Dealing with Health Information

Table of Contents

Dealing with Health Information

Key Points

- You must store your patients' personal health information in a reasonably secure manner and in accordance with the prescribed requirements, if any.
- If your patients' personal health information is stolen, lost or accessed by unauthorized persons, you must notify your patients as soon as possible.
- You must retain personal health records for their minimum retention periods, and as long as needed to allow patients to exhaust any legal recourse available to them involving an access request.
- You must dispose of your patients' personal health records in a secure manner.
- You may transfer your patients' personal health records as described in the Act so long as you do so securely.

Storage and Retention

The Rule

Storage

You must store your patients' personal health information in a reasonably secure manner and in accordance with the prescribed requirements, if any.

If your patients' personal health information is stolen, lost or accessed by unauthorized persons, you must notify your patients as soon as possible. (There is an exception under the law for researchers. See the Research section for details.)

Retention

The Act does not establish specific retention periods, but does require records containing personal health information to be kept:

- no longer than prescribed by law, and
- for as long as needed to allow a patient to exhaust any legal recourse a patient has regarding a request for access.

Note: The Regulations made under the Act do not currently contain any specific storage or retention rules; however, the Regulations made under the *Public Hospitals Act* that deal with record retention do continue to apply.

What You Need To Do

- Retain your patients' personal health information in a reasonably secure manner. See the Security section for guidelines on keeping information secure.

- The steps you take must address your:
  - physical security (for example, locked filing cabinets, restricted office access and alarm systems),
  - technological security (for example, passwords, encryption and firewalls), and
  - administrative controls (for example, security clearances, access restrictions, staff training and confidentiality agreements).

Note: If you are a physician and you keep electronic health information, make sure you:

- can display and print your records for each patient in chronological order,
- can retrieve your records by the patient's name and health card number (where applicable),
- keep an audit trail that:
  - records the date and time of each entry for each patient,
  - shows any changes in the record,
  - preserves the original record's content when changed or updated, and can be printed separately from other patients' records,
- use password protection or other features to secure the records from unauthorized access, and
- install automatic back-up for file recovery to protect your records from loss and damage.

- Retain personal health records for their minimum retention periods. This means in every instance you need to know the retention periods various laws prescribe and why the information you are dealing with was collected.
- When patients have requested access to their own personal health records, retain those records as long as needed to allow the patients to exhaust any legal recourse involving the request.

What You Should Do

- Establish procedures for record storage. These procedures should be based on the guidelines provided in the Security section.
- Establish procedures for record retention. These procedures should be based on the information in the Summary of Retention Periods.
- Retain clinical records for the periods described in the Summary of Retention Periods. Retain educational, administrative, funding and research records for as long as you need them to serve their purpose, and then securely dispose of them.
- In deciding how long you need to keep your patients' personal health information, follow three steps:
  - First, consider why you collected the information (for example, for research, funding or clinical purposes).
  - Second, consider how long the law requires you to keep the records.
  - Third, decide whether under the circumstances you should hold onto the records longer than required to manage legal risks (for example, where patients have sued in the past).
- A general practice is to retain information for 10 years from the time the record was last updated or from when a minor attained the age of majority.
- Consider your own risk management. What if a patient sues you after the minimum retention period has ended and you have destroyed records that could help defend you? Before disposing of files, ask yourself whether the patient's case was one that might lead to a lawsuit. For example, certain kinds of treatment have a higher incidence of negligence claims (such as gynaecology and obstetrics). You may want to retain these records for longer periods than legally required.
- See the Summary of Retention Periods for retention periods for:
  - Health Records
  - OHIP Records
  - Research Records
  - Education Records

Disposal

The Rule

You must dispose of your patients' personal health records in a secure manner. The Act does not specify disposal methods.

What You Need To Do

- Dispose of your patients' personal health records in a secure manner.

What You Should Do

- Outline very clear procedures for securely disposing of personal health records and make sure your procedures are always followed.
- For hard copy records, secure disposal means shredding or burning them.
- For electronic records, secure disposal means either physically destroying the media they are stored on (such as a CD) or magnetically erasing or over-writing the information (in such a way that it cannot be recovered). Encrypting information is not a method of disposal even if the encryption keys are destroyed because it is possible that encrypted information may be recovered at some time in the future, even though keys have been destroyed.
- For more information on the security aspects of record disposal, see Security – People – Personal Responsibilities for Security.
- When you dispose of personal health records, record:
  - the names of the patients whose records were disposed of,
  - the dates the records were disposed of, and
  - that you properly followed your hospital's disposal procedures.

  Keep this record of disposal for as long as your hospital by-laws require.

  Note: This is a requirement of the *Public Hospitals Act*.

Transfer

The Rule

You may transfer your patients' personal health records as described in the Act so long as you do so securely.

What You Need To Do

Transfer to Another Facility

- When you transfer your patient's personal health records to another facility or physician, you must keep the original record and only transfer a copy.

  Note: This is a requirement of the *Public Hospitals Act* and the *Medicine Act*.

Transfer to a Successor

- When you transfer your patients' personal health records to your successor, make reasonable efforts to notify your patients before transferring their records or, if that is not reasonably possible, as soon as possible afterwards.

Transfer to Archives

- When you transfer your patients' personal health records to:

  – the Archives of Ontario, or

  – in certain prescribed circumstances, a prescribed person whose duties include collecting and preserving records of historical or archival importance, if the transfer is made for that purpose,

  make sure you have the archivist's agreement to the transfer.

  Note: In this context, the transfer is made for storage purposes.

What You Should Do

- Follow the guidance provided in the Security section to make sure you are transferring information securely.

Related Sections of the Act

Sections 2, 3, 4, 10, 12, 16, 17, 42, 52, 72 of the Act

Sections 1(10), 14 of the General Regulation

Checklists, Templates and Tools

Summary of Retention Periods

See the Security section for additional checklists, templates and tools.

SUMMARY OF RETENTION PERIODS

Retention Periods for Health Records for Hospitals

Patient Care Records:

Adults: 10 years after the patient's discharge or death (inpatient), or
10 years after the patient's last visit or death (outpatient)

Minors: 10 years after the day the patient turns or would have turned 18

Diagnostic Imaging Records:

Adults: 5 years after the day the record was created, except for diagnostic imaging records of a breast examination, which must be retained for 10 years

Minors: 5 years after the day the patient turned 18, except for diagnostic imaging records of a breast examination, which must be retained for 10 years after the patient turns 18

Adults and Minors:

Videotapes of diagnostic imaging examinations need not be kept unless the videotape constitutes the only record of the examination

Investigations

If a notice for an investigation or inspection under the *Regulated Health Professions Act*, *Health Insurance Act* or *Coroners Act* is received, the records must be retained until the investigation or inspection and any subsequent hearing is completed

Patient Access Requests

A personal health record cannot be disposed of if the patient the record relates to seeks access to those records and has not yet exhausted all avenues allowing for access

Lawsuits

Where a claim of negligence may arise:

Adults: A minimum of 15 years from the date on which the act or omission upon which the claim of negligence could be based occurred

Minors: A minimum period of 15 years from the date the patient turned 18

In both cases, if the patient cannot commence a claim because of a mental, physical or psychological condition and the individual has no litigation guardian, the records should be kept longer

The rules around discoverability of a negligence claim are complex and are dependent on the specific facts of each case

For specific retention periods regarding individual cases, consult your lawyer

Retention Periods for OHIP Records for Hospitals

The *Health Insurance Act* requires that records be maintained to demonstrate that:

- an insured service was provided
- the hospital provided these services
- the service was medically and therapeutically necessary

A minimum of 10 years, in line with statutory retention periods for clinical records, to assist in proving billing was necessary

Retention Periods for Research Records for Hospitals

General Principle

Identifying data should be retained only as long as necessary to fulfill the research purpose; however,

- in a case where a claim of negligence may arise, records should be kept longer
- due to the complexity of the discoverability rules in relation to claims of negligence, for record retention periods for specific research projects, consult your lawyer

If research is conducted without patient consent, the researcher receiving the information must follow any return restrictions imposed by the originating health information custodian

Retention Periods for Health Records for Physicians (Private Office Records)

Patient Care Records:

Adults:	10 years after the last entry date, or until the physician stops practicing
Minors:	10 years after the day the patient turns or would have turned 18 or until the physician stops practicing

Special Notes:

Family medicine and primary care physicians should refer to special transfer and disposition rules if they plan to stop practicing

Dispensing physicians should refer to Supplementary Tables A and B for retention rules relating to dispensing medications

Investigations

If a notice for an investigation or inspection under the *Regulated Health Professions Act, Health Insurance Act* or *Coroners Act* is received, the records must be retained until the investigation or inspection and any subsequent hearing is completed

Patient Access Requests

A personal health record cannot be disposed of if the patient the record relates to seeks access to those records and has not yet exhausted all avenues allowing for access

Lawsuits

Where a claim of negligence may arise:

Adults:	A minimum of 15 years from the date on which the act or omission upon which the claim of negligence could be based occurred
Minors:	A minimum period of 15 years from the date the patient turned 18

In both cases, if the patient cannot commence a claim because of a mental, physical or psychological condition and the individual has no litigation guardian, the records should be kept longer

The rules around discoverability of a negligence claim are complex and are dependent on the specific facts of each case

For specific retention periods regarding individual cases, consult your lawyer

Retention Periods for OHIP Records for Physicians

The *Health Insurance Act* requires that records be maintained to demonstrate that:

- an insured service was provided
- the physician provided these services
- the service was medically and therapeutically necessary

A minimum of 10 years, in line with statutory retention periods for clinical records, to assist in proving billing was necessary

Retention Periods for Research Records for Physicians

General Principle

Identifying data should be retained only as long as necessary to fulfill the research purpose; however,

- in a case where a claim of negligence may arise, records should be kept longer

- due to the complexity of the discoverability rules in relation to claims of negligence, for record retention periods for specific research projects, consult your lawyer

If research is conducted without patient consent, the researcher receiving the information must follow any return restrictions imposed by the originating health information custodian

SUPPLEMENTARY TABLE A

RETENTION PERIODS FOR RECORDS RELATING TO DRUGS DISPENSED UNDER THE ONTARIO DRUG BENEFIT PLAN

Document	Retention Period
Statement of daily transaction totals	2 years from the statement preparation date
Summary remittance or reject statement from the Minister	2 years from the statement receipt date
Claim for payment or reversal submitted to the Ministry, with a record of the claim submission date	2 years from the claim submission date
Monthly Ontario drug benefit eligibility card or copy of the cards for each eligible person for whom a drug is dispensed	2 years from the first drug dispensing date
Prescription with a no substitution direction and accompanying copy of the Health Canada adverse drug reaction form	2 years from the receipt date
Ministry confirmation that drug is to be supplied if it meets the applicable clinical criteria set out in Part III of the Formulary	2 years from the confirmation receipt date
For each extemporaneous preparation supplied for an eligible person, the formula, including the compounding time, all of the ingredients and the quantities and cost of those ingredients	2 years from the supply date
Where the acquisition cost of a drug is claimed, a copy of the supplier's invoice and a detailed calculation in accordance with section 14 of the cost of purchasing the drug product	2 years from the receipt date

SUPPLEMENTARY TABLE B

RETENTION PERIODS REQUIRED FOR PATIENT RECORDS RELATING TO DISPENSING OF DRUGS UNDER *THE DRUGS AND PHARMACIES REGULATIONS ACT*

Document	**Retention Period**
Required dispensing records	6 years after the last entry date or until the physician stops practicing

Security – Introduction

The Rule

You must implement reasonable physical, technical and administrative measures to safeguard personal health information.

You must implement these measures to ensure the security and confidentiality of personal health information. Specifically, you must:

- prevent unauthorized use, copying or disclosure of the information,
- protect the information during collection, storage, transfer and disposal, and
- protect the integrity of the information by preventing unauthorized modification or disposal.

You must also notify your patients as soon as possible if their personal health information is stolen, lost or accessed by unauthorized persons.

The Act does not prescribe specific security standards and safeguards; instead it asks you to take reasonable steps. What is reasonable depends on the threats, risks and vulnerabilities to which the information is exposed, on the sensitivity of the information and on the extent to which it can be linked to an identifiable individual. What is reasonable can also be judged by comparing the steps you take with the best practices that other similar organizations with effective security have implemented.

It is clear that taking reasonable steps includes implementing systems and controls that safeguard how you collect, use, modify, disclose, retain, transfer and dispose of personal health information. These steps cover:

- physical security (for example, locked filing cabinets, restricted office access and alarms),
- technical security (for example, passwords, encryption and firewalls), and
- administrative controls (for example, security clearances, access restrictions, staff training and confidentiality agreements).

The four security sections that follow are designed to help you identify and implement best practices for safeguarding personal health information. When you read them, you will see statements such as “What you need to do…” You should interpret this as “What you need to do to implement best practices for

safeguarding personal health information" as opposed to "What you must do to comply with the law". Ultimately, it is up to you to decide what taking reasonable safeguard steps means for your organization, but we strongly suggest that adopting best practices is the approach to take. Clearly, if you take no steps, you are in violation of the Act.

As you read the four security sections, you should keep in mind some simple principles of security that will help you make decisions and determine priorities:

- Take a "**defence in-depth**" approach that assumes no single measure is perfect. So if it fails, you have other lines of defence to maintain protection. Consider mixing your measures between technical/physical measures and administrative measures (people and processes). Just having all technical measures could leave you exposed in situations such as power failures.

