronic assets. Users should review and understand this policy as most aspects contained in Security-1 are incorporated into the ‘Confidentiality and Acceptable Use Acknowledgement’ document that they are required to sign.

2.0 ADDITIONAL REFERENCES

All policies are interrelated and have some similar content - it is highly recommended that you review and become familiar with these other policies which will provide a richer context to the Privacy-20 Confidentiality and Acceptable Use Policy:

Security-1 ‘Information Security Policy’

3.0 POLICY - ACTION ITEMS

Action Items referencing the set of tools (forms, templates, checklists) available in the excel document ‘Privacy & Security Implementation Workbook’ (‘Workbook’) that are used to implement the policy if the health organization decides to implement the policy as written. These tools can also be leveraged if the health organization already has protocols and tools in place that may need augmentation.

The action items/tools listed may also be referenced in other policy/s action item lists as all privacy and security policies have interrelated content.

These action items will be recorded in the health organization’s ‘Action Plan’ also housed in the ‘Workbook’:

| Privacy & Security Implementation Workbook | | |
|---|--|------------------------------------|
| Action Item TAB-Tool | Purpose | Policy content section it supports |
| C&A Use Acknowledgement Template | <i>Provides a template to leverage - for contractors, students and volunteers (i.e. deemed as 'staff') working with the health organization - to read, acknowledge and sign to ensure all sensitive information held is protected.</i> | 1.0 |
| User Access Template | <i>Provide Eight (8) forms to track/manage the health organization users' access to digital systems as well as physical environments in your organization.</i> | 1.0 |



Ted Roque
Chief

