**<enter Health Organization name>**

<enter logo>

Privacy and Security

Policy and Procedures Manual

**MIS Version: 2.5**

**May 2018**

Permission to Reproduce & Adapt Content

The privacy and security policies contained in this document may be reproduced, in part or in whole and by any means, without warranty of any kind, whether express or implied. If adapted to a health organization needs, the intent of each policy cannot be changed and must remain true to the original policy meaning. The author does not make any warranties about the completeness, reliability and accuracy of any adapted policies.

Warranty Disclaimer

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

Limitation of Liabilities

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

How this Document is Organized

There are 4 different levels of Privacy and Security policies that a health organization might need to put in place to protect sensitive information associated with the delivery of health care services to a client. This includes clinical services as well as delivery of programs like mental health, addictions and counselling:

Level 1 Health Services documentation using paper methods

* Policies to protect the privacy, confidentiality, and accuracy of paper records.

Level 2 Health Services documentation using a local electronic medical record system

* Policies to protect the privacy, confidentiality, and accuracy of electronic records.

Level 3 Connecting with provincial/regional systems to view or contribute information:

* Policies to support sharing of information with partners external to the site.

Level 4 First Nation based data governance

* Policies to integrate privacy in the context of a First Nation’s comprehensive data governance framework (e.g. to meet requirements such as Ownership, Control, Access and Possession (OCAP), secondary use, lands and resources, etc.).

Privacy and Security policies in this document are intended to address Level 1 and Level 2 requirements for a health organization governed by private sector privacy legislation. The policies and tools included in the P&S Toolkit have been designed to support the health organization’s implementation of OCAP Principles. It also includes policies to address those Level 3 requirements that were known at the time of publication.

This document provides:

1. An explanation of what is considered Personal Health Information ‘PHI’ and applicable to the set of privacy and security policies herein.
2. A Table of Contents listing the Policies linked to the policy page.
3. An introduction and explanation of the recommended framework that the health organization should use to establish a robust privacy and security culture. (Sections ‘A’, ‘B’, ‘C’)
4. A set of approved Privacy and Security policies that can be used either as stand-alone policies or in their entirety (each policy has a recommendation and approval section). (Privacy:1-20, Security:1-9)

The policies are written in jargon free language to address fundamental privacy and security laws that are applicable to any provincial or territorial health organization across Canada, recognizing that specific provincial or territorial requirements may need to be added to a policy/s. For example:

* Policy Privacy-2 ‘HIC’ is specific only to the province of Ontario so would not be used by a health organization in any other province or territory.
* Policy Privacy-3 ‘Privacy Contact Responsibilities’ can be leveraged by all health organizations with a customization added for the province of British Columbia that both a Data Steward and Data Custodian need to be designated.

*Refer to the P&S Implementation Workbook* ***TAB*** *‘****Provincial Legislation’*** *that provides links to each province’s specific legislation for consideration to customize this manual to the health organization location.*

4.1 Each Policy has 3 sections:

**Section 1.0** ‘Policy’ - that sets out the policy content for legislative compliance.

**Section 2.0** ‘Additional References’ - that provides a list of other interrelated policies.

**Section 3.0** ‘Policy Action Items’ - that lists Action Items relevant to a set of tools (forms, templates, checklists) available in the ‘Privacy & Security Implementation Workbook’ that are used to help implement the policy. Noting that the Action Item/tool may be applicable to one or more policies and therefore may appear more than once throughout the policies.

* These action items will be recorded in the health organization’s ‘Action Plan’ also housed in the ‘Privacy & Security Implementation Workbook’.

*Noting that the ‘Action Plan’ should be regularly monitored by the health organization for progress and completion to meet the implementation timeline.*

* Once the Action Plan is populated with the tools that the health organization will implement to support the adoption of the relevant policy – Section 3.0 can be **removed** from the Policy Manual.

4.2 Strategy for implementing Policies – see section ‘C. Implementing Privacy & Security Policies and Procedures’ that describes the implementation strategy available to help the health organization ensure P&S compliance.

|  |
| --- |
| To personalize this document to the health organization:  Use the ‘Search in Document’ function to find: **“<enter health organization name>”** and ‘replace all’ with the Health Organization Name. |

PROTECTING PERSONAL HEALTH INFORMATION ‘PHI’

The policies and procedures contained in this document are designed primarily to protect personal health information ‘PHI’ at the health organization based on federal and provincial laws. The policies can easily be extended to apply to other sensitive and confidential information that the health organization may manage such as financial information about a client or client.

Each province / territory has enacted their own privacy act/s. The law that applies to the health organization is the one applicable to a private sector organization.

Because the health organization may need to collaborate with other health care partners in a client’s circle of care who may be considered public sector and therefore may be governed by different legislation – there will always be a degree of judgement and balance that needs to be applied when deciding what is considered PHI and how it is protected to truly meet the needs of the clients and community.

All employees, contractors, volunteers, students (‘staff’) and anyone privy to sensitive information associated with the health organization needs to be aware of the policies and procedures in this document.

1. **What is considered PHI about a client or client?**

Within the context of the health organization generally PHI is considered:

* Recorded information, either on paper or digitally, about an identifiable individual that forms part of the delivery of services by the health organization to the individual. (e.g. demographic and/or financial information evident on paper forms, notes, reports or visible system screens/current or archived database files showing an individual’s name, address, blood type, educational history, employment history, birth date, eye colour, gender, race and other such personal information);
* Sensitive and private Information about an individual that is spoken and may be overheard (e.g. a provider may be discussing a client’s health situation in an area of the health organization that is not private or sound proofed);
* Separate unidentifiable items of seemingly innocuous information that when put together, would allow someone to accurately infer information about an individual (e.g. in a small community an unauthorized person may see a client’s initials on a list left at reception for a prenatal workshop – which may allow the person seeing the list to identify the person who is pregnant in the community);

*Refer to the Implementation Workbook* ***TAB ‘PHI Guidelines’*** *for a more detailed list*

1. **What is NOT considered PHI?**

Within the context of the health organization, information not considered PHI and therefore not applicable to the policies and procedures in this document is:

* Information that enables an individual (meaning staff, volunteers, contractors, etc.) to be contacted, including the individual's contact name, job title, business address, business phone number, business email, business fax number, and other such business information.

**CONTENTS**

A. Key Privacy and Security Standards 9

B. Canada-Wide Privacy Laws 11

C. Implementing Privacy & Security Policies and Procedures 13

D. Implementing P&S Policies and Procedures for National Expansion Project 14

PRIVACY-1: STATEMENT ON PRIVACY GUIDELINES AND PRINCIPLES 16

PRIVACY-2: (ONTARIO) - HEALTH INFORMATION CUSTODIAN ‘HIC’ RESPONSIBILITIES 19

PRIVACY-3: PRIVACY CONTACT RESPONSIBILITIES 22

PRIVACY-4: SECURITY CONTACT RESPONSIBILITIES 25

PRIVACY-5: PRIVACY POLICY FOR PERSONAL HEALTH INFORMATION ‘PHI’ 28

PRIVACY-6: DATA CLASSIFICATION FOR PERSONAL HEALTH INFORMATION ‘PHI’ POLICY 33

PRIVACY-7: RETENTION OF PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY 36

PRIVACY-8: ARCHIVING & ACCESSING PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY 38

PRIVACY-9: DESTRUCTION OF PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY 40

PRIVACY-10: DE-IDENTIFYING HEALTH INFORMATION POLICY 42

PRIVACY-11: CONSENT POLICY FOR COLLECTING, USING & DISCLOSING INFORMATION 44

PRIVACY-12: ACCURACY OF DOCUMENTATION POLICY 49

PRIVACY-13: CLIENT ACCESS AND RELEASE OF ‘PHI’ POLICY 51

PRIVACY-14: INFORMATION CORRECTIONS AND APPEALS POLICY 54

PRIVACY-15: SENDING AND RECEIVING SENSITIVE INFORMATION POLICY 56

PRIVACY-16: SOCIAL MEDIA POLICY 59

PRIVACY-17: PROGRAM AUDIT BY A THIRD-PARTY POLICY 61

PRIVACY-18: WHISTLE BLOWER PROTECTION POLICY 63

PRIVACY-19: INFORMATION DATA RESEARCH POLICY 65

PRIVACY-20: CONFIDENTIALITY AND ACCEPTABLE USE POLICY 67

SECURITY-1: INFORMATION SECURITY POLICY 1

SECURITY-2: MOBILE DEVICES POLICY 8

SECURITY-3: INFORMATION TECHNOLOGY ASSET MANAGEMENT POLICY 10

SECURITY-4: BUSINESS CONTINUITY MANAGEMENT PLAN POLICY 12

SECURITY-5: USER ACCESS AND ACTIVITY AUDIT POLICY 14

SECURITY-6: PRIVACY & SECURITY INCIDENT RESPONSE POLICY 18

SECURITY-7: ORGANIZED OFFICE 22

SECURITY-8: AUDIO/VIDEO SURVEILLANCE 24

SECURITY-9: CLOUD-BASED DELIVERY OF SERVICES POLICY 26

INTRODUCTION - FRAMEWORK

## Key Privacy and Security Standards

This ‘Privacy and Security Policies and Procedures Manual’ was developed for health organizations to help foster a culture of privacy and security and is based on widely-accepted Canadian standards and legislation.