- Make sure your security program is **balanced and comprehensive**. Security is only as strong as the weakest link. Paying too much attention to one vulnerability at the expense of others will leave you exposed and will not provide you with the best value for your security dollar. It is better to have a $50 lock on both front and back doors than a $1,000 lock on the front door and none on the back.

- Don't rely **only** on technology. Using technology will be important to help you protect personal health information but people and processes are often more important. Technology is useless if people don't use it properly. And unfortunately, your people will often likely be the cause of security problems. So having informed, motivated staff using well designed processes is critical.

- Security is not just the job of the security professionals – **security is everyone's job**. Once someone has "security" in their job title you may think you can relax and assume that they are taking care of everything. Staff must be made aware that they are all key to good security.

- Keep personal health information in **places you can best protect it**. This sounds obvious but there are choices you can make to centralize the storage of both hardcopy and electronic information in areas that have good security controls such as supervised filing areas or servers managed by an IT department. Wherever possible, avoid letting the information be stored where you have less control, such as individual offices or personal computers.

You should also apply your thinking to everyone who has access to personal health information within the institution, including employees, agents, contractors and volunteers. Throughout these sections we will collectively refer to these people either as "staff", or "user" if we are talking about electronic access to information. You must also think beyond your boundaries to how the security

protections will apply to third parties who handle personal health information on your behalf.

In the next four sections, we'll deal with the critical aspects of an effective security program:

- Section 1: Security – First Steps
    - Security Program and Policy
    - Roles and Responsibilities
    - Information Inventory and Classification
- Section 2: Security – People
    - Personal Responsibilities for Security
    - Authentication and Authorization
- Section 3: Security – Institutional Safeguards
    - Perimeter Security
    - Malicious Software
    - Wireless and Portable Devices
- Section 4: Sustaining Security
    - Business Continuity
    - Development and Maintenance
    - Audit
    - Recommended Standards

Security – First Steps

Table of Contents

Security – First Steps

Key Points

To implement security effectively, you need a balanced approach that covers your staff, your administrative processes and your technology. This section deals with the fundamental first steps:

- Set up a security program that takes a comprehensive approach to your physical, technological and administrative operations.
- Assess your current security situation to determine your priorities and serve as a baseline for the program.
- Develop a security policy that commits the organization to appropriate security measures and provides high-level direction on how this will happen.
- Develop an appropriate set of security standards and procedures based on your policy.
- Appoint a staff member with overall responsibility for security.
- Define, document and communicate the responsibilities of this role and all the other roles required to support your security policy.

Documents you should create as a result of carrying out these steps include:

- Security Policy, Standards and Procedures
- Initial Security Review Results
- Personal Health Information Inventory (Appendix B)

Security Program and Policy

You must take reasonable steps to keep personal health information secure. What is reasonable may vary depending on your organization's size and complexity, and the nature and extent of risks faced within the organization. Large hospitals dealing with significant amounts of sensitive personal health information that have internal networks, centrally managed IT and many staff members accessing information electronically will need different security than small offices. You must decide where your organization falls on the range between large institution and small office. Scale your measures to a reasonable level that fits your circumstances.

What You Should Do

Set up a security program that takes a comprehensive approach to your physical, technological and administrative operations.

Assess your current security situation to determine your priorities and serve as a baseline for the program.

Develop a security policy that commits the organization to appropriate security measures and provides high-level direction on how this will happen.

Develop an appropriate set of security standards and procedures based on your policy.

Your security program must be comprehensive because good security does not rely only on a strong lock on the front door. Good security relies on a series of measures in place just in case the lock gets broken or the back door is left open. Your program must also cover all security measures and not just technical ones. Installing anti-virus software to secure personal health information is important. But, it is not enough. Security is easily breached by simple mistakes such as sensitive information being left lying around or a wrong number being punched in when faxing a patient record.

You need to make an initial assessment of your current security situation to determine the critical areas you must address first and also to set the baseline you will measure against to determine the effectiveness of your security program. This assessment should analyze both your current security risks and controls. If

you don't have the skills within your institution to do this, seek outside help to do the assessment properly since it will serve as the foundation for your program.

A written security policy is important as it will guide your staff on overall security matters and provide a base for creating specific standards and procedures. Your initial security assessment will provide input to help you build the policy that best meets your security needs. You also need to have a good understanding of your legal, regulatory, ethical and contractual security obligations in order to build your policy.

At a minimum, the highest levels of your management should approve your security policy. Your security policy should include:

- what security means to your institution and why it is so important,
- key security goals and principles,
- individuals' basic security responsibilities and accountability,
- how staff will be trained,
- who will review and update your policy, and
- how you will comply with your contractual and legal security obligations.

You should use your policy to help develop a fully documented set of security standards (for example, password rules) and security procedures covering both:

- how you protect your perimeter (such as the main entry point to your building or computer network), and
- what occurs inside your building or network (because your employees are not free to see any information they want, nor are they immune from mistakes or bad judgement).

The security policy should integrate with other policies, particularly privacy.

Tell your staff and outside contractors about the policy.

Small Office Applicability

- Give your staff a concise written set of security rules that also explain why the rules must be followed.
- Remember that everyone must play their part in protecting your patients' personal health information and your facilities.

- The Small Office Applicability sub-sections in this section will help you customize rules that fit your office.

Roles and Responsibilities

What You Should Do

Appoint a staff member with overall responsibility for security.

Define, document and communicate the responsibilities of this role and all the other roles required to support your security policy.

- Assign at least one staff member (for example, the Security Officer) overall responsibility for security. See Appendix A for a sample of this person's responsibilities.
- Establish a cross-functional team of senior managers to review security status, requirements and direction and ensure security issues are addressed with long-term solutions. The team should meet regularly.
- Consider appointing a Data Steward to define the exact policies for access to stores of personal health information.
- Appoint one staff member in each critical process (such as transferring health records) to be responsible for that security process. This role differs from the Data Steward role as the latter deals with disaster recovery requirements rather than specific data-handling requirements.
- Define, document and communicate security responsibilities for personnel managers, general employees, and those with security roles for specific processes.
- Define specific security duties for employees responsible for maintaining security controls and with special access for technical support.
- Ensure security through "separation of duties." Individuals should neither audit their own performance nor authorize their own access to a system.

- If security responsibilities can be delegated, for example, where a Data Steward may appoint someone to perform day-to-day data access approvals, define the delegation precisely.
- Do not delegate responsibility for determining security requirements to third parties. Define security requirements in any contract with third parties with access to personal health information. Build in appropriate monitoring measures to ensure they comply.
- Your list of security responsibilities should cover specific security incident response procedures (such as responding to security breaches).

Small Office Applicability

- The law makes physicians ultimately responsible for security.
- While all staff play a role, the buck stops with the custodian of personal health information.
- Make clear to your staff what are their security responsibilities (as described in other sections of this Toolkit). Train staff on these responsibilities when hired. Ask them to sign that they understand and will abide by their responsibilities.

Information Inventory and Classification

What You Should Do

Maintain a categorized inventory of all your stores of personal health information.

- List all stores of personal health information. Capture the essential facts about the information and how it should be handled. (A sample Inventory Template is included in Appendix B).
- The inventory should include all formats and media used to store personal health information including electronic, hardcopy, microfiche, audiovisual media, photographs and other images.

- Build your security policy around a data classification scheme. Categorize the types of information you collect and store and define security controls for each category. Typical categories include:
  - **public** – no restrictions,
  - **internal** – for use inside the institution only,
  - **confidential** – for use only on a "need to know" basis, and
  - **restricted** – controlled access to specified individuals.
- All personal health information should be classified as at least confidential.

Small Office Applicability

- Keep accurate records of the personal health information you store. Include both hardcopy and electronic information and information that may be outside your office.
- Implement appropriate security measures to protect the information. At a minimum, store hardcopy information under lock and key and protect electronic information by password.

Checklists, Templates and Tools

Appendix A – "Roles and Responsibilities" provides a sample of a Security Officer's Responsibilities

Appendix B – "Information Inventory and Classification" provides a sample Information Inventory Template

APPENDIX A – ROLES AND RESPONSIBILITIES

Sample Security Officer Responsibilities

- Setting, reviewing and updating security policy.
- Ensuring staff and contractors are aware of the policy and informed on how they should support it.
- Driving implementation of supporting procedures and controls.
- Ensuring security controls are audited.
- Conducting Threat Risk Assessments (TRA) for any changes to processes or IT systems that could affect security. (See sample TRA form in Sustaining Security section.)
- Investigating security incidents and ensuring long-term solutions are in place. (Security incidents occur whenever your security controls are compromised or challenged beyond any thresholds you have set. If the incident compromises personal health information, it also raises privacy issues; you should follow the guidelines in the Oversight section of this Toolkit to manage a privacy breach.)
- Developing a close working relationship with the contact person or equivalent (since these roles are intimately connected).
- Advising staff and contractors on security.

APPENDIX B – INFORMATION INVENTORY AND CLASSIFICATION

Sample Information Inventory Template

Create and maintain a high-level inventory of all the computer and hardcopy stores of personal health information you have. Remove the sample information and customize the table according to your needs.

Name	Information Types	Info Steward	Location	Backup Copies	Security	Retention
Master Patient Health Records	Patient info: - Name - Contact info - Health # - Family info - Health history	John Q. Deere	UNIX server at College Street location	Offsite storage facility in Markham	Confidential: password-protected via EHR application on encrypted in storage	Archive after patient inactive for • years
MRI Records	MRI images with: -patient name -health # -date	Jane P. Doe	MRI Cabinet, 4th floor, University Avenue	None	Confidential: Locked cabinet (key with Jane) Sign-out sheet for borrowing records	Destroy after patient inactive • years

Storage requirements should include any special measures needed for the type of media used, such as limits on heat, humidity, ultra-violet light and magnetic fields.

Security – People

Table of Contents

Security – People

Key Points

Your security is only as strong as your staff. Even the best technological security is vulnerable if you do not have staff committed to safeguard confidential information. This section deals with the steps needed to address the people aspect of security:

- Inform and motivate all staff and contractors. Give them the necessary tools to carry out their personal security responsibilities. Training should include awareness and commitment to:
  - Security Policy
  - Malicious Software Rules
  - Responsibilities for Physical Security
  - Acceptable Use Policy
  - Rules for Fax Machines
  - Confidentiality Agreement
  - Password Policy
  - Guidelines for Mobile Computing
  - Incident Reporting Rules
- Impose controls to ensure no one gains access to personal health information without proper authorization.

Documents you should create as a result of carrying out these steps include:

- Staff Responsibilities for Physical Security (Appendix A)
- Acceptable Use Policy and Rules for Fax Machines (Appendix A)
- User ID and Access Management Procedures (Appendix B)
- Password Policy (Appendix B)

Personal Responsibilities for Security

What You Should Do

Inform and motivate all staff and contractors. Give them the necessary tools to carry out their personal security responsibilities.

- Run appropriate background checks before hiring staff who:
  - deal with personal health information,
  - work on IT infrastructure, and
  - have special security responsibilities.
- Staff should sign confidentiality agreements.
  - Have staff sign the agreement when they are hired and initial their pledge annually as a reminder. Use this as an annual opportunity to reinforce training on privacy and security and brief staff on recent changes.
- All third-party contractors (for instance, consultants) and key contractor staff who may have access to sensitive information should sign an agreement before they begin work.

Physical Security

- Your staff must:
  - be aware of physical security responsibilities,
  - lock up sensitive material,
  - wear identity badges,
  - secure information outside the normal work area, and
  - report suspected incidents.

- See Appendix A for more detailed guidance on physical security and use of fax machines.
- Tell staff what they need to do for on-line security. Issue an "Acceptable Use" policy (see Appendix A for a sample).
- Provide staff with necessary security tools (such as anti-virus software and laptop computer cable locks).
- Create an ongoing security awareness and training program, reinforced with regular updates.

Small Office Applicability

- Lock up hardcopy personal health information if left unattended. Assign someone the task of making sure the office, all personal health information and computers are locked at the end of each day.
- Set power-on passwords on all computers. Install locking screen savers and instruct staff to use the screen saver whenever they leave their computer. Set the screen saver to automatically kick in when the computer is idle for a reasonable period of time.
- Use your computers' built-in security features, such as power-on and hard-drive passwords.
- Make sure staff understand that they should not install any unauthorized software or connect any unauthorized devices to their computers, or use their computers for unauthorized purposes.
- Make sure staff understand that they may not copy or transmit any information from their computers unless authorized. This includes using email or instant messaging.
- Avoid accidental exposure of personal health information, like the "reader over the shoulder" or the neighbour who overhears loud conversations.
- Give staff facilities (for example, shredding machines) to securely dispose of personal health information no longer required.

Authentication and Authorization

Although the following guidelines focus on computer systems, many apply equally to voicemail and hardcopy records.

What You Should Do

Impose controls to ensure no one gains access to personal health information without proper authorization.

- Authentication establishes someone's identity.
- Authorization establishes what someone may do.

Restrict access to all personal health information to only those who "need to know". Give access only to people whose job requires access.

Always provide only the minimum access needed to perform the job.