* **Canadian Standards Association ‘CSA’ Model Code for the Protection of Personal Health Information ‘PHI’**

The CSA Model Code balances the privacy rights of individuals with the information requirements of organizations collecting the information. The 10 commonly accepted principles found in the CSA Model Code that guide the protection of personal health information ‘PHI’ are listed in the following table:

| **10 Principles for the Protection of PHI** | |
| --- | --- |
| 1 | **Accountability**  Each health organization that collects PHI must put at least one person in charge of making sure their privacy policies and practices are respected and followed. |
| 2 | **Identifying Purposes** Clients must be told why their PHI is being collected when or before it is collected. |
| 3 | **Consent** Clients must agree (or “consent”) to the collection, use and disclosure of their PHI. Consent can be withdrawn at any time. |
| 4 | **Limiting Collection** Only PHI that is required for the identified purposes should be collected. |
| 5 | **Limiting Use, Disclosure and Retention** PHI can only be used or disclosed for the identified purposes. Added consent is required for any other purposes. PHI should only be kept as long as necessary for the identified purposes. |
| 6 | **Accuracy** PHI must be as accurate, complete and up-to-date as possible to minimize any risk of errors in decisions or PHI disclosure about a client. |
| 7 | **Safeguards** Health organizations must protect PHI from inappropriate use by establishing security safeguards to prevent loss, theft, unauthorized access, disclosure, copying, use or modification. |
| 8 | **Openness** Health organizations must make their privacy policies and procedures easily available and visible to clients. |
| 9 | **Individual Access** Clients have the right to ask to see their PHI, know who has access to their PHI and any disclosure of their PHI. They can question the accuracy of their PHI and ask for corrections. |
| 10 | **Challenging Compliance** Health organizations must deal with any inquiries, challenges or complaints from clients about the organization’s privacy practices and principles around PHI. |

* **ISO 27002 Code of practice for PHI security management.**

The key document that guides security standards for PHI in Canada is ISO 27002. It was developed by the International Standards Organization ‘ISO’. The ISO recommends 11 “best practices” for the protection of confidentiality, integrity, and availability of PHI - listed in the following table:

| **11 Best Practices for the Protection of PHI** | |
| --- | --- |
| 1 | **Security Policy** Each health organization should develop a written information security policy to protect PHI being collected. |
| 2 | **Organization of Information Security**  Assign responsibility to an individual/s to maintain security and to control use of PHI including liaison with external authorities on security matters when required. |
| 3 | **Asset Management** Identify someone to manage information and communication technology ‘ICT’ equipment “assets”, such as computers and smart phones by using an inventory checklist or system to classify and track these assets as well as defining ‘Acceptable Use’ policies for employees. |
| 4 | **Human Resources Security** Ensure security before, during, and at the end of employment for all employees, contractors, students, and volunteers. Make sure that individuals know about their obligations to maintain PHI security. |
| 5 | **Physical and Environmental Security** Secure areas and protect the facility that houses PHI and ICT. Protect equipment from risk of loss or damage and have a ‘Clean Desk and Clear Screen’ policy. |
| 6 | **Communications and Operations Management** Develop and use operational procedures and monitoring that ensure PHI, network, and systems security is maintained. |
| 7 | **Access Control** Control access to PHI, networks, applications and operating systems. Ensure that staff are using strong passwords and keep them confidential. |
| 8 | **Information Systems Acquisition, Development and Maintenance** Build security into information technology systems and software, do regular system maintenance and change control. |
| 9 | **Information Security Incident Management** Have procedures and protocols in place for managing security incidents to report, assess, respond to and learn from. |
| 10 | **Business Continuity Management** Use business continuity management to protect PHI in the event of disasters or other hazards. |
| 11 | **Compliance** Identify legal, contractual and security policy requirements and perform regular reviews to make sure the rules are being followed. |

## Canada-Wide Privacy Laws

1. **First Nation Laws**

Each First Nation in Canada has jurisdiction to create their own laws, including privacy laws. A First Nation that has passed its own privacy law would have to review the law to see how it applies to their PHI management and operations.

If a First Nation does not have a First Nation law relevant to privacy or PHI, then the provincial/territorial privacy law applies to guide appropriate PHI collection, use and disclosure. Many health organizations use provincial/territorial privacy laws as their key guide for protection of PHI privacy.

1. **Provincial/Territorial Privacy Laws**

Each province and territory in Canada has enacted their own privacy law. This law applies to a person or organization providing health care services, including First Nations, if there is no applicable First Nation law.

*Refer to the P&S Implementation Workbook* ***TAB ‘Provincial Legislation’*** *to reference privacy and security laws and contact information for the Office of the Information and Privacy Commissioner for each province.*

Provincial/territorial privacy laws set the *requirements* for the collection, use, and disclosure of ‘PHI’ ‘but deems governance as the responsibility of each health organization. Specifically, a health organization is required to:

* be responsible for staff, contractors, students, or volunteers who collect, use or disclose PHI on their behalf;
* designate a Privacy Contact; (privacy is hand-in-hand with security);
* have a public written statement that explains how PHI is collected, used and disclosed;
* keep accurate records of PHI and create protocols for clients who request access to their PHI or request corrections if they believe there is an error;
* describe the circumstances in which PHI can be disclosed both internally and externally (to third parties);
* provide protocols for client consent and the use of substitute decision-makers;
* promote sharing PHI in appropriate ways so that clients can receive and benefit from integrated health services; and
* identify the responsibility and relationship with the provincial/territorial Information and Privacy Commissioner to make sure their health organization is aware of privacy requirements and current directions.

1. **Federal Privacy Law**

The Privacy Act is the federal law that regulates how federal departments and agencies handle personal information (which can be interpreted as PHI for health organizations).

The *Privacy Act* applies to Health Canada employees in the performance of their duties in a health facility. As an example, First Nation Inuit Health Branch ‘FNIHB’ nurses working at a health facility in a remote and isolated community would be subject to the *Privacy Act*, while community-employed health staff within the same facility would follow the applicable provincial/territorial privacy law.

The federal *Privacy Act* is very similar to provincial/territorial privacy law. It requires health care providers and staff to:

* Only collect PHI directly related to a federal program or service (for its intended purpose/s);
* If possible, inform clients about the purpose for which PHI is collected;
* Use PHI only for the purpose it was collected. Most of the time the individual needs to give their consent for any other use; and
* Not disclose PHI under their control, unless the client gives consent.

## Implementing Privacy & Security Policies and Procedures

There are 5 key steps to develop and implement robust privacy and security policies and practices. Completing these steps is not a one-time activity, but rather a continuous model for quality improvements around privacy and security practices to help foster a privacy and security culture at the health organization. If a health organization is embarking on a major new initiative like adding an eHealth solution (e.g. Mustimuhw cEMR) these steps must be completed:

Step 1. **Assess**

Step 2. **Address**

Step 3. **Review**

Step 4. **Approve**

Step 5. **Implement**

*Refer to the P&S Implementation Workbook* ***TAB ‘The Five Steps’*** *to review the details involved with each Step.*

Before you begin at Step 1. **Assess,** the first activity is to designate both a Privacy Contact and a Security Contact. Depending on the capacity at the health organization, the privacy contact may also be the person responsible for security because privacy and security are interdependent. The privacy contact may be a Health Director, Community Health Nurse, or another trusted individual with responsibility for health care. The security contact designate is often the person responsible for information technology at the health organization.

*Refer to the P&S Implementation Workbook* ***TAB ‘HO P&S Contacts’*** *to document the designates for the health organization.*

Some health organizations may also decide to set up a ‘Privacy Security Committee’ or ‘Privacy Security Working Group’ to assist in reviewing and revising policies and procedures when required – but ultimately the privacy/security contact is responsible for leading the adoption and use of the policies and associated procedures to foster a culture of privacy and security at the health organization.

*Refer to the P&S Implementation Workbook* ***TAB ‘P&S TOR’*** *for a sample Terms of Reference* that can be leveraged for this working group or committee.

## Implementing P&S Policies and Procedures for National Expansion Project

The following process checklist provides the privacy/security contact with the strategy and overall process involved for privacy and security regarding the Mustimuhw Information Solutions National Expansion Project.

**Step 1. Assess’ process**

* 2-hour Assessment Workshop with the health organization’s privacy/security contact - the health organization will be provided with a P&S implementation overview presentation and guided through completing a ‘Privacy & Security Assessment’ that will help identify any policy gaps and specific Action Items to be completed to ensure privacy & security legislation compliance.
* All Action Items and ‘Next Steps’ with target completion dates arising from the 2-hour assessment workshop will be documented for the health organization in their ‘Action Plan’ in the health organization’s Privacy & Security Implementation Workbook. The action plan will be provided to the privacy/security contact following the workshop. (Note that in some cases more than one workshop may be necessary in order to complete the Assessment).
* The privacy and security contact will also receive the P&S Policy Manual that should be reviewed by the health organization to help identify any further gaps. Additional gaps would be entered into their ‘Action Plan’. Any questions that arise should also be noted in the Action Plan for review at subsequent scheduled meetings.
* 1-hour Check-in meeting/s can be scheduled to track progress that support the implementation path. The ‘Policy Implementation Checklist’ housed in the Privacy & Security Implementation Workbook should be updated accordingly to ensure that the required P&S policies are in place to allow the health organization to sign the attestation or ‘go live’ letter.

**Policy Groupings**

Each policy has been assigned to an 'Implementation Priority Group' to indicate the priority order in which policies should be adopted or identified within existing policies gaps closed. All policies are important, but the groupings provide guidance on the order in which implementation should occur.

|  |  |
| --- | --- |
| **Priority Group** | **Timeline for Implementation** |
| A | Within 1 month after completing Privacy & Security Assessments |
| B | 6 months after completing Privacy & Security Assessments |
| C | 12 months after completing Privacy & Security Assessments |

A checklist is provided which can be used to show at a glance the status of the adoption of the privacy and security policies from the Policy Manual and the supporting practices/tools from the Workbook.

*Refer to the P&S Implementation Workbook* ***TAB ‘How To Implement a P&S Program?’*** *for the seven steps to follow to implement a P&S program or enhance an existing program.*

*Refer to the P&S Implementation Workbook* ***TAB ‘Policy Implementation Checklist’*** *for a checklist that can be leveraged to show the status of the implementation of the privacy and security policies and the recommended grouping of the policies to simplify implementation*.

**<enter health organization name>**

# PRIVACY-1: STATEMENT ON PRIVACY GUIDELINES AND PRINCIPLES

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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:

1. only ask for PHI that is needed for the indicated purposes;
2. only use or share PHI for the purposes for which it was provided, unless required to do so by law;
3. keep PHI only as long as required by provincial regulations and/or special territorial requirements;
4. be transparent about sensitive information that may be collected and managed by secure third parties;
5. keep PHI accurate and up-to-date, allow only authorized people to see PHI;
6. commit that client sensitive information will be protected under provincial or territorial laws.
   1. **Statement/Poster Messaging**

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

1. installing posters in visible prominent areas in the health organization facility (e.g. clinics, lobby, etc.)
2. 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:

* **<enter health organization name>** values the trust you have placed in us. We respect your personal privacy and do our best to safeguard its confidentiality and security.
* **<enter health organization name>** understands the sensitivity of your personal health information. We are committed to protecting your privacy.
* When you receive care and services from **<enter health organization name>**, we will collect, use and share your personal health information for these reasons:
* To identify and keep in contact with you about your health care
* To provide ongoing care
* To support the provision of care by health care partners
* To help us plan, monitor and improve our care and services to you
* To understand your eligibility for benefits and services
* Where relevant to support billing to medical services
* To analyze, manage and control disease outbreaks and monitor the overall health of people
* Conduct research (as permitted by law and approved by an appropriate research governing body)
* To deliver teaching and education
* As required by law (e.g. court order, reportable conditions)
* **<enter health organization name>** complies fully with the privacy principles as established by the Canadian Standards Association ‘CSA’ and as enshrined in our <provincial/territorial - select which one applies> privacy laws <insert name/s of relevant Acts>.
* Understanding Implied Consent

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

* Understanding Expressed Consent

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

* That all **<enter health organization name>** staff and volunteers are trained on the appropriate collection, use and disclosure of sensitive information
* You are entitled to enquire about privacy and to request access to your personal information; to do so please ask to contact our Privacy Officer<enter contact name, and contact information such as address, email address, phone number) or the office of the Privacy Commissioner <enter contact name, and contact information such as address, email address, phone number>.
  1. **Privacy & Security Feedback from a Client**

If a client has any questions, comments or complaints about the health organization’s privacy policies and procedures, the privacy & security contact information for **<enter health organization name>** must be readily available and provided. This includes the privacy contact’s name, job title, office location, telephone number and email.

As part of their service and best practice protocols, the health organization’s privacy contact will provide the client with contact information for the applicable Provincial Office of the Information and Privacy Commissioner.

1. **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-1 Statement on Privacy Guidelines and Principles Policy:

*Privacy-5 Privacy Policy For PHI*

1. **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 |
| *Poster Templates* | *Poster design that the health organization can leverage (add logo and health organization name)* | 1.1 |
| *Provincial Legislation* | *Provides applicable provincial/territorial Office of the Information and Privacy Commissioner contact information.* | 1.2 |

**<enter health organization name>**

# PRIVACY-2: (ONTARIO) - HEALTH INFORMATION CUSTODIAN ‘HIC’ RESPONSIBILITIES

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **Health Information Custodian ‘HIC’ Responsibilities:**

1. Identify a Privacy Contact responsible for following PHIPA rules, and responding to questions, access or correction requests, and complaints;
2. Limiting the collection, use, and disclosure of PHI to only what is necessary to meet the purposes identified in the Privacy Notice;
3. Making a Privacy Notice available that describes PHI practices;
4. Ensure that the client is provided with the contact information for eHealth Ontario if the relevant personal health information is under the ownership and control of eHealth Ontario or another health organization (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);
5. Ensure that for all eHealth Ontario electronic systems (even view-only HICs) receive and process client consent directives no later than 4 days and send the request to eHealth ONTARIO to apply these consent directives (eHealth Ontario will process within 7 days).
6. Ensure that if a client requests access to their PHI or wants to apply a consent directive that is not under the care of the HIC, that the individual will be re-directed to the relevant HIC/organization and notify eHealth ONTARIO.
7. Ensure that all privacy incidents and breaches are reported to eHealth ONTARIO by the end of the next business day after becoming aware of them.
8. Following steps to ensure PHI is accurate;
9. Maintaining physical, technical, and administrative controls to keep PHI safe and support secure disposal;
10. Developing a process to manage user accounts so only authorized users providing health care services or other approved activities have access to PHI;
11. Providing access to or correction of a client’s PHI upon written client request, subject to some exceptions (PHIPA Sections 52 and 55);
12. Developing policies and procedures to support the collection, use, and disclosure of PHI including privacy or security breaches, record keeping and destruction; and
13. Notifying affected individuals of privacy breaches.
14. Attest annually that the HIC remains compliant with the all obligations of their Privacy and Security Policies.
    1. **Inquiries and Complaints**

Inquiries and complaints that are related to PHI maintained by <enter health organization name> 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. The HIC’s public privacy poster (including website page/s) must have the eHealth Ontario contact information.

* 1. **Annual self-attestation of compliance to HIC responsibilities**

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

* 1. **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. **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.

1. **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*

1. **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 |
| *Attestation to Compliance* | *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.* | 1.3 |

**<enter health organization name>**

# PRIVACY-3: PRIVACY CONTACT RESPONSIBILITIES

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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 <enter health organization name>.

* 1. **Knowledge**

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

* 1. The health organization’s approved privacy policies and procedures;
  2. Applicable provincial/territorial privacy laws;
  3. First Nation privacy laws, if applicable;
  4. Privacy principles and guidelines;
  5. How to protect individual and community privacy in aggregate formats, such as community reports.
  6. **Key Responsibilities**

The privacy contact will actively handle the following responsibilities:

1. Help staff follow established privacy policies and procedures to ensure health organization remains compliant
2. Intervenes on privacy-related issues when required and is available to staff to provide advice and answer privacy related questions;
3. 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;
4. Investigates and reports privacy breaches;
5. Responds to questions from leadership and management regarding how PHI is managed, protected and disclosed.
6. 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;
7. 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;
8. 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;
9. 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;
10. 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;
11. 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;
12. Conducts scheduled audits of the consent directives to ensure that they are still appropriate.
13. Responds to client questions, complaints, access, and correction requests related to information practices;
14. 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;
15. Advises management and staff about how privacy policies, practices, and procedures can be consistent with applicable privacy obligations and privacy best practices;

1. **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*

1. **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** |
| *HO P&S Contacts* | *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.* | 1.0 |
| *P&S Job Responsibilities Review* | *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.* | 1.2 |
| *P&S Contact Activity Checklist* | *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.* | 1.2 |
| *Information Privacy Assessment* | *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)* | 1.0 |
| *Action Plan* | *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.* | 1.0 |

**<enter health organization name>**

# PRIVACY-4: SECURITY CONTACT RESPONSIBILITIES

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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 <enter health organization name>.

* 1. **Knowledge**

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

1. The health organization’s approved security policies and procedures;
2. Applicable provincial/territorial privacy laws;
3. First Nation security laws, if applicable;
4. Security principles and best practices;
5. The health organization’s security policies and procedures.
   1. **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

* + 1. Intervenes on security-related issues when required and is available to staff to provide advice and answer security related questions;
    2. 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;
    3. Responds to security questions and complaints from clients and clients;
    4. 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;
    5. Identifies security training, assessment tools, and awareness opportunities for staff;
    6. Investigates and reports security breaches.
    7. 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;
    8. Ensures that applications and systems have appropriate security measures in place and regularly monitors to ensure that vulnerabilities are identified and resolved;
    9. 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;
    10. Advises management and staff about how security policies, practices, and procedures can be improved and consistent with best practices;
    11. 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.

1. **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*

1. **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** |
| *HO P&S Contacts* | *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.* | 1.0 |
| *P&S Job Responsibilities Review* | *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.* | 1.2 |
| *P&S Contact Activity Checklist* | *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.* | 1.2 |
| *Information Security Assessment* | *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.* | 1.0 |

**<enter health organization name>**

# PRIVACY-5: PRIVACY POLICY FOR PERSONAL HEALTH INFORMATION ‘PHI’

|  |  |
| --- | --- |
|  | Page 1 of 5 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**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. **Responsibility for Personal Health Information ‘PHI’**

The <Provide Title> has been designated as the Privacy Contact and is the person responsible for the protection of PHI as described in this policy.

* 1. **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. **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. **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.

1. 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:

1. Maintain contact with them about their health care;
2. Provide ongoing care;
3. 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).
4. Identify and provide the most appropriate health care services and benefits based on eligibility;
5. 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;
6. 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);
7. To deliver teaching and education;
8. 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.
9. 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.

1. 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.

1. 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. **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. **Limiting Collection of PHI**

1. 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.
2. Occasionally, PHI may be collected from other sources if consent has been obtained or if permitted by law.
   1. **Limiting Use, Disclosure, and Retention of PHI**
3. 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.
4. 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.
5. PHI is securely and permanently destroyed following the retention period.
   1. **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. **Safeguards for PHI**

1. 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.