- Where possible, use two-factor authentication to grant access to personal health information. This requires users to (1) know something, like a password, and (2) have something, like an ID badge. This is especially important when providing remote electronic access to personal health information.
- Implement effective password policies and practices, including standards on password choice, protection and updating. (A sample password policy is found in Appendix B.)
- Avoid shared User IDs so you can hold all individuals accountable for their use of computer and network resources.
- Manage User IDs and associated access rights from issuance through deletion. Appendix B provides details on the practices you should adopt, including:
  - periodically checking to see that User IDs are still needed, and
  - creating special measures for User IDs with access overrides, such as those technical support staff use.

Small Office Applicability

- Provide staff with their own computers, User IDs and passwords, where possible. At a minimum, staff should have their own User IDs and passwords to access personal health information.
- Remove or change access as soon as staff leave or change responsibilities.
- Instruct your staff to create passwords that are hard to guess. Tell them not to write passwords down and, if they must, to store the paper someplace secure. (Recommend passwords at least 8 characters long containing both numbers and letters.) Ask them to change these passwords periodically and never re-use old ones.
- Instruct your staff never to share their passwords except for temporary authorized backups. Passwords should be reset immediately afterwards.

Related Sections of the Act

2, 3, 4, 10, 12, 13, 14, 42, 53

Checklists, Templates and Tools

Appendix A – "Personal Responsibilities for Security" provides a sample List of Staff Responsibilities for Physical Security, a sample Acceptable Use policy and guidance on using fax machines.

Appendix B – "Authentication and Authorization" provides a sample password policy.

APPENDIX A – PERSONAL RESPONSIBILITIES FOR SECURITY

Sample List of Staff Responsibilities for Physical Security

- Lock cabinets and secure removable computing devices such as laptops.
- Follow "clean desk" practices especially in unattended workspaces.
- Wear identity badges, challenge "tail-gaters" entering restricted areas, and sign-in and escort visitors in restricted areas.
- Secure information and computers used outside the normal work environment (for example, in a home office or while tele-commuting or travelling for business).
- Avoid accidentally exposing information, for example, allowing a computer screen to be viewed or a conversation to be overheard.
- Dispose of hardcopy personal health information properly (for example, using a shredding machine). Disposal methods such as shredding machines should meet security standards.
- Properly dispose of digital media by either physical destruction (for example, shredding CDs) or by first erasing information in an approved manner.

Sample Acceptable Use Policy

Modify the following sample policy to suit your requirements. Review with your lawyers before publishing.

- **Applicability**
  - All users, including full- and part-time employees, contractors, temps, affiliates, consultants, and interns, of **[Insert Your Organization's Name]** IT resources are subject to this Acceptable Use Policy.
- **Business Use**
  - Use **[Insert Your Organization's Name]**'s resources exclusively to conduct **[Insert Your Organization's Name]** business or for other uses management authorizes.
  - The following statement (or equivalent statements) must be presented to individuals logging onto **[Insert Your Organization's Name]**

systems during the identification and authentication process if the **[Insert Your Organization's Name]** system is running an operating system that can provide notification (otherwise labels containing the text should be placed visibly at the user interface):

- Use is subject to audit at any time by **[Insert Your Organization's Name]** management. **[Insert Your Organization's Name]** may from time to time monitor use of its IT resources, including email and the Internet, to ensure business use or to investigate suspected problems. Users are advised of this practice before being permitted access to **[Insert Your Organization's Name]** IT resources.

- **Personal Use of Computing Equipment**

  - Only **[Insert Your Organization's Name]** management may approve personal use of **[Insert Your Organization's Name]** computing equipment (if the use is clearly insignificant and complies with **[Insert Your Organization's Name]'**s Business Conduct Guidelines). Personal use may not be approved if it:

    - interferes or competes with **[Insert Your Organization's Name]** business,
    - interferes with any employee's job performance,
    - involves any additional costs to **[Insert Your Organization's Name]**,
    - involves commercial solicitation,
    - divulges company information to others, or
    - involves commercial or personal distribution lists.

  - Questions concerning personal use of **[Insert Your Organization's Name]** computing resources and Internet services should be discussed with the employee's manager.

  - Incidental or infrequent personal use of **[Insert Your Organization's Name]**'s e-mail systems and access to the Internet for personal use may be allowed without management approval provided none of the above prohibitions are violated.

Security – People

- **Instant Messaging**
  - Internal Instant Messaging is subject to all **[Insert Your Organization's Name]** Acceptable Use standards and is subject to the same policies and standards as e-mail communications.
  - External or public Instant Messaging software and services may not be used on any **[Insert Your Organization's Name]** machines or from within the **[Insert Your Organization's Name]** network.
  - Only the authorized **[Insert Your Organization's Name]** Instant Messaging solution may be used.
- **Cell Phones**
  - Cell Phones should not be used to store or transmit confidential information.
  - Use of cell phone cameras is prohibited within **[Insert Your Organization's Name]**.
- **Wireless Network Access**
  - Management must approve in writing all Wireless Access Points. A Risk Assessment must be performed prior to their implementation.
  - Only **[Insert Your Organization's Name]** approved and installed Wireless technology is permitted on an **[Insert Your Organization's Name]** machine or within **[Insert Your Organization's Name]**.
- **Chain Letters, Hoaxes and Virus Warnings**
  - Using **[Insert Your Organization's Name]** computer systems to send, forward or reply to chain letters, free offers, hoaxes or virus warnings is prohibited.
  - Should you receive an e-mail notice about a supposed virus or harmful code threat, notify the Help Desk or check the **[Insert Your Organization's Name]** intranet site.

- **Offensive and Inappropriate Material**
  - **[Insert Your Organization's Name]** employees may neither access nor distribute any material that could be considered inappropriate, offensive or disrespectful to others. Examples include material that:
    - contains sexually explicit images or descriptions,
    - advocates illegal activity, or
    - advocates intolerance for others.
  - Employees should obtain company directives from their managers.
- **Internet Use**
  - These rules apply to both the Internet and internal **[Insert Your Organization's Name]** intranet network.
  - Unprotected information posted on the Internet is available to countless unknown people worldwide, not all of whom support **[Insert Your Organization's Name]**.
  - **[Insert Your Organization's Name]**'s information, computing assets, and corporate image on the Internet must be rigorously safeguarded from loss, modification or destruction.
  - Using the **[Insert Your Organization's Name]**'s Internet access is regulated by policy. Any infringement can result in disciplinary action up to and including termination. Prohibited uses can include:
    - viewing or posting any material considered inappropriate, offensive or disrespectful to others,
    - using unauthorized file exchange or sharing of services (such as Napster, Gnutella, WinMX, LimeWire, BearShare, Morpheus and Kazaa),
    - trading securities,
    - gambling on-line or entering prize competitions,
    - downloading entertainment software or games or playing games, and

    - uploading software or data owned by or licensed to **[Insert Your Organization's Name]** without appropriate authorization.

  - **[Insert Your Organization's Name]** may block access from within our networks to any sites we determine are inappropriate for any reason. If you find yourself connected incidentally to a site that contains inappropriate material, you must disconnect from the site immediately.

  - Posting information about **[Insert Your Organization's Name]**'s employees, vendors, suppliers or partners without a valid business justification is prohibited. Posting personal opinions about **[Insert Your Organization's Name]**'s staff or affiliates is prohibited.

  - Revealing confidential or personal health information, and any other material on chat rooms is prohibited.

  - Downloading infected, unlicensed or unregistered software is prohibited.

- **Electronic Mail**

  - Electronic mail (e-mail) is a business tool that should be used with the same considerations for quality and appropriateness as any other business communication.

  - E-mail is the property of **[Insert Your Organization's Name]** and may be monitored or audited at any time to ensure compliance with Security Policies and Standards or for other reasons at management's discretion.

  - Employees may not represent themselves as someone or something they are not.

  - Sending, creating or storing offensive or disruptive material using email is strictly prohibited. Violating **[Insert Your Organization's Name]**'s business conduct guideline is also prohibited. Prohibited content includes, but is not limited to, racial or ethnic slurs, profanity, and messages containing sexually explicit language or graphics.

  - Any communication using **[Insert Your Organization's Name]**'s e-mail or Internet systems could be construed as representing **[Insert Your Organization's Name]**'s corporate position. Only duly

authorized individuals may speak or write on **[Insert Your Organization's Name]**'s behalf.

- Users must never attempt to gain access to another user's email messages without permission.

- Critical information should not be stored in email.

- **Representation of [Insert Your Organization's Name] using IT facilities (such as email or the Internet)**

  - Employees representing **[Insert Your Organization's Name]** must identify themselves accurately and completely (including their position and function where requested).

  - Any false representation of authority or engagement in unauthorized business is strictly prohibited.

  - Only duly authorized employees or officials may represent **[Insert Your Organization's Name]** and its policies in speech or writing to the media, analysts, or at public gatherings. Other employees may participate in newsgroups or chats in the course of business, when relevant to their duties, as individuals speaking only for themselves. Individuals participating who are identified as an **[Insert Your Organization's Name]** employee or agent must refrain from any unauthorized political advocacy, endorsement or apparent endorsement by **[Insert Your Organization's Name]** of any commercial product or service.

  - Electronic mail addresses may satisfy the requirement for a legal signature. Employees must avoid creating unwarranted contractual obligations. Where the possibility exists, a disclaimer must be included, indicating that official approval must be obtained before agreement.

  - **[Insert Your Organization's Name]** does not accept responsibility for the personal opinions its Internet users express. **[Insert Your Organization's Name]** does not act as a publisher; it simply allows the means to distribute statements its employees make. Employees with Internet access must understand how Canadian intellectual property, defamation and criminal laws may expose **[Insert Your Organization's Name]** to legal liability.

Security – People

- **Compliance With Legal, Statutory and Regulatory Requirements**
  - **[Insert Your Organization's Name]**'s facilities and computing resources must not be knowingly used to violate the laws of Canada or Ontario or of any other jurisdiction in any material way. Using institutional resources for illegal activity is grounds for immediate dismissal, and **[Insert Your Organization's Name]** will cooperate with any legitimate law enforcement activity.
  - Any software or files downloaded via the Internet into the **[Insert Your Organization's Name]** network become the **[Insert Your Organization's Name]**'s property. These files or software may be used only in ways consistent with their licences or copyrights.
  - No employee may knowingly use **[Insert Your Organization's Name]** facilities to download or distribute pirated software or data.
- **Malicious and Damaging Activities**
  - Employees must never use **[Insert Your Organization's Name]**'s Internet facilities to propagate any virus, worm, Trojan Horse or trap door program code.
  - Employees must never use **[Insert Your Organization's Name]**'s Internet facilities to disable or overload any computer system or network, or circumvent any system intended to protect another user's privacy or security. Employees also must never use **[Insert Your Organization's Name]**'s computing resources to gain unauthorized access to remote systems. Any attempts to do so will be reported to the remote systems' administrators and law enforcement personnel where warranted. Deleting, examining, copying or modifying other users' or entities' data or files without their consent is prohibited.
  - Employees must never run security-testing tools or programs against any Internet system or server.
  - Employees must never knowingly write or run any computer program or process (including email) that would consume more computer resources than needed to perform **[Insert Your Organization's Name]**'s work.
  - Employees must not use **[Insert Your Organization's Name]**'s network to perform an Internet transaction that may consume significant system resources and interrupt or delay system use.

Information Technology management must approve any repetitive or large data transactions.

Rules for Transmitting Personal Health Information using Fax Machines

- Transmit personal health information by fax only when no more secure practical alternative exists.
- When you do need to send a fax, always remove common identifiers, such as a patient's name and address (an ID number may be all that is required) from personal health information.
- Because the fax machine receiving your transmission may not be located in a secure area, always let your recipients know that you are about to fax sensitive material to them and confirm their fax number.
- Always include a cover page with your name, telephone number, date and number of pages sent.
- Carefully enter the fax number to ensure you do not misdirect the message and seriously breach someone's privacy.
- To avoid manual keying errors to routine destinations, use the fax machine's auto-dial features, if available.
- Confirm that the intended recipient has received all pages you sent.
- Immediately try to recapture any misdirected fax, and follow the guidelines in this Toolkit for handling a privacy breach if appropriate.

APPENDIX B – AUTHENTICATION AND AUTHORIZATION

Sample User ID and Access Management Practices

- Manage user IDs and access rights.
  - Appoint one person to approve user ID set-up and periodically review that access is required.
  - Make sure users immediately change temporary passwords to a password only they know when they first log on. Never issue temporary passwords that are easy to guess (like "welcome").
  - Transmit passwords securely and separately from information that identifies the user.
  - Immediately remove access when people leave or change jobs.
  - Never reuse old User IDs.
  - Use Identity Management software to manage this process where possible.
- Implement "need to know" access.
  - Give access only to those people whose jobs require access. (For example, those caring for or treating a patient would need to know the personal health information relating to their role in the patient's current primary care and treatment.)
  - Restrict access by the specific fields and range of records each person needs access to do the job. If the technology does not allow a fine enough degree of control, modify or replace the technology as soon as possible, using manual controls in the meantime. (This usually requires spot-checking for correct use of information after the fact).
  - Set default access to read-only (view), and add only where the job function requires more.
  - As the type of access needed increases, the level of approval should increase.