1. 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. **Openness about Health Information Privacy and Security Practices**
2. 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. **Client Access to Personal Health information**
3. 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. **Questions or Concerns about <enter health organization name>** **PHI Practices**
4. 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 for the health organization’s Privacy Contact must be provided in the Privacy Notice that is posted for public view.
5. **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*

1. **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*** | *Provides a tool to document withdrawal of consent by a client.* | 1.4 iv. |
| ***Authorization to Disclose*** | *Provides a means to document a health organization's client consenting to allow disclosure of personal health information 'PHI'.* | 1.4 iv. |
| ***Statement of Disagreement template*** | *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.* | 1.5, 1.8 |
| ***ISA Guiding Principles*** | *Provides a minimum set of items that should be included in an Information Sharing Agreement 'ISA' in place with another organization.* | 1.7 i. |
| ***Provincial PHI Retention*** | *Provides a quick reference to the provincial retention policies for personal health information 'PHI' / or patient record retention.* | 1.7 ii. |
| ***Poster Templates*** | *Poster design that the health organization can leverage (add logo and health organization name)* | 1.10 |
| ***Request to Access PHI*** | *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.* | 1.11 |

**<enter health organization name>**

# PRIVACY-6: DATA CLASSIFICATION FOR PERSONAL HEALTH INFORMATION ‘PHI’ POLICY

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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. **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. **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** |
| --- | --- | --- |
| Low  Inappropriate access could cause very little or no injury/harm, such as minor embarrassment | First, middle, and last name of an individual, age and gender  For example, perhaps the individual considers their middle name an embarrassment. If disclosed would not likely cause injury/harm but may cause minor embarrassment | Generally, no need to have any safeguards in place. |
| Medium  Inappropriate access could cause personal injury or harm, such as identity theft | 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  A minimum of five of these pieces of information provide positive identification of the individual | 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).  Safeguard examples:   * 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. |
| High  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 | Client`s health file | Limited access for authorized staff using privacy principles of ‘need-to-know’ and ‘least privilege’.  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).  Safeguard examples:   1. Same as above with audit review procedures supported by a robust privacy and security program that includes an assessment and monitoring process. |

1. **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

1. **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** |
| *No additional tools currently available* |  |  |
|  |  |  |

**<enter health organization name>**

# PRIVACY-7: RETENTION OF PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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. **Time Period**

The health organization will need to keep active client files in a secure location andas 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. **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.

1. **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*

1. **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*** | *Provides a quick reference to the provincial retention policies for personal health information 'PHI' / or patient record retention.* | 1.0 |

**<enter health organization name>**

# PRIVACY-8: ARCHIVING & ACCESSING PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**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 timethat 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. **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. **Archiving General Guidelines**

The health files that are archived will be:

1. 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);
2. 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);
3. 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 that 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;
4. 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. **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** |
| ***P&S Health File Archive Log*** | *Tool to help track the health organization's management of archived records - both paper-based and digital.* | 1.0 |
|  |  |  |

**<enter health organization name>**

# PRIVACY-9: DESTRUCTION OF PERSONAL HEALTH INFORMATION ‘PHI’ RECORDS POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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. **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:

1. privacy and confidentiality are maintained when health files are destroyed - only those individuals authorized to view the files handle the process;
2. only health files held beyond the legally required retention period are eligible to be destroyed;
3. health files destroyed at any particular time can be easily identified in a recorded log for potential audit or reference;
4. 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.
5. 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** |
| ***P&S Destruction Log*** | *Provides a tool to track the paper-based personal health information held beyond the required retention period that will be safely and securely destroyed.* | 1.0 |

**<enter health organization name>**

# PRIVACY-10: DE-IDENTIFYING HEALTH INFORMATION POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **Personal Health Information**

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

1. Will not collect, use or disclose information if **other information** (such as de-identified information) would serve the purpose and is available;
2. 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. **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. **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. **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** |
| ***De-identifying PHI*** | *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.* | 1.0 |

**<enter health organization name>**

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

|  |  |
| --- | --- |
|  | Page 1 of 5 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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.

1. ***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.
2. ***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. **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:

1. 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;
2. 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);
3. Identify who needs to give consent, and ensure the person is capable of giving consent;
4. 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. **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. **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. **Who will give the consent?**

1. A capable person has the right to make his/her own decisions about the collection, use and disclosure of PHI.
2. 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.
3. 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.
4. Documentation of all information regarding the obtaining of all client’s consent whether it is verbal, understood, implied or written is crucial.
5. 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. **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. **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:

1. ability to understand the information that is relevant to making a decision about the collection, use, or disclosure of PHI; and
2. ability to appreciate the probable results (“reasonably foreseeable consequences”) of giving or not giving, withholding, or withdrawing the consent.
   1. **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:

1. 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);
2. 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);
3. The individual’s representative appointed by a consent and capacity board (if the representative has authority to give the consent);
4. The individual’s spouse or partner;
5. A child or parent of the individual (unless the parent has only a right of access (visits) to the individual).
6. 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;
7. A parent of the individual with only a right of access to the individual;
8. A brother or sister of the individual; and
9. 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*** | *Provides a guide/ template to determine if the situation warrants that consent capacity should be determined.* | 1.6 |
| ***Consent Guidelines*** | *Provides examples of consent and to use as a reference when your staff has questions around consent when dealing with personal health information 'PHI'* | 1.3 |
| ***Client PHI Consent*** | *Provides a template to use when a client needs to give their written express consent. This 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.* | 1.8 ii. |

**<enter health organization name>**

# PRIVACY-12: ACCURACY OF DOCUMENTATION POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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. **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:

1. Answer questions or concerns about the care that was given to the client.
2. Determine quality improvement tools to monitor established indicators of the structure, process and outcomes of care and as risk management tools.
3. Compile statistical data on client visits and workload at the health organization in order to facilitate capacity and need for staff resources.
   1. **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:

1. That documentation is done in a timely fashion, is complete, factual and in the client’s own words;
2. Include data that supports the assessment of conclusions including plans, implementation and evaluation.
3. 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** |
| ***Information Accuracy Checklist*** | *Provides a CHECKLIST of how to ensure all sensitive information including personal health information is kept accurate.* | 1.0i |

**<enter health organization name>**

# PRIVACY-13: CLIENT ACCESS AND RELEASE OF ‘PHI’ POLICY

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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. **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. **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. **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. **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. **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** |
| ***Request to Access PHI*** | *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'.* | 1.0 |
| ***PHI Access Request LOG*** | *Provides health organization with a LOG to track requests for PHI information from patients or their authorized representative.* | 1.0 |

**<enter health organization name>**

# PRIVACY-14: INFORMATION CORRECTIONS AND APPEALS POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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. **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.

1. 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.
2. 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.
3. 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.
4. 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-14 Information Corrections and Appeals 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** |
| ***Provincial Legislation*** | *Provides a quick reference to your provincial legislation and whom you can contact for help.* | 1.2 iii. |
| ***Statement of Disagreement*** | *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.* | 1.0 |

**<enter health organization name>**

# PRIVACY-15: SENDING AND RECEIVING SENSITIVE INFORMATION POLICY

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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:

1. Use extreme caution to ensure that the correct email address is used for the recipient(s).
2. Personal email accounts may not be used to support delivery of any health organization programs or services unless specifically authorized in advance.
3. Email messages must contain professional and appropriate language at all times.
4. Chain messages should be deleted immediately without sending on to others.
5. Save email messages as directed by authorized support personnel.
6. 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.
7. 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.
8. 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.
9. 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.”
10. Should a staff member not know the client’s health file number they must contact their clinical support staff to obtain the correct number.
11. Any message or file sent via email must have the user’s name and contact information attached.
12. Any message or file sent via email must have a Confidentiality Statement at the bottom of the email.
13. 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.
14. Verify the identity of the intended recipient when texting them for the first time.
15. Treat texts as temporary communications (similar to phone calls) and document any significant texts in the client’s file.
    1. **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:

1. 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?
2. 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.
3. 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.
4. 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.
5. 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. **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.

1. 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.
2. 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** | *Provides further information for some of the methods of transmission that may be used for sending/receiving personal health information about a client.* | 1.2 |
| **Confidential & Acceptable Use Acknowledgement template** | *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.* | 2.0 |

**<enter health organization name>**

# PRIVACY-16: SOCIAL MEDIA POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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 guidelines are 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.
* If video footage or still images are intended to be captured from health organization hosted group events you must have a publicly visible Group Release Form posted that anyone attending the event can clearly see and read, and ideally publicly advise prior to the event that there will be cameras at the event for the purposes of capturing footage and images of the event for possible use on the health organization’s website and social media pages. If specific individuals are featured in the captured footage or images the health organization intends to use - an Individual Release Form must be completed that is signed by the individual before any images, voice or name of the individual is published on the health organization’s website or social media pages.
  1. **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:

1. Never accept a request from a client or program participant in that person’ chats, blogs or social networking groups; or accept a “friend” or similar request from a client or program participant;
2. Never use photos, logos or images of the health organization, its clients, employees, contractors, students, volunteers or programs;
3. Never discuss the health organization operations, decisions or activities in chat rooms, on blogs or social networking sites; and/or,
4. Never make derogatory, negative or defamatory statements about the health organization clients, employees, contractors, students, volunteers or others accessing the health organization or it’s 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:

*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** |
| **Group Release Form**  *(in P&S Posters word document for ease of use)* | *Provides a template to leverage when video footage or images are captured at health organization group events that may be intended for publication on the health organization website or social media pages.* | 1.1 |
| **Individual Release Form**  *(in P&S Posters word document for ease of use)* | *Provides a template to leverage when video footage or images are captured of a specific individual (i.e. interview or individual is prominently featured) at health organization events that may be intended for publication on the health organization website or social media pages.* | 1.1 |
| **Confidential & Acceptable Use template** | *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.* | 2.0 |

**<enter health organization name>**

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

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. 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.
  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.
  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.
  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** | *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.* | 2.0 |

**<enter health organization name>**

# PRIVACY-18: WHISTLE BLOWER PROTECTION POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. 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.
  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).
  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.
  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.
  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 Whistle 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** | *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.* | 1.2 |

**<enter health organization name>**

# PRIVACY-19: INFORMATION DATA RESEARCH POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**1.0 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. **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.
  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 incudes age groups within a small population may make it possible to infer the identities of the individuals in the given age group.
  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-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** |
| ***Consent Guidelines*** | *Provides examples of consent and to use as a reference when your staff has questions around consent when dealing with personal health information 'PHI'.* | 1.0 |
| ***Client PHI Consent Template*** | *Provides a template to use when a client needs to give their written express consent.* | 1.0 |

**<enter health organization name>**

# PRIVACY-20: CONFIDENTIALITY AND ACCEPTABLE USE POLICY

|  |  |
| --- | --- |
|  | Page 1 of 3 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **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. **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:

1. Privacy and security awareness training has been received;
2. Understanding that accessing only information required for job duties is allowed;
3. Accessing the user’s own personal information including family and friends without proper authorization is not permitted;
4. Accuracy and completeness in collecting and recording data is always maintained;
5. Userid and Password constitutes a personal ‘signature’;
6. Use of the health organization’s network and internet is a privilege, not a right;
7. Only software authorized by the organization should be used.
8. If a health professional, applicable regulatory body credentials will be maintained;
9. 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. **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.
   2. **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.
   3. **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.
   4. **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*** | *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.* | 1.0 |
| ***User Access Template*** | *Provide Eight (8) forms to track/manage the health organization users' access to digital systems as well as physical environments in your organization.* | 1.0 |

**<enter health organization name>**

# SECURITY-1: INFORMATION SECURITY POLICY

|  |  |
| --- | --- |
|  | Page 1 of 7 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**1.0 POLICY**

The health organization will ensure that an effective information security program is implemented to safeguard sensitive information involved with the delivery of health care services and programs. This includes access and activity on all computer devices, networks and software related to electronic health data and information including password management. Every employee, contractor, student and volunteer (staff) who has access to and deals with sensitive information on paper or in health management systems will be made aware of the program to protect themselves, the health organization’s reputation to establish community trust.

Staff who fail to follow this policy will result in temporary or permanent suspension of access to the information and systems, and include disciplinary action up to and including termination, cancellation of contractual arrangement, as well as civil and criminal action. If a user is unsure about how to comply with any aspects of the established security program, they should contact their immediate supervisor or the organization’s security contact or their designate.

* 1. **Health Organization Operations – involved persons**

The health organization is dependent in many ways on information and health information management systems, so information security should be a team effort. If sensitive information is unavailable, unreliable, or disclosed improperly, the organization and the clients could suffer serious harm or loss.

Operational responsibilities of all users to help prevent and respond to different types of threats to information and information systems include unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use. All employees, contractors, students and volunteers must treat these security measures as confidential.

* 1. **Involved Systems**

This policy applies to all computer devices and network systems owned by and/or administered by the health organization, as well as any personal devices if authorized to be used for work. It applies to all platforms (operating systems), all computer sizes (from personal digital assistants through to servers), and all software (whether developed by the organization or purchased from third parties). The policy covers only information handled by computers and/or networks. Although this document mentions other forms of information such as voice and paper, it does not directly address the security of information in these forms.

* 1. **Security Program Management and Operations**

Responsibility for the security program management is assigned to the organization’s security contact and management team. The security program management process follows the requirement for appropriate separation of duties. For example, the person requesting access to information cannot be the person approving the request.

* 1. **Authorized Support Personnel Responsibilities**

The organization’s security contact and authorized support personnel are responsible for the following functions that support the security program:

* Act with “Administrator” privileges on all computers. Ensure that end users do not have Administrator privileges unless authorized by the health organization’s management team;
* Manage the security of the computer network and infrastructure;
* Ensure that a record is kept of users that have keys, fobs, passcodes or alarm codes for secure areas;
* Ensure that a record is kept of all information and information technology assets;
* Ensure that user roles and access privileges are reviewed at least once a year to ensure that they are still appropriate for each user’s job function;
* Ensure that background reference checks are performed on individuals prior to granting user access to secure areas or systems;
* Ensure that all users have signed the ‘Confidentiality and Acceptable Use Acknowledgement’ prior to receiving access to information and information systems and annually thereafter;
* Enable and disable user accounts on direction from the organization’s management team. In particular, accounts must be disabled within 24 hours of the end of the user’s relationship with the organization;
* Ensure that firewalls are used on portable devices and dedicated internet links (ADSL, Cable);
* Manage all computer equipment installations, disconnections, modifications, repairs, servicing and relocations;
* Ensure that users back up data on personal computers and laptops, including documents, contact lists, and email messages. All backups containing critical or confidential information must be stored at an approved off-site location with physical access controls or encryption;
* Ensure that all software used to carry out the business of the organization is appropriately licensed;
* As applicable, ensure that Virtual Private Network (VPN) Split tunnelling is disabled;
* Ensure that current virus detection software is installed on all technology assets including mobile devices, operating correctly, and configured to automatically update daily;
* Identify the encryption tools to be used when PHI is stored on laptop computers and for secure transmission by email. Assist users with the use of encryption;
* Ensure that software is updated on a regular or automatic basis. In particular, recommended security patches are installed for the operating system and other applications in use;
* Monitor the computer network for unauthorized access, viruses, spyware and other security breaches;
* Ensure that all user access to systems is automatically logged with the user’s login name, date and time of access, the system / application accessed, and the action taken.
* Ensure that computer access logs are saved securely for a period in accordance with the organization’s policy for retention (e.g. for a minimum of two years);
* Ensure that clinical files are saved securely for a period in accordance with the organization’s policy for record retention;
* Investigate any alleged misconduct in consultation with the organization’s management team. All investigations will be performed on a case-by-case basis.
* Document procedures for key business processes such as system backup and restore, software upgrades, patch management, etc.
  1. **Physical and Access Location Security**

Access to every office and room in the health organization that contains confidential (non-public) information is physically restricted to only people who have a need to know. The organization’s security contact or their designate should establish physical key/fob management protocols for all employees, contractors, students and volunteers accessing the physical areas in the organization that contain sensitive information.

* Authorized users will be given keys or door pass codes to allow access to secure areas of the health organization. Key computer system components have battery backup to protect equipment and information if there is a power failure.
  1. **User IDs and Passwords**

Each staff member, contractor, student or volunteer accessing the health organization’s computer systems has a unique user identification (user ID) and a private password. User IDs are used to limit access to the system based on the job duties and role of each user. Each worker is personally responsible for his or her user ID’s and passwords and no master password list should be maintained by any staff member or IT service provider. The following protocols should be followed:

* User ID’s & Passwords

Passwords are personal to each authorized user. There are no shared accounts. Users may not access computers or networks anonymously, such as by using “guest” user IDs.

* Easy to remember but difficult to guess passwords

To minimize the risk of unauthorized access and maintain password confidentiality, user passwords should be easy to remember but hard for others to guess. Passwords must not be related to the user’s job or their personal life. For example, the following should not be used as passwords:

* User’s address, spouse’s name or licence number; or
* Single words including names, places, slang words or technical terms.

Password controls should be in place to support the principle of passwords being difficult to guess. As much as possible, these controls are managed automatically. For example, passwords are set to expire every 3-6 months so that users have to change their passwords frequently to ensure security.

* 1. **Release of Information**

Unless it has been specifically designated as public information, all information maintained by the health organization must be protected from disclosure. This includes client demographic data (such as name and address), contractual and employment information, and data in summary form (such as immunization coverage reports). All release of information (except public information) must be approved. Such information releases may include questionnaires, surveys and interviews, but does not include client requests for access to their own information or a person for whom they are a substitute decision maker.

* 1. **Network Infrastructure Security**

Only authorized devices will be permitted to access the organization’s network. Wireless access points, peer-to-peer wireless connections and Wi-Fi personal devices of any kind must not be connected to the network without management approval. Network devices connected to the computer network must not be modified, disconnected or relocated without management approval.

* Health organization management reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security or other concerns to the organization’s network.
* Health organization management, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be allowed or banned.
* Users may have access via the network to PHI, employee records, financial information and other confidential information. All access to such information must be authorized and used only for conducting the business of the health organization.
  1. **Internet Access**

Employees, contractors, students and volunteers are provided with internet access if needed to perform their job functions. Such access may be terminated at any time at the discretion of the worker’s supervisor. Internet use is monitored to ensure that workers do not visit internet sites unrelated to their work and for potential security issues.

Specific authorization is required in advance for workers to do the following:

* Represent the health organization in internet discussion groups or other forums; or
* Post any information (including public information) managed by the organization to the internet.

All information received from the internet should be treated cautiously unless the source has been confirmed to be reliable.

* 1. **Electronic Mail**

Employees, contractors, students and volunteers who use computers for their work are given an email address. It is recommended that email communication on behalf of the health organization use the email address issued by the organization. The use of personal email addresses is not recommended.

* A standard email “signature” (authorized by the organization’s management team) that includes the user’s full name, job title, address, and phone number, along with a privacy statement should be used.
* Sending sensitive information in the body of an email should not be done. If email is used the recommended approach is to 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 – once sent following up with phone call to the recipient providing the password.
* When sending emails to groups of recipients, the blind carbon copy (Bcc) feature or a distribution list should be used to avoid revealing the email addresses of other recipients. Sound judgment must be used when distributing messages. Client-related messages should be carefully guarded and distributed to only the essential people. Staff must also abide by copyright laws, ethics rules, and other applicable laws.
  1. **Computers, Laptops, Peripherals, Media/mobile Devices Device Security**

The following security program measures apply to the use of all computer equipment provided by the health organization, and should be made known to staff, contractors and volunteers by the health organization’s security contact or their designate:

* All computer equipment and mobile devices including peripheral portable storage should be kept away from obvious hazards such as direct cold, heat, smoke and liquids;
* Only authorized organization support personnel are permitted to service electronic equipment and devices;
* All computer equipment must have proper physical security mechanisms in place (i.e. be protected by key locks and cables and/or alarms or stored in a security locked and hazard-free location) when not in use or left unattended or in open areas to avoid risk of theft.
* The security contact or their designate must ensure that data on computers and laptops is backed-up. All backups containing critical or confidential information must be stored at an approved off-site location with physical access controls or encryption.
* All computers and portable devices (e.g., laptops and cell phones) that access the network and/or data must be password protected.
* Automatic password protected screen savers must be used with timeout periods appropriate to the sensitivity of the data being accessed (For example, the more sensitive the information, the faster a screen saver should activate during periods of inactivity).
* Computers must not be left logged on when unattended or at the minimum should be locked or shut down completely when not in use. The automatic log off must be set to run after a short period of inactivity;
* Any computer device displaying confidential information must be positioned out of public view.
* Users must ensure that confidential information is not left unattended on desks or on computer screens unless the doors and windows into the room where the computers are located are locked.
* Users are not provided with administrator privileges on any computer system, with the exception of authorized support personnel and any individuals authorized by the organization’s management team.
  1. **Remote and Mobile Usage of Computers, Laptops, Peripherals, Media and Mobile Devices**