- Always consider whether the job can be performed effectively with either anonymous rather than personal information.
- Build access rules in terms of defined job roles, such as “emergency room physician” or “acute care nurse,” instead of evaluating individual requests.
- Consider other methods to support “need to know” access, such as:

Relationship Based Access Control	Location/ Method Based Access Control	Time Based Access Control
		
User has a particular relationship with the patient before access is granted, (e.g., attending physician)	Access may be denied if the request comes from an insecure location or method (e.g., no access from home)	Access is given only for specific times (e.g., no after hours access)

- Users with special support User IDs that provide more powerful access capabilities should:
  - have a regular User ID for when not performing support functions,
  - not have special IDs in both production and test/development environments, and
  - not have access to delete or modify audit logs.
- Systems should lock User IDs automatically after three failed logon attempts in a row and these events should be logged.

Sample Password Policy

Modify the following Password Policy to suit your environment and requirements, automating as many of the rules as possible.

Security – People

- Password Protection
  - Do not transmit user passwords in clear text form over the Internet, public networks or wireless devices. Passwords generated for an individual user must be conveyed to the user in a secure manner, such as in a telephone or face-to-face conversation, password-protected voicemail box or encrypted electronic mail, or by separating the password from its context (user ID).
  - A new password may be generated only after the system administrator or designated authority has positively identified the user.
  - When temporary passwords are issued for new or reset User IDs, the user should immediately change to a password no one else knows when first logging on.
  - Change default user IDs with default passwords shipped with operating systems and program products for use during system and product installation and set up as soon as possible during or following their initial use.
  - If possible, user passwords must be encrypted when stored in files or databases on systems and servers. If passwords cannot be encrypted, access to the file or database element containing the passwords must be restricted to only authorized system security administrators. If passwords are not encrypted during storage and transmission, they may be hashed with a one-way function. Hashing with a one-way function is considered acceptable protection for passwords when transmitted across a network.
  - Do not disclose to or share with anyone your password, including administrative assistants or secretaries, unless individual accountability can be maintained.
  - User password management is a condition of your employment.
  - Do not write your password down. If this is unavoidable and you must write it down, protect the writing containing your password as confidential information, keeping it in your possession or under lock and key at all times.
  - Do not store passwords in a file on any computer system (including Palm Pilots or similar devices) without strong encryption.

- Passwords must never be included in any automated log-on process (for example, stored in a macro or function key) or plain-text batch files residing on a user's local workstation to hasten log on without having to key the user-ID/password combination in.

- Close or log out of password protected web sessions as soon as you have finished with them.

- Password files for a system must be separated from other system and application data, and should never be available to non-administrative users.

- Passwords for critical systems and network components must be sealed and stored in a physically secured location to permit emergency use by designated personnel when necessary.

- Do not possess nor use any tool that would obtain, disclose or capture another user's password.

- Controls must be in place to prevent an unlimited number of invalid logon password attempts (like password hacking). This will be accomplished by either revoking or locking the user ID on the fourth consecutive invalid attempt or using a logon inductor to exponentially increase the amount of time between sign-on screens (to prevent automated tool password hacking).

- Passwords must be changed regularly (monthly or quarterly). Old passwords should not be re-used.

- If an account or password is suspected to have been compromised, report the incident and change all passwords.

- All unsuccessful authentication attempts will be logged.

- The Information Security Department or its delegates will perform password cracking or guessing periodically or randomly. If a password is compromised during one of these scans, the user will be required to change it.

- Password "Don'ts":

    - Never reveal your password to anyone including your manager, family members and co-workers, except as part of an authorized password management process.

- Never discuss your password in front of others or hint at your password's composition (for example, "my family name").
- Never reveal a password on questionnaires or security forms.
- Never use the "Remember Password" feature on applications (for example, Internet Explorer, Eudora, Outlook, Netscape Messenger).

- Password-cracking programs can break weak passwords in minutes. Observe these rules to build strong passwords.
  - Passwords should be at least 8 characters long.
  - Passwords should contain a mixture of letters, numbers and special characters (for example ! @ # $ %), if possible.
  - Avoid dictionary words within the password.
  - Avoid using passwords based on easily guessed ideas, such as birth dates, family or pet names, hobbies, sports or months.
  - Avoid keyboard sequences (for example QWERTY) and logical sequences (for example, ABC, 1-2-3, zyx, 10-9-8).
  - Avoid repetitive sequences (a number or letter used more than twice).
  - Do not use the same password for work and non-work User IDs (for example, personal ISP account, option trading, benefits, etc.). Avoid using the same password for multiple work User IDs.
  - Do not re-use old passwords.
  - Temporary passwords for new or reset User IDs should not be re-used (generate a new one for each situation) and should not be easy to guess (for example "welcome").

Security – Institutional Safeguards

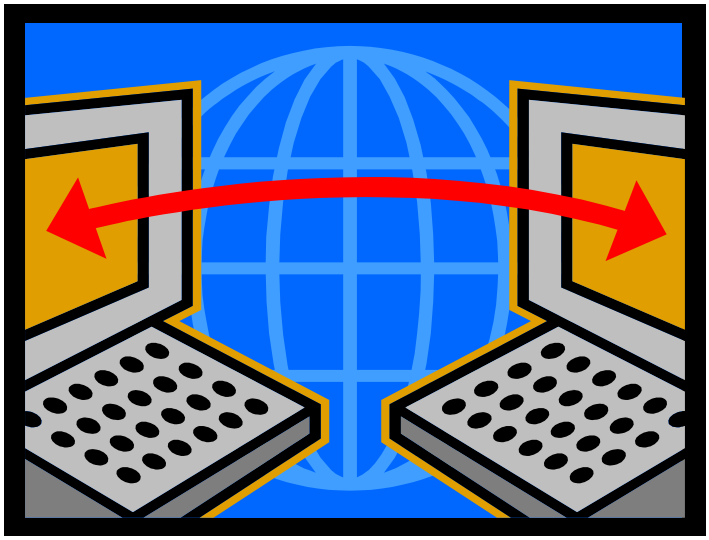


Table of Contents

Security – Institutional Safeguards

Key Points

To implement security effectively, you need a balanced approach that covers your staff, your administrative processes and your technology. This section deals with the steps needed to secure the institution. These steps have some implications for general users but would largely be carried out by IT professionals:

- Secure the physical and electronic (computer) points that provide access to personal health information.
- Use appropriate measures to protect information technology from malicious software.
- Implement an incident response plan to address any incidents that do occur.
- Put policies and procedures in place to reduce the security risks associated with wireless and portable devices.

Documents you should create as a result of carrying out these steps include:

- Malicious Software Policy (Appendix B)
- Malicious Software Guide (Appendix B)
- User Guidelines for Mobile Computing (Appendix C)
- An Incident Response Plan
- A Plan to Manage Computer or Digital Media Theft or Loss (Appendix A)

Perimeter Security

What You Should Do

Secure the physical and electronic (computer) points that provide access to personal health information.

Physical Perimeter Security

- Lock printed files and removable storage media (CDs etc.) containing personal health information in secure places.
- Use physical entry barriers to restrict access to personal health information to identified and authorized personnel. Examples include:
  - active supervision by a security guard or receptionist, or requiring visitors to sign-in, and
  - passive control through an automated security badge system, surveillance cameras or alarms.
- When printed health records are used outside the controlled area:
  - use a sign-out log to record who borrows the record,
  - tell them how the record is secured, and
  - check the sign-out log at the end of each day to ensure all records due back have been returned.
- Supervise third-party access (for example, cleaners, building security and landlords) to areas where personal health information is kept.
- Monitor printers and fax machines for documents containing personal health information or keep these devices in rooms with restricted access.
- Remove or encrypt any personal health information from computer equipment sent off-site for maintenance. Ensure those who service your equipment sign an agreement as well (see the Managing Contracts and Agents section).

- Use secure medical courier delivery services wherever possible for transporting personal health information.
- Use sealed containers to transport personal health information between secure facilities. Consider using packaging that reveals when it has been tampered with and check that quantities sent and received match.
- Secure centrally managed computing equipment and network cabling to prevent tampering or unauthorized connection of other devices.

Electronic Access Points

- Use network security measures, such as firewalls, to stop unauthorized traffic from entering your computer network.
- Segregate the network into different security zones to provide more protection for information that needs it. See Appendix A for details on Security Zones of Control.
- Use secure remote access methods, such as Virtual Private Networks (VPNs), to provide authorized users with secure remote access to your institution's network.

  Note: VPNs refers to technology that allows authorized users to send information over a public network, like the Internet, in a protected manner with safeguards equivalent to that of using the organization's private network.

- Do not tolerate unmanaged network access points (for example user-connected dial-up modems or wireless hubs).
- Erase or destroy personal health information stored on computer equipment when selling or disposing of the equipment. (Just using the "delete" or "format" function is often not good enough; you may need to destructively erase the storage devices, such as using a magnetic eraser, so the information cannot be recovered).

Small Office Applicability

- Keep physical files containing personal health information in an area that is locked and supervised when not locked.
- Watch printers and fax machines when in use or keep them in a locked area.

- Run up-to-date Personal Firewall software on all computers in your office that store personal health information.
- Destroy or destructively erase the storage devices on your computers when selling or disposing of the computer (just using the "delete" or "format" function is often not good enough).
- Make sure personal health information is not exposed when your equipment is serviced. Remove or encrypt any information that is not protected by a hard drive password when equipment goes off-site and have those servicing your equipment sign an agreement (see the Managing Contracts and Agents section).

Malicious Software

What You Should Do

Use appropriate measures to protect information technology from malicious software.

Implement an incident response plan to address any incidents that do occur.

Malicious software is designed to damage, break, overtake or steal information from your computers. It includes viruses, worms, Trojan Horses, logic bombs and spyware. Personal computers are especially vulnerable since most malicious software targets them directly. Protecting personal computers is vital.

- Implement a malicious software policy and provide simple rules for your staff to follow (See Appendix B for a sample policy and user guide).
- Develop an incident response plan to combat any malicious software attacks. Appoint one staff member to:
  - co-ordinate your response,
  - assess the incident's severity and scope,
  - identify the best way to address the incident,
  - tell staff what to do,

  - implement a business continuity plan to restore lost facilities, programs and data, and
  - implement long-term solutions.

- Track and implement any applicable updates software vendors develop to fix known security problems with their software.
- Larger institutions should consider workstation management software or services that automatically send vendors' fixes to all users.

Small Office Applicability

- Run up-to-date Anti-Virus, Firewall and Spyware software on all computers that store personal health information.
- Use the associated update service to ensure your software can catch the latest known viruses.

Wireless and Portable Devices

What You Should Do

Put policies and procedures in place to reduce the security risks associated with wireless and portable devices.

Portable devices include Laptop Computers, Personal Digital Assistants and Cell Phones.

- Do not use wireless devices (such as email or cell phones) to transmit personal health information unless the system is designed to support wireless devices securely (for example, with data encryption).
- Do not use portable devices to store personal health information, except systems designed to support portable devices securely.
- Instruct staff using portable devices outside of the secure work area to take precautions against theft and unauthorized access. Remind them that the "reader over the shoulder" is a real risk.

- If you do not have the skills on staff, get an IT security professional to help design and implement your wireless systems securely.

Small Office Applicability

- Assume wireless and portable devices are not secure unless you had a security professional set them up to be secure.
- Do not use wireless and portable devices to store or transmit personal health information. Cell phones are not secure and you need to be careful when deciding what information to discuss on a cell phone (use a regular phone whenever possible).

Related Sections of the Act

2, 3, 4, 10, 12, 13, 14, 42, 53

Checklists, Templates and Tools

Appendix A – "Perimeter Security" provides guidance on Security Zones of Control, LAN Management and Managing Computer Theft

Appendix B – "Malicious Software" provides a sample policy on malicious software and a sample guide for users

Appendix C – "Wireless and Portable Devices" provides a sample user guide and sample technical standards

APPENDIX A – PERIMETER SECURITY

Network Design – Security Zones of Control

The concept of security zones is most applicable to large institutions with complex networks serving many different types of user including the public and external suppliers. A security zone is an area where a defined set of security policies and measures combine to achieve a specific level of security. In a large networked environment it is usually better to define multiple zones that group computing resources with similar security requirements and cluster levels of risk together. Specific security mechanisms and policies outline the criteria that should be met to transit from one zone to another. Separating the zones ensures that security failures in less secure zones do not compromise more secure zones. Large organizations typically use the following zones.

A *Highly Secure Zone* is used to store or process sensitive, private or confidential information. Access is strictly limited to identified entities. Very stringent security mechanisms protect the Highly Secure Zone. User credential information (password files) and highly sensitive personal health information typically belong in the Highly Secure Zone. Any information requiring the highest confidentiality, integrity or availability should be considered for this zone.

An *Internal Zone* is used for storing and processing sensitive, private or confidential information. Security policies are strictly enforced, but access need not be as restricted as in the Highly Secure Zone. The Internal Zone includes the network, applications and facilities implemented to support internal systems. It also includes internal systems outsourced to external partners, but does not include systems that act as access points-of-entry for those partners.

The Internal Zone is subdivided into *Security Sub-Domains*. In general, a sub-domain is a logical boundary separating a collection of resources that must be separated from the rest of the security zones for some special purpose, but are still considered part of the larger zone. These sub-domains should not weaken the larger zone and may require additional security controls to isolate them from the common infrastructure. Note that Sub-Domains should be exceptions and limited in number.