Staff, contractors, and volunteers should follow all protocols in the previous section 1.11 when using equipment remotely. Additionally, with remote usage, requirements also include the following:

* Personal mobile devices must not be connected to the network without management approval;
* Users must not take portable devices or media off the premises without the informed consent of their immediate supervisor. Informed consent means that the supervisor knows what equipment is leaving, what data is on it and the purpose for its use;
* Remote access to the network, applications, and data is for business purposes only. The organization’s management team must approve all remote access to sensitive information;
* Log in passwords must be used on all remote-computing devices;
* Users should not use the “Remember Password” feature of any software application (e.g. Internet Explorer);
* Computers and mobile devices supplied by the organization must not have their hardware or software configuration changed in any way, without management approval. Only authorized support personnel are permitted to make configuration changes;
* All portable laptops, notebook computers and mobile devices, including storage media, must use standard encryption technology when used to carry personal identifiable information or other confidential electronic data;
* Refrain from using remote access while travelling, particularly at airports or working outside the province/territory including while outside Canada.
  1. **Network Threats and Malicious Code from External Sources**

All users are responsible for following security protocols while accessing the computer network and services to protect the organization against viruses, worms, Trojan horses and other malicious code. The following security measures are required of all employees, contractors, students and volunteers to minimize these threats:

* All software installation must be coordinated through authorized support personnel;
* Users must not knowingly allow malicious code such as spyware, worms, viruses or other software that may cause a threat to the network to be installed on computers managed by the organization;
* Before use, users must scan for viruses on all portable storage media (including CDs, DVDs, and media sticks) that are new or are of unknown origin;
* The downloading or installing of any files is not permitted unless authorized by the organization’s management team. This includes (but is not limited to) software programs, screen savers, music and video files from the internet;
* Only software with a license agreement and management approval is to be installed on computers;
* Any user who suspects that his/her workstation has been infected must immediately power off the workstation and call their authorized support personnel. Users must not attempt to destroy or remove malware, viruses, spyware and/or other internet-born security threat, or any evidence of them, without direction from authorized support personnel;
* Users must immediately report to their direct supervisor and authorized support personnel any signs or suspicions of computer or network tampering, intrusions, or security breaches; and
* If any computer device is damaged, lost or stolen, the user must immediately notify their direct supervisor and follow the Incident Management process.
  1. **Right to Search and Monitor**

The organization’s management team or their authorized agents have the right to monitor, inspect, or audit all information systems used by the organization staff, contractors, students and volunteers. Such an examination may take place with or without consent, or the knowledge of the involved people. The information systems subject to examination may include among others:

* Email files;
* Hard drive files;
* Voice mail files;
* Printer files;
* Fax machine printouts; and
* Desk drawers and filing cabinets

Employees, contractors, students and volunteers should have no expectation of privacy regarding information stored in or sent using the organization’s information systems.

Audits may be performed:

* in response to a complaint or concern;
* in response to a trigger from system monitoring software;
* on a proactive, scheduled or random basis.

1. **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 Security-1 Information Security Policy:

*Privacy-1 Statement on Privacy Guidelines*

*Privacy-4 Security Contact Responsibilities*

*Privacy-13 Client Access and Release of Information*

*Privacy-15 Sending and Receiving Information*

*Security-7 Incident Management*

1. **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 |
| ***User Access Audit Templates*** | Provides the health organization with 3 audit Checklists to leverage for conducting required user audits associated with personal health information 'PHI' or clinical systems. | 1.4 |
| ***C&A Use Acknowledgement template*** | 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. | 1.4 |
| ***Password Management Tips*** | To provide the health organization staff with tips for password management for devices and systems - which is a key consideration to maintain privacy and security for personal health information. | 1.6 |

**<enter health organization name>**

# SECURITY-2: MOBILE DEVICES POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**1.0 POLICY**

The health organization will ensure that employees, contractors, students and volunteers (‘staff’) who have access to and control of personal health information ‘PHI’ know they have a responsibility to protect the privacy of information stored on their mobile devices to mitigate risks associated with their use which includes devices issued by the organization and personal devices if authorized for use by the organization.

Mobile devices such as smart phones, laptops, tablets and USB keys offer convenience; however, they raise risks for privacy and the protection of PHI. They are also at risk of threats such as viruses and spyware. All staff will read, understand and sign the health organization’s ‘Confidentiality & Acceptable Use that includes a section acknowledging their responsibility to protect PHI when using mobile devices.

For some health organizations that have geographically challenging circumstances the reality is that texting on mobile devices may be the only tools available to be used by the staff to ensure that they can contact clients, particularly in emergency situations where the client can’t be contacted any other way. In this situation, staff will use their best judgement and limit the content contained in the texts to the minimum needed to contact the client, and/or the client’s parent or guardian and will limit the recipients to only authorized health organization staff that have a ‘need to know’ of the information. The health organization may decide to designate specific individuals that would be authorized to send texts in these situations.

* 1. The following policy protocols should also be followed by all staff to help reduce the risks associated with the use of their mobile devices:
* Turn off calendar reminders, text/message popups, email popups etc. to prevent exposing sensitive client information that may be in them;
* Learn how to enable privacy and security settings on the mobile device;
* Only store PHI on the mobile device if it is absolutely necessary;
* Ensure that mobile devices are protected with hard-to-guess passwords;
* Use an automatic lock feature so a password is required to access information;
* Use encryption technology to provide added protection for PHI. If using a USB mobile stick – encryption must be in place or it must not be used to store sensitive information.;
* Install and run anti-virus, anti-spyware, and firewall programs on mobile devices – and keep those programs up-to-date;
* Don’t send PHI over public wireless networks (e.g. coffee shop hot-spots). Public wireless networks may not be secure and there is a risk that others may be able to capture the information;
* Keep mobile devices in sight. Never leave a mobile device unattended in a public place or a vehicle;
* Keep laptops locked up when not in use – a security cable attached to an immovable piece of furniture will deter theft;
* Ensure that information stored on a mobile device is purged before the device is discarded.

1. **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 Security-2 Mobile Device Policy:

*Security-1 Information Security Policy*

1. **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*** | *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.* | 1.0 |

**<enter health organization name>**

# SECURITY-3: INFORMATION TECHNOLOGY ASSET MANAGEMENT POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **POLICY**

The health organization will maintain an inventory for all information and information technology assets accessed and/or used by employees, contractors, volunteers and students within the health organization.

* 1. **Information Assets**: Includes personal health information ‘PHI’ in both electronic and paper form and other types of information that are not considered ‘PHI’ but are still important to the organization, such as financial reports and operating plans.
  2. **Information Technology (IT) Assets**: includes all hardware and software used to deliver the health organization’s programs and services.
  3. When assets are purchased, assigned to a health organization employee, contractor, student or volunteer (‘staff’), or retired from use, the Asset Management Inventory form should be updated and kept current. At the minimum information captured for each asset should include the following:
* Asset Name
* Description
* Type
* Used to store PHI?
* Critical to Operations?
* Linked to BCP (Business Continuity Plan)?
* Backup Profile
* Arrived on (Date)
* Retired on (Date)
* Serial Number
* Make
* Model
* Location
* Provisioned To

1. **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 Security-3 Information Asset Policy:

*Security-1 Information Security Policy*

1. **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 |
| ***User Asset & Access Template*** | Eight (8) forms to manage the health organization users' access to systems and physical environments in your organization. | 1.3 |
| ***P&S Asset Management Inventory*** | Provides a template to help manage all assets used to work with personal health information 'PHI’ (information, hardware and software assets) when onboarding/off boarding staff (including volunteers, contractors, etc.) by anyone working with the health organization. | 1.3 |

**<enter health organization name>**

# SECURITY-4: BUSINESS CONTINUITY MANAGEMENT PLAN POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **POLICY**

The health organization will have a Business Continuity Management ‘BCM’ plan in place to help the organization to continue its operations following a disaster or disruptive event. Examples of such events include fire, floods, power disruption, information system failure, illness that affects large numbers of people, etc. The BCM plan involves establishing business continuity and disaster recovery plans for all services, clients, employees, contractors and volunteers.

* 1. **Key Individuals involved**

The health organization’s Business Continuity Management Plan ‘BCMP’ will require a Coordinator, active and committed support from a team of senior staff, and input from key individuals from across the organization:

1. The **BCM Coordinator** is a person working for the health organization that organizes the BCMP, takes direction from the BCM Senior Team, and works with key individuals in the organization to ensure that departments across the organization participate and contribute to the plan. Identify an Alternate BCM Coordinator and identify the reasons when delegation to the Alternate will occur (e.g. primary BCM Coordinator is not available due to illness or vacation).
2. The **BCM Senior Team** provides strategic direction and guidance for the BCM process, approving BCM-related policies.
3. Key Individuals represent the different business areas of the organization, acting as contacts for planning purposes and as leaders when a disruptive event happens.
4. In the event of a disruption, the delegated individuals will be responsible for assessing the damage and directing recovery activities.
5. All key and authorized individuals will have a copy of the BCMP and any supporting documentation housed in a secure location with restricted access - that can be reached in the event of a disruption (e.g. a copy at an authorized person’s home, a copy located within the health organization facilities, and all relevant documentation required to recover critical information assets (refer to the Information Asset Management Log) and essential services that are affected by a disruption.

1. **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 Security-4 Information Asset Policy:

*Privacy-8 Archiving & Accessing PHI*

*Security-6 Privacy & Security Incident Response*

1. **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 |
| ***Business Continuity Plan ‘BCP’*** | Provides a Business Continuity Plan 'BCP' template to support the continuity of health care service delivery in the event of a disruption resulting in the unavailability of facilities, systems and/or associated hardware. Provides five TABLES that can be filled out so that you are prepared in the event of a disruption to the operations of the health organization. | 1.0 |
| ***BCP -*** ***TABLE - Health Organization BCM CONTACTS*** | Provides a tool for documenting the key people involved with the BCM plan. | 1.1 ‘F’ |
| ***BCP – TABLE- BCM Documents Referenced During Disruptions*** | Provides a tool to document health organization records of where key documents are located. | 1.0 |

**<enter health organization name>**

# SECURITY-5: USER ACCESS AND ACTIVITY AUDIT POLICY

|  |  |
| --- | --- |
|  | Page 1 of 5 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **POLICY**

The health organization will ensure that regular privacy and security user access and account activity audits are conducted for each employee, contractor, student, or volunteer (staff) to validate that the scope of their access continues to be relevant to the individual’s job duties as well as to identify breaches that require incident management. This includes audits for access and activity relevant to electronic information as well as physical access and activity (e.g. buildings, keys).

Where there is a potential to view sensitive clinical information in the data being reviewed during the audit at least one clinical staff member must be involved. Other staff members including the organization’s privacy/security contact or designate could be present for the part of the audit that does not include sensitive clinical client data.

* 1. **What should trigger an audit?**

The frequency and type of auditing should be a risk-based decision taking into account risk-related factors such as:

* Size of the health organization;
* Number and variety of users;
* Scope of user access;
* Frequency of access to PHI;
* Sensitivity of the information;
* Access by third parties;
* History of previous privacy breaches or incidents.

**Reactive access audits** are conducted based on a specific complaint, request, incident or other activity that suggests a user may have inappropriately accessed physical locations, sensitive information or abused special privileges.

**Proactive access audits** must be conducted at least annually and when triggered by staff changes. They may be conducted more frequently (periodically or semi-annually) based on highly sensitive situations such as access to highly sensitive clinical information or where staff may have family or personal relationships with clients.

* 1. **Proactive Access Auditing threat examples**

The following list of threat use cases are used to guide the frequency and scope of the access audit. Other threat use cases will be included as they are identified.

* A user accesses their own record or records of a family member.
* A user accesses PHI outside of normal working hours.
* A user accesses PHI from an unusual location (e.g. user is based in one location and is accessing client health files in another location.
* A user accesses a large number of health files over a short period of time for his/her job function.
* A user conducts a large number of client searches for his/her job function.
* A user generates a lot of system errors such as frequent login errors, or client not found errors.
* A user accesses a high-profile client and they are not in that person’s circle of care.
  1. **Responsibility to Inform Staff about Audit**

During Privacy and Security Awareness Training, that should be conducted for all staff annually at a minimum, the privacy contact will ensure that staff:

1. Commit to the confidentiality and acceptable use requirements e.g. by signing/resigning the appropriate form;
2. Are reminded that their access and activity is regularly audited and that there are consequences if inappropriate access/activity is determined up to and including dismissal;
3. Are reminded that if a user suspects inappropriate access they should report it without concern of retaliation.
   1. **Managing Privacy/Security Audit Outcomes**

If the outcome of any audit identifies a potential privacy and/or security breach, it must be documented and reported using an ‘Incident Reporting Form’ and investigated in accordance with the health organizations policies.

* 1. **Types of Privacy Access Audits**

The health organization’s privacy contact or designate will ensure the following types of audits are regularly conducted:

1. **User access requirements** – applications - user access (including employee, contracted resources, student, volunteer) to system application menus and functionality to ensure the access continues to be relevant to the individual’s job duties. This review must also confirm that the scope of access is appropriate. For example, the role(s) assigned in clinical systems (applications) is appropriate for the staff member at the time of the audit. If necessary changes are identified, immediate action must be taken to decommission access or provision a different role to the user;
2. **User account activity** – applications - user account activity to identify inactive accounts (e.g. no recent activity). If inactive user accounts are identified, the audit must verify whether these accounts are still required by the individuals to perform their job duties. If a user account is no longer required, it must be immediately decommissioned;
3. **User access** – information - user access to sensitive and important information assets to identify possible inappropriate access;
4. **Consent-related updates** - user access to a client health file when consent directives have been added, removed, modified or overridden to ensure that user access is appropriate, and the client was notified of consent overrides.
   1. **Types of Security Access Audits (physical & electronic)**

The health organization’s security contact or designate will ensure the following types of audits are regularly conducted:

1. **User Physical access – user access to buildings/offices/clinical rooms, wiring closets, communications cables and areas storing sensitive information to** identify potential security weaknesses or breaches, or any unusual patterns and anomalies of access to or unsuccessful attempts to access the sensitive and important information. This includes access to keys, access badges, FOBs, and alarm codes (e.g. buildings, offices, file cabinets, desks, etc.);
2. **User Computer-based tool access** – user access to email, internet, network drives, network logs, system logs, ability to install software, personal computers, printers, scanners, fax machines, cell phones, cameras, intranet, other special equipment, etc.;
3. **Documentation systems** – user access to systems such as electronic medical records or other clinical systems, financial systems, etc. to ensure that the access is appropriate.
4. **Special privileges** - such as afterhours access to buildings, remote access to computer-based networks and tools, ability to take sensitive data offsite, access to sensitive file storage areas such as personal information storage areas, privacy and security records, system and user access logs, archived records, etc.
   1. **Incident/ Breach from an Audit**

An audit may reveal a possible incident or breach when PHI may have been stolen, lost, subject to unauthorized use/access or disclosure such as unauthorized copying, modification or disposal, or as a result of a privacy or security failure. Possible incidents or breaches must be investigated following applicable health organization policies.

1. **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 Security-5 User Access and Activity Audit Policy:

*Privacy-18 Whistle Blower Protection Policy*

*Security-6 Privacy and Security Breach Incident Response Policy*

1. **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 Template*** | 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. | 1.3 |
| ***Access Audit Process*** | Provides the health organization with more details around the process on how to conduct User Access Audits - from both a privacy AND security perspective. | 1 |
| ***User Access Audit Templates*** | Provides the health organization with 3 audit Checklists to leverage for conducting required user audits associated with personal health information 'PHI' or clinical systems. | 1.5 |
| ***How to Respond to A Breach*** | To provide the health organization staff involved with protocols and a checklist to respond to breaches. | 1.7 |

**<enter health organization name>**

# SECURITY-6: PRIVACY & SECURITY INCIDENT RESPONSE POLICY

|  |  |
| --- | --- |
|  | Page 1 of 4 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**1.0 POLICY**

The health organization will ensure that privacy and security incident protocols are in place including an effective investigation process in order to respond quickly to any privacy and security incidents or breaches that are identified and subsequent communication protocols. Authorized key individuals such as the privacy and security contact/s, IT personnel and senior health organization management will be assigned clearly defined roles and responsibilities for the management of incidents and breaches.

* 1. **Privacy and Security Incident Response protocols**

Having a strong set of protocols and procedures in place for how to respond to incidents and breaches will demonstrate that the health organization has a robust privacy and security culture in place that:

1. Limits potential damages resulting from a breach or incident;
2. Makes it easier to address any breach or incident and;
3. Prepares health organization management to work with the Information and Privacy Commissioner if required.
   1. **Responding to incidents/breaches**

This policy covers addressing both an **incident** involving either a privacy and/or security event that has the potential to become a breach or is an actual breach. Examples include:

* An **Information Privacy Incident** is an illegal collection, use, disclosure, storage, or disposal of an individual’s personal health information.
* An **Information Security Incident** is an unwanted or unplanned event that threatens the confidentiality, integrity, and/or availability of sensitive information like personal health information ‘PHI’.
  1. **Defining a Breach**

This policy covers when an actual breach occurs where PHI is stolen, lost, subject to unauthorized use or disclosure such as unauthorized copying, modification or disposal, or as a result of a privacy or security failure. Examples include.:

1. Theft, loss, damage, unapproved destruction or changes to PHI;
2. Accidental or improper disclosure of confidential PHI in paper and/or electronic format;
3. Improper disclosure of summary information that identifies a particular community and/or a particular subset of the community;
4. Improper use of information assets or unauthorized access to information assets by an employee, contractor, student or volunteer;
5. Loss or theft of any information technology device such as desktops, laptops, BlackBerry, cell phones, CD/DVD, or any other electronic media that hold (or are capable of holding) PHI or other confidential/sensitive information;
6. Criminal activity, such as piracy, copyright abuse, system or application hacking, virus attacks; and
7. Failing to follow your health organization’s security and privacy policies, procedures and standards, such as disclosing PHI on social network sites.
   1. **Reporting and Communicating a Breach**

After confirmation of a privacy breach, the health organization will fully document the details of the breach and communicate with the required individuals:

* Reporting Person’s Information
* Background/Details
* Healing Actions Planned / Taken to Prevent / Minimize Future Occurrences
  1. **Privacy Commissioner Reporting Guidelines**

After confirmation of a privacy breach, consider the following factors in order to determine if the Privacy Commissioner should be notified:

1. The person committing the breach knew or ought to have known that their actions are not permitted (e.g. looking at an ex-spouse’s medical history for no work-related purpose, looking to see why a local celebrity or co-worker was receiving treatment);
2. The personal information recorded on paper, laptop, or other electronic device was stolen, including information that was subject to a ransomware or other malware attack or information seized through use of a portable storage device;
3. Following an initial privacy breach, the information was or will be further used or disclosed without authority (e.g. a person receives an incorrect fax, and although they return the fax, they keep a copy an threaten to make the information public or wrongly accessed patient information is subsequently used to mark products or services or to commit fraud such as health care or insurance fraud);
4. The personal information involved is sensitive;
5. There is a risk of identity theft or other harm including pain and suffering or loss of reputation;
6. A large number of people or a significant volume of information are affected by the privacy breach;
7. More than one person was responsible for committing the breach;
8. The information has not been fully recovered;
9. The privacy breach is the result of a systemic problem or a similar privacy breach has occurred before;
10. When disciplinary action is taken against a college member (e.g. when an employee who is a member of a college has been terminated, suspended or discipline as a result of a breach, or the individual resigns, and this action is related to a breach);
11. When disciplinary action is taken against a non-college member (e.g. a clerk is suspended because they posted patient information on social media after an unpleasant encounter with a patient);
12. Your organization or public body requires assistance in responding to the privacy breach; or
13. You want to ensure that the steps taken comply with the organization’s or public body’s obligations under privacy laws.
    1. **Privacy Breach Risk Factors**

To determine what other steps are immediately necessary, the health organization will assess the risks associated with the privacy breach. The risk factors that would need to be part of the risk assessment include:

* Personal Information Involved
* Cause and Extent of the Privacy Breach
* Individuals Affected by the Privacy Breach
* Foreseeable Harm from the Privacy Breach
* Recovery of Personal Information

1. **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 Security-6 Privacy & Security Incident Response Policy:

*Security-5 User Access and Activity Audit Policy*

1. **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 |
| ***How to Respond to A Breach*** | To provide the health organization staff involved with protocols and a checklist to respond to breaches. | 1.1 |
| ***Assessing Breach Risk Factors*** | To provide the health organization staff with a checklist to assess any risks that need to be mitigated following an incident or breach. | 1.5 |
| ***Incident Reporting Template*** | To provide health organization with a template to record any privacy incidents either revealed by the proactive Privacy Access Audit process and or any privacy and security incident identified that needs to be documented. | 1.4 |
| ***Incident LETTER Template*** | To provide the health organization with a framework communication letter to send to the person whose privacy & security has been compromised. | 1.4 |

**<enter health organization name>**

# SECURITY-7: ORGANIZED OFFICE

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

1. **POLICY**

The health organization requires that employees, contractors, students and volunteers working on behalf of the health organization ensure that all sensitive and confidential information including personal health information ‘PHI’, whether it be on paper, on a storage device or a hardware device is safeguarded by practicing organized office protocols. Paper and electronic devices containing PHI must be properly locked away or disposed of when not in use to reduce the risk of unauthorized access, loss of, and damage to sensitive information during and outside of normal business hours or when workstations are left unattended. This includes computers/laptops, cameras, USBs, mobile phones) etc.

* 1. Office configuration should be considered by the privacy and security contact or designate to make it easier for staff to protect themselves and the health organization’s clients. For example, where people are sitting and where they need to go to perform their job duties; how their equipment is setup to avoid unauthorized people from viewing paper and screens that may contain sensitive information.
  2. Staff, especially those individuals who do not have a private space, need to be reminded that sounds may carry, and that if any conversations involve personal health information about a client, they should move to an area that is more sound proof and keep the volume of conversation low.
  3. When leaving their office workstation for a period of time and/or at the end of the business day, staff must ensure the area is cleared of all client information, and personal or sensitive information of any kind. Paper records containing personal sensitive information must be stored in a locked cabinet or location and not left lying around. Keys for accessing drawers or filing cabinets should not be left unattended at a desk. If staff have their own office, the door should be locked when the staff member leaves; even if it’s only for a coffee or lunch break.
  4. All mobile devices (i.e. cell phones, cameras, laptops, USB devices, CDs and DVDs) must be locked up when the work station or office is unoccupied for a length of time, and completely shut down and/or locked up at the end of the work day. For example, if staff are using laptops they should be locked up in a drawer at the end of the day and not left out in the open.
  5. All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins. Ideally a cross-cut shredder should be made available to staff so that there is no possibility that the resulting waste could be put back together.
  6. Printers/scanners, and fax machines should be treated with the same care under this policy. Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, the “Locked Print” functionality should be used so when a document is sent to the printer, the individual needs to physically go to the printer and enter a code to release the document for print. This ensures no unauthorized staff inadvertently or purposefully read sensitive information before retrieval by the authorized individual.

1. **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 Security-7 Organized Office Policy:

*Privacy-20 Confidential & Acceptable User Policy*

*Security-1 Information Security Policy*

*Security-2 Mobile Devices Policy*

*Security-3 Information Technology Asset Management Policy*

1. **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 |
| ***How to Respond to A Breach*** | To provide the health organization staff involved with protocols and a checklist to respond to breaches. | 1.1 |

**<enter health organization name>**

# SECURITY-8: AUDIO/VIDEO SURVEILLANCE

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**1.0 POLICY**

The health organization will ensure that before any audio and/or video surveillance equipment is installed, the rationale and purpose for the surveillance is fully considered, documented and approved by the health organization’s privacy/security contact and senior management. This includes carefully weighing the loss of privacy when considering the potential use of video surveillance and the liabilities for the organization around protection, use, disclosure, retention and access. All relevant Canadian/provincial and territorial laws will apply.

* 1. Video surveillance will be considered as a last resort after exhausting other less privacy-invasive alternatives to meet the documented need because it puts the health organization at risk for violating privacy and security laws. Safeguards and procedures will be put in place if the health organization chooses to use surveillance equipment for a defined and documented need.
  2. The organization will put periphery applications and management tools in place for both the equipment itself and the footage captured as well as how it is maintained, stored and retrieved including the following considerations:

1. Surveillance is susceptible to misuse by those who can access the system and use the video in unauthorized ways so only authorized staff will be given access.
2. Extracts of the recorded footage will be provided to individuals who request a copy of their personal information (with their image), and software must be used to blur faces of third party individuals whose image appears in the footage to protect them from exposure if the footage is released.
3. Audio and/or video surveillance equipment must be placed and calibrated so that it only collects the personal information that is necessary to achieve the intended purpose that has been documented and approved.
4. Use of the equipment must be approved by senior management before it is installed.
5. The audio/video equipment must be positioned so that the general public cannot see any display of what is being captured and wherever possible, viewing by staff is kept to a minimum to those that are authorized by the privacy contact or their designate.
6. Once audio and/or video equipment is installed, a clear and understandable warning poster must be visible for individuals to read prior to entering into the space being monitored by the equipment.
   1. Storage, Retention and Destruction - The data and information stored on the audio and /or video surveillance equipment must be encrypted. Access to this information must be restricted to those individuals that maintain security of the building, room or item that is under surveillance. Retention, archival and destruction of the data and information must follow health organization policies.
   2. Training – authorized staff that setup and maintain the audio and/or video surveillance equipment must receive appropriate training to ensure they understand how to configure it properly to avoid any privacy and security risks.
7. **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 Security-8 Audio/Video Surveillance 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*

*Security-1 Information Security Policy*

Refer to the following online guides for further information:

* [Guide to using overt video surveillance](https://www.oipc.bc.ca/guidance-documents/2006) published by the Office of the Privacy Commissioner for BC.
* [Guidelines for Overt Video Surveillance in the Private Sector](https://www.priv.gc.ca/en/privacy-topics/surveillance-and-monitoring/gl_vs_080306/) published by the Office of the Privacy Commissioner of Canada.
* [Video Surveillance and Privacy Compliance in a Medical Clinic](https://www.oipc.bc.ca/media/16910/ac-p16-01-surveillance-and-privacy-compliance-in-a-medical-clinic-final.pdf) published by the Information and Privacy Commissioner for B.C.

1. **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 |
| ***‘Poster Templates’ for an ‘Audio & Video User’ sample poster*** | Provides the health organization with poster templates designs | 1.2 vi. |

**<enter health organization name>**

# SECURITY-9: CLOUD-BASED DELIVERY OF SERVICES POLICY

|  |  |
| --- | --- |
|  | Page 1 of 2 |
| APPROVAL  REVIEW AND REVISION DATES: | May 2018 |

**1.0 POLICY**

The health organization will ensure that safeguards are in place to support any cloud-based delivery of services that is being used as part of the organization’s operations. Specifically, sensitive information including personal health information/data that is stored and accessed on a third-party server in any cloud-based application/service will be protected under the relevant Canadian/provincial and territorial laws.

* 1. If the health organization is using any cloud-based services for any aspects of health care delivery the privacy/security contact will need to determine the risks to privacy/security and implement safeguards.
  2. The organization will need to mitigate any privacy and security risks if a network of remote servers hosted on the internet is being used to store, manage, and process data, rather than using a local server or personal computer for that purpose.

Cloud services used by organizations typically fall into the categories of a private cloud (example: Mustimuhw Client Health Portal), or a public cloud (Dropbox, Survey Monkey).

* 1. If sensitive information is involved and the cloud environment is managed by a third-party organization, then the security contact and privacy contact, or their delegates, are responsible for ensuring that the third-party organization has all required safeguards in place before sensitive data is collected and stored on the cloud-based service. For example:
* The cloud-based service is provided through a private cloud and meets all relevant Canadian/provincial and territorial laws and meets all of the health organization’s privacy and security policies.
* The third-party servers are located on Canadian soil so that all privacy and security laws are relevant.
  1. The privacy contact will confirm that the third-party sign organization has appropriate Confidentiality Agreements in place to ensure that responsibility to protect sensitive information is clearly understood and if not, ensure that appropriate agreements are in place.

**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 Security-9 Cloud Based Delivery of Services Policy:

*Security-1 Information Security*

*Privacy-1 Statement on Privacy Guidelines and Principles*

*Privacy-3 Privacy Contact Responsibilities*

*Privacy-4 Security Contact Responsibilities*

*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 |
| **C&A Use Acknowledgement** | Provides a template for Confidentiality & Acceptable Use Acknowledgement document. | 1.4 |
| **ISA Guiding Principle** | Provides guidelines and a minimum set of items that should be included in an Information Sharing Agreement 'ISA' in place with another organization. | 1.4 |