A *Buffer Zone* (Internal Controlled) houses applications and services provided to give entities in the Public or External Business Zone access to less-sensitive resources. Security controls are applied at the Buffer Zone's entry points and between the Buffer and Internal Zones. No direct connection between the Public/External Business Zones and the Internal Zone is allowed (meaning all connections to the Internal Zone should be via the Buffer Zone).

External Business Zone (External Controlled) is where information and systems are shared with other institutions, stakeholders and external users. Equivalent security policies and standards are mutually acceptable and verifiable. The External Business Zone generally is another organization's infrastructure that your organization connects to for specified business activities. For instance, a regional hospital might link to local hospitals in this way.

In the *Public Zone* (External Uncontrolled), information and systems are open and uncontrolled. Security policies and standards cannot be enforced. A hospital's public website might represent such a zone.

Guidance For Managing Computer and Digital Media Theft and Loss

Most of the following steps for managing theft or loss should be taken before an incident occurs. Some of the steps address your options following a theft.

- Conduct a regular inventory of all of your IT equipment and assets and ensure sure you have the following information:
  - Owner Name
  - Description (brand, model, and features)
  - Location
  - Serial Number
- Larger institutions should consider using asset management software to inventory software assets on workstations.
- Map assets:
  - that support critical business functions within the Business Continuity Plan, and
  - containing the critical information identified in the Information Inventory and Classification section.
- Put Acceptable Use and other personal security policies in place that require staff to take protective measures, such as:
  - physically locking portable IT assets (including computers, PDA's, and portable media such as hard drives, CDs and USB memory keys) and keeping them hidden from view, and

  - using encryption for sensitive data and employing hard drive passwords.

- Take additional steps for very valuable assets and those containing very sensitive data:
  - Install GPS tracking devices.
  - Use storage devices that over-write data when tampered with.
- Establish a process to manage stolen or missing IT assets.
  - Designate a contact point for reporting stolen assets (such as a Help Desk).
  - Appoint a coordinator to:
- establish how critical the lost or stolen asset is,
  - contact law enforcement or tracking agencies as appropriate, and
  - tell those who may be affected of the asset's loss (see Section on Managing a Privacy Breach).

When an incident occurs, take the following steps:

- Report the incident to police and internal security (providing serial numbers).
- Lock any computer accounts associated with the asset.
- Notify managers of affected departments to stem any wider implications the loss may have.
- Notify your legal department and communications staff if you think any information leak may affect the public or clients so they can decide whether to alert regulators and draft a press statement.
- Review the incident (consider any motive involved and look at similar incidents).
- Consider prosecution if an individual is apprehended or identified.
- Review security practices to determine whether the incident could have been prevented.

Sample LAN Management Guidelines for Large Installations:

LAN stands for Local Area Network

Modify the following guidelines to suit your needs and own local area network.

LAN Management Physical Security

- Treat LAN devices like computers or servers and follow same physical and logical security rules for servers.
  - LAN devices should be house in a secure enclosure accessible to only authorized personnel.
  - Grant access to a LAN device following the same rules and restrictions for physical access to a server.
- Do not expose LAN cables or leave them open to unauthorized access, except at their terminal end when connecting to the user workstation.
  - Wiring closets and patch panels should be locked and accessible to only authorized personnel.
  - Cable runs should not be accessible from public-use areas. If cable runs are accessible, consider using positive-pressure sealed conduits.
- LAN connections should be available only inside internal areas with access restricted to authorized employees.
  - If LAN connections are needed in semi-public areas (like meeting rooms used for visitors or visitors' waiting areas) enable Media Access Control (MAC) address filtering on those ports to accept only connections from known machines. If policy-based networking has been implemented, stronger protections may be deployed.
  - If visitors need a LAN connection, it should be routed to a public network zone in the network (Internet) and not to the internal LAN.
  - Verify and audit physical port counts regularly.

LAN Management Logical Security

- Segment the LAN based on application and data usage. For example, Human Resources data should reside on servers on a different network than patient data.

- Intelligent LAN devices (for instance, large switches and routers) must be protected by passwords the same way and following the same rules as a server. Do not use default or generic passwords.

- Consider using an out-of-band management network to manage networked devices. If direct console access is necessary, use a terminal server with strong authentication options.

- Upgrade LAN devices using control software that can be maintained with patches as required.

    - Treat these LAN devices the same way as a server and apply the same procedures for maintenance and security patches.

    - Maintain strict controls on who may change these devices and keep backup copies of configurations in a separate backup location.

- Do not enable remote access to network devices.

    - If a valid administrative reason requires remote access, treat the access the same way as a server remote access, protecting it in the same way (using digital credentials, smartcard, or similar authentication mechanisms).

- Only authorized computers or servers should connect to the LAN.

    - At a minimum, if a computer or server not controlled by **[Insert Your Organization's Name]** must be connected to the LAN, it should be inspected and verified by **[Insert Your Organization's Name]** personnel to ensure no malicious elements (viruses, Trojan horses, etc.) are hidden in it.

    - For stronger protections, consider policy-based networking, which typically combines authenticating before end-users gain access to the network, enforcing security policies and standards, and verifying that the end-client is patched and up to date.

- No "shares" or folders should be visible or available in the LAN without a proper login using a password that follows **[Insert Your Organization's Name]** password rules.

    - LAN passwords should follow the same rules as other critical passwords and have similar expiry times.

- The protocols used in the LAN environment must be up-to-date and comply with the security policy. Avoid protocols that are obsolete or have known vulnerabilities. (For example, wherever possible, do not use basic SNMP, using common public and private community strings for access. SNMP versions 2 and 3 offer much more suitable authentication and encryption options).

- Dual homing (connecting a computer to two different networks at the same time) is not allowed, unless **[Insert Your Organization's Name]** controls both networks and the networks have identical security controls.

  - Dual homing exists when a single computer is connected to the LAN and another network, such as a wireless one, another LAN, or a dial-up.

- Control all outside access into the LAN from outside and deny access to unauthorized users.

  - Protect all connections to other LANs and the Internet with Firewalls.

  - Deploy Intrusion Detection Systems (IDS) in Internet connection points to detect unauthorized attempts to access the LAN.

  - Enable logging-in LAN devices whenever supported.

  - Archive access logs in a protected server and review them regularly. Review can be automated or manual, but should be at regular intervals. Reports should be generated if any event flags intrusion attempts.

- Disable all unused network ports.

- Disable all unnecessary protocols.

- Use anti-virus software, bandwidth throttling and other Quality-of-Service (QoS) mechanisms to help prevent and impede network-based malicious code from spreading.

Sample LAN Management Guidelines for Small Installations

Modify the following guidelines to suit your environment and your requirements.

LAN Management Physical Security

- Locate LAN hubs or switches out of the general public's reach.

- LAN access ports should not be accessible to the general public.
- Allow only authorized computers to connect to the LAN.

LAN Management Logical Security

- No critical “shares” or folders should be visible or available in the LAN without proper password protection.
- If the LAN is used to access the Internet, use a router with built-in firewall as the main access point.
- No computer should be connected to the LAN and another network (such as a wireless one or a dial-up connection) at the same time.
- Do not use default or generic passwords on networking equipment.

APPENDIX B – MALICIOUS SOFTWARE

Sample Policy for Protecting Against Malicious Software

Modify the following sample policy to suit your environment and your requirements.

- To protect the integrity of software and information, implement precautions to prevent, detect, and cleanse the introduction of malicious software.
- The following controls shall apply to all workstations (business or personal) used for **[Insert Your Organization's Name]** business:
  - A formal policy requiring compliance with software licenses and prohibiting the use of unauthorized software.
  - **[Insert Your Organization's Name]** supplied malicious software detection and repair software must on any workstation used for **[Insert Your Organization's Name]** business or connected to the **[Insert Your Organization's Name]** network.
  - Signature files routinely updated to within the two most recent versions.
  - Anti-virus software activated at boot-up time.
  - If supported by anti-virus software, automatic scanning is enabled.
  - Scanning any floppy or CD-ROM used for the first time.
  - Scanning any files on electronic media of uncertain or unauthorized origin, or files received over un-trusted networks, for viruses before use.
  - Scanning any electronic mail attachments and downloads for malicious software before use. This check may be carried out at different places, for example, at electronic mail servers, desk top computers or when entering the **[Insert Your Organization's Name]**'s network.
  - Employees may download data from known and trusted suppliers after following the virus-checking process and using the approved virus detection package.

- Staff are trained for security awareness, covering the virus protection on systems, training in their use, incident reporting procedures, and recovering from virus attacks

- Appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements.

- Users are instructed not to intentionally write, generate, compile, copy, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any computer's memory, file system or software.

- Computer users are instructed to not knowingly write or run any computer program/process that would consume more computer resources than necessary for performing **[Insert Your Organization's Name]** work.

- Users are aware of the dangers of browser executable code and active scripts

- Browsers' ability to run ActiveX, JavaScript, Java and other forms of active scripts of code are disabled, where feasible.

- Users know to allow executable code and active scripts to be run from only trusted sites.

Sample Malicious Software Guide for Users

Modify the following sample to suit your environment and your requirements.

- Do not remove or alter the anti-virus software installed on your computer and do not shut down its regular scanning activity. Contact the Help Desk if you suspect it is not running correctly.

- If you suspect your computer has a virus, contact the Help Desk immediately, inform you manager and do not use your computer again until you get further instructions from the Help Desk

- Do not respond to any instructions for dealing with viruses that are not from the Help Desk or not posted on our intranet site.

Security – Institutional Safeguards

- Do not send colleagues any instructions for dealing with viruses you receive. The instructions may not be appropriate for them. Our virus response team will handle all communications.
- Beware of unexpected e-mail and e-mail from someone you do not know. Attachments may contain a virus.
- Never use web-based e-mail at the office or download software from the Internet. These files are not scanned for viruses.
- Always scan for viruses files downloaded from the Internet, e-mail attachments, CDs, DVDs, and diskettes.
- Always scan new software for viruses before installing it on your computer.
- As a precaution against a virus attack, make sure your critical files are backed up and retrievable.

APPENDIX C – WIRELESS AND PORTABLE DEVICES

Sample User Guidelines for Mobile Computing

Modify the following guidelines to suit your environment and requirements.

- **Laptop Computer and Travel Security**
  - Always use a cable lock to secure your laptop to your workstation
  - Keep your laptop in your possession as far as possible when travelling.
  - When traveling by air, do not check laptops in as baggage, and be alert to the possibility of theft when going through airport security checkpoints.
  - Never leave your laptop for an extended time in an unoccupied vehicle. If you must leave your laptop in an unoccupied vehicle, ensure it is not visible and secure the laptop to the body of the vehicle inside the trunk with a locking cable.
  - Avoid leaving your laptop in a hotel room. If you must, lock it in the hotel safe or use a locking cable to secure it out of sight in your room.
  - If you are traveling with **[Insert Your organization's Name]** sensitive or confidential material on portable media such as paper, diskettes, notebooks, or other devices, protect this media following the same guidelines listed above for protecting your laptop.
  - Do not work in open public areas where others may view user IDs, passwords, or **[Insert Your organization's Name]** data. (Be especially cautious on airplanes).
  - Never discuss **[Insert Your organization's Name]** confidential information in public areas where you may be overheard, including in conversations on telephones or cell phones.
  - Report the loss of any mobile device containing **[Insert Your organization's Name]** information to the Help Desk immediately.

Security – Institutional Safeguards

- **Security of Handheld Devices**

  - Hand-held devices (such as Personal Digital Assistants, RIM BlackBerry, and mobile phones with data access) storing or accessing **[Insert Your organization's Name]** confidential or business-sensitive data require physical and electronic access controls. The following actions are required:

  - Keep handheld devices in your possession whenever possible.

  - Activate data encryption, power-on password and password-controlled time-out/lock-out features on all hand-held devices supporting these security features.

  - Remote synchronization via modem to move the **[Insert Your organization's Name]** data between the device and your workstation must go through a **[Insert Your organization's Name]** authorized remote access gateway.

- **Wireless/Remote Network Access**

  - Use only **[Insert Your organization's Name]**'s approved remote network access facilities to gain access to the network from outside the office.

  - Ensure that you are not connected to any other network (for example via dial-up modem) at the same time you are connected to the **[Insert Your organization's Name]** network.

  - Never use publicly available wireless networks (often referred to as "hotspots"), unless you (a) have adequate perimeter and antivirus controls and (b) are not transmitting sensitive **[Insert Your organization's Name]** information.

  - Only **[Insert Your organization's Name]** approved and installed Wireless technology is permitted on any **[Insert Your organization's Name]** machine or within **[Insert Your organization's Name]**'s environment. Installation of personal wireless technology into the **[Insert Your organization's Name] environment is considered to be a serious breach of [Insert Your organization's Name]** security policy.

Sample Technical Standards for Wireless Connections

Modify the following sample to suit your environment and requirements.

- Cellular-based wireless is assumed to be public and untrustworthy. **[Insert Your organization's Name]**'s secure remote access mechanisms must be used to access **[Insert Your organization's Name]** resources over cellular-based networks.
- The following standards must be observed for all wireless LANs:
  - Unless explicitly for public-access use only, open wireless LAN networks must not be deployed. If public-access wireless is deployed, it must be adequately isolated from the other parts of the network.
  - Simultaneous wireless and wired connections on the same machine are prohibited.
  - Wireless Access Points must be isolated by firewalls and application proxies.
  - Sensitive applications and data should not be available via wireless connections unless additional layers of security have been added at OSI Layer 2 (WPA, EAP, LEAP, PEAP) and OSI Layer 3 (IPSEC VPN Tunnel).
  - Mitigate basic potential exposures created by the passive interception of wireless network traffic. Some exposures can be mitigated through good wireless network management, including:
    - MAC address filtering must be used to prevent unauthorized clients from connecting through wireless LAN access points. While these addresses can be imitated (spoofed), this does protect against casual attacks and unintentional client associations.
    - Service Set Identifier (SSID) broadcast must be disabled or the beacon interval must be increased to the maximum interval. As these broadcasts can be intercepted, naming conventions (for SSID, status fields, for instance) must not reveal any information (such as department or company name). Default (vendor-supplied) SSIDs are not permitted.
    - Connections from "null" or "any" SSIDs must be denied.
    - Default administrative passwords must be changed to strong passwords. This should include SNMP community strings accessible from the wired side of any Access Point.

    - All unnecessary protocols on the Wireless Access Point must be disabled (including ad hoc networking capability). Adhoc networking (peer-to-peer) must also be disabled on all **[Insert Your Organization's Name]** wireless LAN clients.
    - Management of Wireless Access Points from any wireless interface must be denied. Access Points may only be managed from wired terminals.
    - IP and MAC address filtering must be used to manage Wireless Access Points.
    - SNMP traps must be set on Wireless Access Point resets or configuration reloads.

- 802.11i Wireless LANs must be deployed where possible to provide the highest level of confidentiality and integrity protections currently available. It combines:
    - strong authentication and/or encrypted authentication channels for single-factor encryption, and
    - robust cryptographic services based on the Advanced Encryption Standard (AES).
- If 802.11i is not supported, WiFi Protected Access (WPA) may be used as it provides:
    - the same cryptographic services as standard wireless LANs but with changing keys to help prevent compromise, and
    - strong authentication and/or encrypted authentication channels for single-factor encryption.
- Where 802.11i and WPA are not supported, an exception to this standard must be obtained. At a minimum, these exceptions must:
    - support strong user-based authentication,
    - enable 128-bit (or higher) WEP encryption, and
    - change default WEP keys to a random value and rotate bi-weekly.
- WEP-based protections must be used for home use. At a minimum, 802.11i and WPA Home Edition are strongly recommended (versions not requiring strong authentication are available).

Sustaining Security

Table of Contents

Key Points

To implement security effectively, you need a balanced approach that covers your staff, your administrative processes and your technology. Security is also an ongoing program and not a one-time project. This section deals with the steps needed to sustain security:

- Ensure critical functions can operate and critical data is protected if local disasters or major technology failures cripple your systems.
- Institute policies to ensure security is considered when developing, buying and maintaining IT resources.
- Regularly audit your actual practices for compliance with your security policy.

Documents you should create as a result of carrying out these steps include:

- Data Backup, Disaster Recovery and Business Recovery Plans (Appendix A)
- Guidelines for Secure Applications (Appendix B)
- Any relevant Threat Risk Assessments (Appendix B)
- Security Review, Spot Check and Audit Results
- A Strategy for Capturing and Using Audit Information (Appendix C)

Business Continuity

What You Should Do

Ensure critical functions can operate and critical data is protected if local disasters or major technology failures cripple your systems.

- Analyze the data and critical systems you need to maintain your operations if the technology fails.
  - Identify key personnel for each critical process, such as health records transfer, who can best identify the systems, staff and data needed to run the process and give specific advice.
- Build backups to support infrastructure, such as:
  - computing facilities (for example third-party hot-site backup and mutual arrangements with other institutions), and
  - power (for example emergency generators, UPS systems, and dual-power feeds).
- Develop a Data Backup plan for critical and highly critical data that includes schedules for backups to be sent to a secure off-site storage facility.
- Secure information being transferred to the off-site facility.
- Ensure the data is secure while in off-site storage.
- Develop a Disaster Recovery Plan describing how basic operations (for example, health, office, computing, power, and communications) will run and how data will be restored from backup. Ensure that key staff securely store copies of the plan at home or off site.
- Develop a Business Recovery Plan describing how to restore critical business processes after the Disaster Recovery Plan.
- Include specific recommendations from key personnel. Since you may not have computers available, develop temporary manual procedures. Designate deputies for key staff who may be unavailable.

- In your plans, identify which activities depend on others and the order in which they should be performed.
- Inventory your data (as suggested in the Inventory and Data Classification section) and measure how critical each set is based on the risk analysis. Critical data covers not only personal health information, such as patient records, but also the procedures that protect your institution.

For example:

Not Critical: losing data will be a mere inconvenience with no significant impact

Critical: losing data will cause severe disruption of operations, potential losses and legal liability

Mildly Critical: losing data will inconvenience the institution, but will not cause significant loss or risk liability

Highly critical: losing data will mean institutional failure, risk of injury or loss of life, or criminal liability

- Test your plans once or twice a year to make sure they still work and that backup data is useable.
- The parts of your plans that cannot be tested in practice should be "paper" tested, with all staff involved walking through the plan together to identify potential problems.

Small Office Applicability

- Regularly back up critical personal health information on your computers to removable media (for example CD) at least monthly.
- Store these back-up copies in a secure off-site location. Secure the copies in transfer.

- Periodically test back-up copies before storing them to ensure they are useable. You do not want to find useless copies when you need the back-up.

Development and Maintenance

What You Need To Do

Institute policies to ensure security is considered when developing, buying and maintaining IT resources.

- Spell out the security requirements that IT systems and software should meet to support your security policy. Specify the audit information that you need to check that specified requirements are met.
- We recommend that you follow the HL7 (Health Level 7) standard for application interconnection in any application managing health records (see the Security Standards section).
- Perform a Threat Risk Assessment (TRA) and a Privacy Impact Assessment (PIA) for any major change to systems or software to identify and address any security and privacy concerns (see Appendix B for a sample TRA form). Include appropriate security questions in your normal application development and IT purchasing processes.
- Ensure that all built-in hardware and software security features in the IT products you buy are used properly (including changing administrator passwords from their default values).
- Separate any development, test and production environments. Strictly control the transfer of code between these environments with a rigorous change control process to avoid introducing new security risks.
- Do not use personal health information from your system to test changes in your test and development systems. Strip identifying details from information used outside your environment.
- Regularly monitor software updates and implement code updates designed to address security vulnerabilities.

Small Office Applicability

- Buy software from only reputable vendors. Professional journals and organizations like the Ontario Medical Association may suggest software for practices like yours.
- Promptly install any updates vendors offer to close security vulnerabilities.

Audit

What You Need To Do

Regularly audit your actual practices for compliance with your security policy.

We interpret audit broadly in this section to mean any review of current practices against policy or standards. This includes spot checks to make sure staff with access to personal health information are protecting it appropriately.

- If you have never audited security, conduct a "gap analysis" review.
  - A "gap analysis" review compares a target of acceptable security practices with current practices, revealing a list of gaps between the two.
  - The list of gaps identifies issues needing immediate attention and constitutes a baseline for future audits.
- The Diagnostic Tool in this Toolkit can be used for a preliminary assessment of security gaps. However, we suggest hiring outside experts to conduct the initial audit if your staff lacks the skills. You can always require the experts to train staff if you wish to perform future audits yourself. Do periodic external audits to make sure you keep pace with technology, standards and what similar institutions are doing.
- Conduct security audits at least annually. If internal staff will conduct the audit, choose individuals:
  - without day-to-day responsibility for the practices, and

  - with appropriate skills and current knowledge of security issues, practices and threats.

- A Security Audit should focus on how well actual security practices compare with the institution's security policy, standards and procedures.
- Use random spot checks to help ensure security policies are being followed and determine whether users are following Acceptable Use Policies, such as locking up sensitive information and locking computers.
- Audit the performance of any third parties handling personal health information on your behalf to make sure they meet the security requirements your agreement specifies.
- Perform Threat Risk Assessments (TRA) and Privacy Impact Assessments (PIA) whenever you make major changes to systems or software to make sure you have addressed any security and privacy concerns (a sample TRA form is included with this Toolkit). Follow up and resolve any problems.
- Your audit results and action plans to correct security risks should be:
  - regularly reviewed within the institution's management system (for example monthly senior management operations review), and
  - built into individual managers' performance measures and evaluation systems.
- Make sure you consider problems that will take time to resolve within the institution's risk management process and get the appropriate senior manager to sign off on the risks.
- Design your systems to give you all the information you will need for audits. (Appendix C contains suggestions.)
- Perform both external and internal security penetration tests (sometimes called ethical hacking) at least annually. (You may need to hire outside professionals to provide the necessary expertise and objectivity for the tests).
- Evaluate your security audit program's effectiveness by reviewing:
  - actual security incidents and determining whether your audit program should have caught them, and
  - staffing levels compared with those at similar institutions having effective security programs to ensure your resources are in line.

Appendix C – "Audit" provides more detailed guidance on capturing and using audit information.

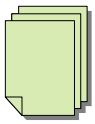
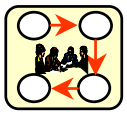
Small Office Applicability

- Perform spot checks on a regular basis to ensure all staff are following the security rules and take appropriate action.

Recommended Standards

What You Need To Know

The emerging international cross-industry standard for security is ISO/IEC 17799. Details of the standard can be found at www.iso.org. The 10 core areas of the framework are summarized below. The topics covered in the above security sections fit into this framework.

Policy	Organization	Asset Classification and Control	Personnel Security	Physical Security
				
Security rules the organization follows	Management framework supporting the policy and ensuring compliance	System to inventory and classify assets so they may be more effectively managed and protected	Rules to reduce the risk of individuals compromising security	Measures to prevent unauthorized access and damage to systems

Sustaining Security

Computer and Network Management	System Access Control	System Development and Maintenance	Business Continuity	Compliance
				
Disciplines to manage IT resources to support security objectives	Mechanisms to ensure that only authorized personnel have access and for only authorized purposes	Disciplines to ensure the IT environment sustains the required security levels	Plan to ensure that critical business activities can be performed if technology fails or local disasters happen	Program to ensure that security measures meet policy and legal and contractual security requirements

Other recommended standards and guidelines include:

- **ITIL (IT Infrastructure Library).** This widely accepted approach to IT Service Management provides comprehensive guidance on best practices for the processes required to support IT, including those critical to security such as Change Management. More details can be found at http://www.ogc.gov.uk/index.asp?id=2261

- **COBIT (Control Objectives for Information Technology).** This widely accepted standard for good Information Technology (IT) security and control practices provides a reference framework for management, users, and IS audit, control and security practitioners. More details can be found at http://www.isaca.org/

- **COACH (Canada's Health Informatics Association).** The COACH-published "Guidelines for the Protection of Health Information," which supplements this Toolkit, provides more detail on how to implement security in a healthcare setting. More details can be found at http://www.coachorg.com/

- **RCMP Guidelines for Threat Risk Analysis (TRA).** Details on this tool for identifying and mitigating security risks can be found at http://www.rcmp-grc.gc.ca (Also see Appendix B for a sample TRA form.)

- **HL7 (Health Level 7).** We recommend any applications managing health records meet the HL7 (Health Level 7) standard for application interconnection. Based on the ISO OSI (Open Systems Interconnection) Level 7 application interconnection standard, this standard is gaining wide acceptance and includes security checks. More details can be found at http://www.hl7.org.

Related Sections of the Act

2, 3, 4, 10, 12, 13, 14, 42, 53

Checklists, Templates and Tools

Appendix A – "Business Continuity" provides a sample Business Recovery and Disaster Recovery Management Guide

Appendix B – "Development and Maintenance" provides more detailed guidance on Secure Applications and a sample TRA form

Appendix C – "Audit" provides more detailed guidance on capturing and using audit information

APPENDIX A – BUSINESS CONTINUITY

Business Recovery and Disaster Recovery Management Guide

1. Establish a Business Recovery and Disaster Recovery Management Process. A Business Recovery and Disaster Recovery management process must be implemented across the organization to reduce an interruption's effects to a level acceptable by service unit management and regulatory authorities.

- Assign a staff member responsibility for Business Recovery planning (Business) for the institution. Also appoint individuals within each service unit performing critical functions and sub-functions.
- Assign a staff member responsibility for Disaster Recovery planning (IT).
- Identify service units critical to the organization, based on criteria management agrees to.
- Define a Business Recovery group with members from each service unit to ensure that adequate recovery plans are instituted and kept current as the business changes.
- Make the Business Recovery group responsible for ensuring that staff from each service unit are assigned and trained on Business Recovery and Disaster Recovery processes and procedures.
- Involve assigned staff in testing the recovery plan (at least annually)
- Review the institution's insurance coverage annually for opportunities to use coverage as an alternative way to manage the risk of an interruption or the organization's response to an interruption

2. Perform a Business Recovery and Disaster Recovery Impact Analysis. Business Recovery and Disaster Recovery planning must be based on the results of a Recovery Requirements Analysis that assesses the impacts of interruptions to critical service. Determine the resources on which those critical functions rely and the maximum period of interruption each critical function can withstand.

- All service units must participate in the Recovery Requirements Analysis.
- The threshold for a critical service unit is based on an analysis of the impact of interruptions to its services and the maximum time those services can withstand interruption.

- Develop strategies to determine the overall approach to Business Recovery and Disaster Recovery and have management endorse them.
- Establish a budget for contingency planning.

3. Develop and Maintain the Business Recovery and Disaster Recovery Plans. Business Recovery and Disaster Recovery Plans will be documented for each service unit identified in the Recovery Requirements Analysis. The plans should:

- include the requirements for alternate sites, hardware, software and service unit specific items,
- make saving human life top priority,
- be supported by documented Crisis Management and Emergency Response procedures and responsibilities,
- include detailed procedures on the tasks the management team must perform when declaring a disaster,
- include detailed procedures on what each service unit must do when a disaster is declared,
- specify authority for activating recovery strategies, such as an alternative location (hot-site) and assign authorities for other specific functions,
- identify the budget that will be made available when declaring a disaster and how the expenditures will be managed during the interruption,
- identify how staff will be informed of the disaster and given instructions on what they should do,
- include the types and frequency of testing required, and
- include maintenance to ensure that currency with business processes and priorities and resource changes.

4. Test the plans. Regularly test Business Recovery and Disaster Recovery Plans to ensure they are up to date and effective.

- Test the plans at least annually or when major changes occur in the organization, priorities or infrastructure
- Testing should range from the following:
    - Table-top dry runs.

  - Simulation testing.
  - Parallel system running.
  - Partial cut-over testing.
  - Full contingency testing.

- Testing may be either planned or unplanned.
- Testing should occur with different staff to ensure cross-training.

5. Maintain and re-assess the plans. Business Recovery and Disaster Recovery plans must be kept current with the business. Use a change management and control process to make sure the plans reflect the organization's current needs. The following changes could affect the plans:

- People with responsibility within specific plans changing functions within the organization
- New business strategies
- New location, facilities or resources
- Amendments to applicable legislation
- New key vendors, personnel, supplies, management or customers
- New service unit processes or priorities
- A service unit providing different services (which could alter whether the unit is designated as a critical service unit).

APPENDIX B – DEVELOPMENT AND MAINTENANCE

General Guiding Principles for Secure Applications

These principles are written for application designers but can also be used to evaluate an application that is being purchased.

- **Avoid Security Through Obscurity.** Assume hackers will inspect source code and design applications accordingly. Secrets, such as hidden fields and path names, may slow an attacker down, but secrets do not stay secret forever. Application security based on "security by obscurity" is doomed to fail.

- **Principle of Least Privilege.** Do not require the application to run on the administrator account. Use coding discipline to determine what privileges actually needed and explicitly grant only the privileges to the non-administrator account on which the application runs.

- **Principle of Least Trust.** Do not trust input external users provide. Assume that external systems are insecure. Vet data and inspect every return code from every function call, including system library routines.

- **Separate Services.** Dedicate a single service to a single platform. Though it may cost less to run multiple services on the same platform, doing so increases the system's overall complexity and increases security vulnerabilities.

- **Principle of Simplicity.** Ensure that security subsystems are manageable and not overly complicated for users and administrators. Large interfaces and complex solutions run a higher risk security vulnerabilities than small interfaces and simple code. The more entrance points available to an application and the more intricate the application's functionality, the higher the potential for bugs, some of which will be security-related. Security functionality added to an application must be easy to install, configure, and use. Otherwise, it will be disabled or bypassed.

- **Avoid a Single Point of Failure.** Applications should never be designed so that a single mechanism failure (such as a firewall or authentication service Failure) jeopardizes the entire application. Also called Defence in Depth, this principle recommends a design where a second mechanism that must be defeated before one mechanism's failure can compromise the application, a third must be defeated if a second fails, and so on. A Buffer Zone is an example of more than single-point failure. If the outer firewall fails, though the web server may be vulnerable and compromised, the rest of the application and data remains safe behind a second firewall.

- **Secure Defaults.** Do not enable services by default unless absolutely necessary. Services should be disabled by default and enabled only by an explicit decision. The default settings should be the secure mode of operation. Security should not have to be turned on; it should always be present unless explicitly disabled.

- **Fail in a secure mode.** Ensure that applications, systems, and subsystems fail in a secure manner. This is called failing closed (as opposed to failing open). Write code to explicitly verify what is allowed before allowing it. Do not attempt to check for the cases where things are disallowed; an event may be missed and the application could fail in a non-secure mode because the failure was not recognized.

  - Examples that translate this principles into design features include:

  - Systems and applications should not store passwords in unencrypted form.

  - Systems and applications should centrally manage time-outs of inactive sessions used to access health information.

  - Applications should have input controls to ensure valid data and prevent data input from causing error conditions.

  - Applications should avoid writing personal information to client devices.

  - Applications should be able to capture and honour any patient consents such as lock-box provisions.

  - Applications should minimize the possibilities for unauthorized transmission, print or cut-and-paste copying.

Sample Threat Risk Assessment Form

Use this sample Threat Risk Assessment (TRA) Form based on RCMP/CSE Methodology. Although a row of sample data is provided, refer to the RCMP website for more guidance. If you have never performed a TRA, consider using outside professional help for your first one.

1. Asset Characteristics							
		Statement of Sensitivity				Effect if Compromised	
#	Description	Value	Confidentiality	Integrity	Availability	Privacy Impact	Potential Loss
1	EHR Database Server	$35K	High	High	High	High	Service, financial, legal, trust
2							
3							

2. Threat Assessment						
#	Threat Details		Exposure			
	Nature	Class	Likelihood	Loss	Impact	Exposure Rating
1	*Server Failure *Computer Component Failure *Criminal Activity *Hacker Activity *Staff Termination *Tampering *IT Malfunctions *Penetration *Theft of Equipment *Theft of Data *Modification of Data *Cryptographic Failure	Disclosure Interruption Modification Destruction Removal / Loss	Medium	Confidentiality Integrity Availability Privacy	High	High
2						
3						

3. Risk Assessment (Current State)				
#	**Safeguard**	**Effectiveness**	**Vulnerability**	**Risk Level**
1	*Identification *Authentication *Authorization *Training *Structural access protection *Climate control *Fire detection/sprinklers *Encryption *Auditing *Testing procedures *Change control procedures *Virus scan *Emergency and contingency planning *A secure physical environment *Limitation of physical access to the server *Strong database management skills *Data reconstruction procedures *Personnel security screening	Medium	Medium	Medium
2				
3				

4. Residual Risk				
#	Mitigation		Outcome	
	Recommendations	Mitigated Risk Level	Decision	Implemented
1	*Applications that draw on information stored within a database, will use the authentication and access controls for authorization provided by the security framework. *Ensure that a Threats and Risks Assessment has been approved for each associated application. *The Database Server should be protected by a firewall for security	Low	Accepted	Yes
2				
3				

APPENDIX C – AUDIT

Guidance on Capturing and Using Audit Information

- Design your processes and systems to capture information from the sources you will need to audit against, such as:
  - application logs (for applications that process personal health information),
  - system logs,
  - network logs,
  - exception logs (for example, failed logon attempts),
  - operator logs,
  - badge access or sign-in logs for restricted areas, and
  - sign-out logs for hardcopy personal health information.
- Make sure these logs contain the information required for your audit analysis and keep them secure.
  - Collect identifying information, such as User ID, the time and date, terminal location, resource being accessed, application being used, and the action being taken on personal health information (for example, view, update or delete).
  - Collect event information, such as failed access attempts, intrusion alerts and other management alarms, policy violations (for example, firewalls) and system failures.
  - Do not store logs on the same server being monitored.
  - Protect logs against destruction or unauthorized changes (users with privileged support IDs should not be able to alter or erase logs).
- Determine a strategy for using the audit information you collect:
  - Start with exceptional incidents where the record captures potentially threatening events, such as excessive failed access attempts.

- Adopt a spot-checking approach, such as reviewing the activity of a user ID (especially privileged IDs) over a period of time to check for regularity. review access to particular records to ensure appropriateness. Access to some records may be worth watching more closely than others (for example those of a well-know politician, celebrity or senior manager).

- If the spot-checks reveal many potential problems or miss problems discovered through other means, increase the frequency.

- Whenever possible, use automated tools to scan the logs and find correlations that may indicate possible intrusion attempts, unauthorized or illegal activities, or suspicious events, such as activity beyond normal bounds of a job role, that require further investigation.

Research

Table of Contents

Key Points

- The Act sets out specific requirements for the collection, use and disclosure of personal health information for research that is conducted without consent.
- The research provisions of the Act apply to:
  - *researchers*, who *collect* and *use* personal health information for research purposes,
  - *health information custodians* (such as hospitals and physicians), who *disclose* personal health information for research purposes, and
  - *research ethics boards*, who review and approve research plans.
- This Toolkit uses the term "you" for the sake of brevity. In this section, the term "you" refers to the health information custodians and researchers reading this section, who must observe the Act's requirements concerning research in their respective roles.
- You may *collect* personal health information for research purposes without consent from non-health information custodians who are not prohibited by law from disclosing the information to you, and from health information custodians who are permitted or required by law to disclose the information to you. Before collecting the information without consent, you must comply with the Act's requirements concerning research plans and research ethics board approval.
- You may *use* personal health information for research purposes without consent if a law permits you to do so. To use personal health information for research purposes without consent, you must comply with the Act's requirements concerning research plans and research ethics board approval. When conducting research under the approved research plan, you must follow the research duties that are listed in the Act.
- You may *disclose* personal health information to a researcher without consent; however, before disclosing the information to a researcher, you must enter into a written agreement with the researcher to protect the information, and receive from the researcher a written application, a written research plan and a copy of the research ethics board's approval of the research plan from the researcher. You may also impose any other obligations on the researcher that you feel are appropriate.

Research

The Rule

You may collect, use and disclose personal health information for research purposes without consent, but only if you meet the strict conditions described below.

- The research provisions of the Act apply to:
  - *researchers*, who *collect* and *use* personal health information for research purposes,
  - *health information custodians* (such as hospitals and physicians), who *disclose* personal health information for research purposes, and
  - *research ethics boards*, who review and approve research plans.
- This Toolkit uses the term "you" for the sake of brevity. In this section, the term "you" refers to the health information custodians and researchers reading this section, who must observe the Act's requirements concerning research in their respective roles.
- The Act has rules on dealing with personal health information, but does not have specific rules on dealing with specimens. You should follow standard best practices when dealing with specimens in research, in addition to the rules in the Act.
- This section of the Toolkit deals with retrospective research for which consent is not obtained. It does not discuss clinical trials, genetic testing or other studies, for which express consent is required.
- This Toolkit only deals with privacy issues. A discussion on other ethical issues relating to research, including risks and harms, is beyond the scope of this Toolkit.
- Nothing in the Act prevents you from collecting, using or disclosing personal health information for research purposes with *express consent*. You may not rely on *implied consent* to collect, use or disclose personal health information for research purposes.

What You Need To Do

Collection

You may collect personal health information for research purposes indirectly and without consent:

- from non-health information custodians (such as family members) who are not prohibited by law from disclosing the information to you,
- from health information custodians who are permitted by law to disclose the information to you, and
- if you are permitted or required by law to collect the information indirectly and without consent.

However, before doing so, you must comply with the Act's requirements concerning research plans and research ethics board approval (which are described below).

The person disclosing the information will ask you to enter into a written agreement concerning protection of the information (which might address the information's use, security, disclosure, return or disposal).

Note: If someone within your hospital provides the information to you, you will likely be asked to sign a Confidentiality Agreement. If someone external to the hospital discloses the information to you, you will likely be asked to sign an Information Sharing Agreement.

Use

You may use personal health information for research purposes without consent if a law permits you to do so.

However, when doing so, you must:

- conduct your research under a research plan that a research ethics board has approved (as described below), or
- follow the rules for research approved outside Ontario (as described below) if the personal health information originates outside Ontario.

When using personal health information for research purposes without consent, you must submit a research plan to a research ethics board outlining your anticipated use of the information.

Once a research ethics board approves your plan (or, in the case of information originating outside of Ontario, a similar research approval body), you must follow the Researcher Duties described below.

If you do not have a research ethics board at your facility, you must have some other research ethics board approve your research plan.

Disclosure

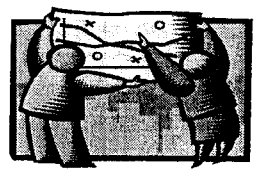
You may disclose personal health information to a researcher without consent if you enter into a written agreement with the researcher to protect the information (which may address its use, security, disclosure, return or disposal) (for disclosure outside the hospital), and receive from the researcher:

- a written application,
- a written research plan (meeting the requirements described below), and
- a copy of a research ethics board's approval of the research plan.

The discretion to grant requests for disclosure remains with you and you may impose additional obligations on the researcher.

Research Plan

The research plan must describe all of the matters listed on the Research Approval Checklist.



Research Ethics Board Composition

A research ethics board must be composed of at least five members, including:

an independent member

a member knowledgeable in research ethics

two members with relevant expertise in the research

a member knowledgeable in considering privacy issues

Research Ethics Board Duties

A research ethics board reviews research plans prepared by researchers. Members of a research ethics board must not review proposals with which they have a conflict of interest.

If the research ethics board is deciding whether to approve a research plan for research to be conducted without consent, it must consider everything relevant, including:

- whether the researcher could reasonably achieve the research goals without using personal health information,
- whether the researcher will put adequate safeguards in place to protect privacy and preserve the information's confidentiality,
- the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose information is being disclosed, and
- whether it would be impractical to require the researcher to get the affected individuals' consent.

A research ethics board should ensure that it considers all matters listed on the Research Approval Checklist. Once it makes a decision, a research ethics board must explain to the researcher in writing:

- whether the research plan has been approved,
- why it has been approved or denied, and
- if approved, whether the approval is subject to any conditions.

Researcher Duties

As a researcher, you must:

- comply with the approved research plan, including any conditions imposed by the research ethics board,
- implement the safeguards for protecting the information (see security and storage guidelines) outlined in your plan,
- use personal health information only for the purposes described in your research plan,
- not publish personal health information in a way that could reasonably allow others to identify the individual whose information was used in the research,
- only disclose the information when required by law,
- not contact individuals whose information is used in the research unless they have given consent to the disclosing health information custodian to be contacted by you (even if personal health information you hold is stolen, lost or accessed by unauthorized individuals),

  Note: The health information custodian who collects the information would obtain this consent.

- comply with the terms and conditions of the written agreement that you enter into with the disclosing health information custodians, and

  Note: Hospitals should develop a clear policy on signing these agreements, which includes the designation of a person responsible for them.

- provide written notice of any breach of the written agreement or any of these duties to the disclosing health information custodians.

If you work under a research plan approved outside Ontario, you must follow the same requirements that researchers whose plans are approved in Ontario must follow.

You may use or disclose personal health information originating outside Ontario for research purposes without consent if a research ethics board (or other body outside Ontario responsible for approving research) has approved the research.

Disclosure Under Other Acts

You must still follow all of the above disclosure rules, where another law allows you to disclose personal health information to a researcher without consent (for example, to Cancer Care Ontario as a researcher).

Transition Rules

The Act provides a three-year transition period for all research projects approved before November 1, 2004.

This means that if you have been using or disclosing personal health information for research purposes without consent within the three years before November 1, 2004 and your research will not continue past November 1, 2007, you do not need to take any additional steps.

If your research will continue past November 1, 2007, however, you must take steps to comply with the Act.

Express Consent

Nothing in the Act prevents you from collecting, using or disclosing personal health information for research purposes with *express consent.* You may not rely on *implied consent* to collect, use or disclose personal health information for research purposes.

The strict conditions described above apply to research that is conducted without consent. As a best practice, you should still comply with these conditions when you collect, use and disclose personal health information for research purposes with express consent.

The research rules in the Act relate to retrospective research for which consent is not obtained. You must obtain express consent when you conduct clinical trials, genetic testing or other research that is not simply retrospective.

For additional guidelines on researching with express consent, see the Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans.

Related Sections of the Act

Sections 2, 3, 4, 12(3), 36(1)(a), 36(1)(d), 36(1)(g), 36(1)(h), 37(1)(a), 37(1)(b), 37(1)(j), 36(1)(k), 37(3), 44 of the Act

Sections 11, 15, 16, 17 and 18 of the General Regulation

Checklist, Templates and Tools

- Research Approval Checklist
- Sample Research Application
- Sample Information Sharing Agreement
- Sample Consent Form

RESEARCH APPROVAL CHECKLIST

The research plan must describe:

- ❑ the name, affiliation, roles and qualifications of everyone working on the research and accessing personal health information
- ❑ adequate justification for disclosing personal health information to these persons
- ❑ the nature of the research
- ❑ the particular research objectives and related research questions
- ❑ the duration of the research
- ❑ the anticipated public and scientific benefit of the research
- ❑ the required personal health information
- ❑ the sources of the personal health information
- ❑ the use of personal health information, including details on information linkage (if any)
- ❑ adequate justification for using the personal health information
- ❑ adequate justification for linking the personal health information
- ❑ adequate consent process/form OR adequate justification for proceeding without consent
- ❑ the reasonably foreseeable harms and benefits of the information use
- ❑ adequate explanation of how foreseeable harms will be addressed
- ❑ adequate privacy and security safeguards
- ❑ how long the information will remain identifiable and why
- ❑ how and when the information will be destroyed or returned to source
- ❑ details on research funding
- ❑ details on whether the researcher has applied for other research ethics board approval and its response or the status of the application
- ❑ details on the researcher's conflicts of interest
- ❑ details on any additional matters the law or ethical guidelines and conventions may require

REB File No.:
Date:

SAMPLE APPLICATION TO RESEARCH ETHICS BOARD

A. GENERAL INFORMATION

PRIMARY INVESTIGATOR

Name	Signature
Dept./Div.	Position
Qualification:	Email Address

CO-INVESTIGATOR

Name	Signature
Dept./Div.	Position
Qualification:	Email Address

CO-INVESTIGATOR

Name	Signature
Dept./Div.	Position
Qualification:	Email Address

OTHER RESEARCH TEAM MEMBERS WHO ARE NOT CO-INVESTIGATORS Please type names, roles and qualifications (signatures not needed)

B. DETAILS OF PROJECT

1. Project Title _____

2. Is this project funded? _____

   ☐ NO

   ☐ YES

3. Sponsor _____

4. Duration of Funding: from __/__/__ to __/__/__

5. Conflict of Interest Declaration – Do you have any conflicts of interest (actual, apparent, perceived or potential) relating to this project?*

   ☐ NO

   ☐ YES

   Description of conflict of interest _____

   Mandatory Signature _____

   (Application will be returned without signature)

   *Conflicts of interest include but are not limited to the following situations and also must be disclosed under institutional policy for review: If you or any of the involved research team members or your/their dependants have:

   (1) employment or consulting arrangements and/or a financial interest in the sponsor of the study, or with proposed subcontractors, vendors or collaborators; or

   (2) a financial interest in the subject of the study.

6. Protocol:

   a) *Nature*

   b) *Objectives*

   c) *Methods*

d) *Statistical Analysis*

e) *Anticipated Public or Scientific Benefit*

f) *Duration of Research*

g) *Foreseeable Harms and Benefits of Research (describe how harms will be addressed)*

C. INFORMATION REQUESTED

1. What patient information do you require?

_____

_____

2. What patient information source are you accessing?

☐ Health Records Clinic/Office Files	Specify which
☐ Electronic Database	Specify which
☐ Outside Institution	Specify which
☐ Other	Specify which

3. Proposed number of research subjects _____

4. Are you requesting information that identifies or potentially identifies individuals?

☐ NO
☐ YES

If yes, explain why you cannot use anonymized or aggregate information:

_____

_____

5. Have you obtained consent from the individuals to collect and use the identifying information on this project?

☐ YES Attach a sample consent form

☐ NO

If no, explain why

_____

_____

6. What security measures will be in place to protect the information during transmission?

_____

_____

D. INFORMATION LINKAGE

1. Does your project involve linking any information from this request to other information?

☐ NO
☐ YES

If yes,

Describe what information is to be linked:

_____

_____

Describe what type of linkage is required:

_____

_____

Describe the rationale for this linkage:

_____

_____

2. Have you received approval from the other information sources including division/department head authorization to conduct this linkage?

☐ NO

☐ YES Please attach the approval(s)

3. Will the information be retained in linked form?

☐ NO

☐ YES

4. When will the information be de-identified after the linkage?

_____

_____

E. DISSEMINATION OF ANALYSIS AND/OR REPORTS:

1. How do you plan to disseminate and/or publish the results of your analyses?

_____

_____

2. What is the expected date of dissemination and/or publication?

_____

F. DISCLOSURE AVOIDANCE PRACTICES

1. How will you ensure that information will be aggregated prior to disclosure, to the level required in the information sharing agreement, confidentiality agreement, privacy policy and other applicable policies and procedures?

_____

_____

_____

2. Attach information collection form or list of fields (mandatory: application will be returned if this information has not been included)
Please note that the content of the form should be adequate to answer the research questions.

3. Are any sensitive issues raised in this study or its publication (e.g. HIV status, mental health status, subjects identifiable, pedigrees, other)

☐ NO

☐ YES Please specify _____

G. SECURITY AND ACCESS

1. The information obtained from the records described above will be used for the outlined research purposes only:

☐ NO If no, a separate request must be submitted
☐ YES

2. List all of the persons who will have access to the records in an individually recognized form for the research purpose described and why they need this access: (name and role in research)

_____

_____

3. Have all these persons signed confidentiality agreements?

☐ NO

☐ YES If no, please indicate when agreement will be signed

_____

_____

H. SECURITY MEASURES

1. Describe how you will keep information secure

☐ Premises will be locked except when one or more of the individuals named in E1(b) are present

☐ Access to the premises will be controlled (passcards, security clearances etc.)

☐ Access to the information will be restricted to the research team by:

☐ Patient code ☐ Files/Folders password ☐ Computer password

Please provide name of password software_____

☐ Other computer security methods that prevent unauthorized access will be used

☐ Encryption ☐ Firewalls ☐ Identifying Information Scrambled/De-linked

Other (Describe):_____

☐ Staff will be trained regarding privacy

☐ Staff will sign a confidentiality agreement

☐ Other, explain

_____

_____

2. Will information remain within the institution?

☐ NO

☐ YES If no, please indicate why and how information will be exported outside

_____

_____

3. Will system files be backed up automatically?

☐ NO
☐ YES

If yes, please specify provisions that would be made for a private drive that cannot be accessed by anyone other than your research team, or that could not be backed up by computer support staff within your organization:

_____

_____

All original personal health records received from ● must be returned to ● and all copies of personal health records that were made or received must be destroyed in accordance with the information sharing agreement.

I certify that the information reported here is accurate and that the personal health information will not be used for future projects without prior approval of a research ethics board.

Primary Investigator Signature _____ Date _____

Division/Department Head Signature of Approval _____ Date _____

Do you plan on accessing information from another division/department?

☐ NO
☐ YES If yes, authorization from the division/department head is requested

Signature of Approval _____ Date _____

In making this request, I acknowledge that failure to comply with the terms and conditions of the information sharing agreement is cause for termination of the agreement and, where applicable, a complaint to the Information and Privacy Commissioner/Ontario.

Date _____ Signature of Requestor _____

Research Ethics Board for Retrospective Research

Signature of REB Chair _____

Date of Approval _____ Approval Expires _____

Level of Continuing Review:

NOTE TO USER: This Sample Information Sharing Agreement is intended to be used for retrospective research. You should consider using a material transfer agreement if your research involves the transfer of specimens. A customized version of this Sample Information Sharing Agreement could be used when a hospital discloses personal health information to a health data institute for research purposes. It would not typically be used when a health information custodian shares personal health information with a researcher from the same hospital; however your confidentiality agreement with your internal researcher should include many of the same standards for confidentiality contained here. Hospitals should develop a clear policy on drafting, negotiating and signing these agreements, which includes the designation of a person responsible for them.

SAMPLE INFORMATION SHARING AGREEMENT

This Information Sharing Agreement is effective as of **[insert date]** between **[insert name of Hospital]** (as the disclosing party) and **[insert name of Researcher]** (as the collecting party)

BACKGROUND:

A. **[Identify the Hospital.]**

B. **[Identify the Researcher.]**

C. **[Outline the details of the proposed disclosure of personal health information and the research.]**

D. The parties now wish to set out terms and conditions about the collection, transmission, use, retention, disclosure and disposal of certain personal health information provided by the Hospital to the Researcher.

E. Section 44 of the Act gives the Hospital and the Researcher statutory authority to engage in this collection, use and disclosure.

F. **[Identify any other legislative authority for the collection, use and disclosure of the personal health information, such as legislation that governs the parties or the research.]**

FOR VALUE RECEIVED, the parties agree as follows:

SECTION 1 - INTERPRETATION

1.1 Definitions

In this Agreement:

(1) ***Act*** means the *Personal Health Information Protection Act, 2004* (Ontario) and where the context requires includes the regulations under that Act, including any amendments;

(2) ***Hospital*** means **[insert name of Hospital]**;

(3) ***Research*** has the meaning set out in Section 2.2(1);

(4) ***Research Plan*** means the research plan attached as Schedule A;

(5) ***Researcher*** means **[insert name of Researcher]**;

(6) ***Shared Information*** has the meaning set out in Section 2.1;

(7) **[Include definitions of any terms or acronyms that may be unique to the subject matter of the Agreement.]**

1.2 Purpose of Agreement

The purpose of this Agreement is to set out terms and conditions about the collection, transmission, use, retention, disclosure and disposal of the Shared Information that is provided by the Hospital to the Researcher for the purposes described in Section 2.2(1) and Schedule A.

SECTION 2 - INFORMATION SHARING

2.1 Shared Information

The Hospital will provide to the Researcher the personal health information described in Schedule B (the "Shared Information").

2.2 Use of Personal Health Information

(1) The Researcher shall use the Shared Information, and shall ensure that the Shared Information is used, only as necessary to fulfill the specific research objectives and related research questions described in the Research Plan (the "Research").

(2) The Researcher shall not collect or use the Shared Information for any purposes other than those purposes described in Section 2.2(1) and Schedule A or specifically authorized by legislation.

(3) The Researcher shall require the prior approval of the Hospital for any proposed changes to the Research described in Section 2.2(1) and Schedule A.

(4) The Researcher confirms that the Research Plan has been approved by the **[insert name of research ethics board]** on **[insert date]** and that a copy of the **[insert name of research ethics board]**'s written approval of the Research Plan is attached as Schedule C.

(5) The Researcher agrees that the Researcher shall comply with the conditions imposed by the **[insert name of research ethics board]** concerning the Research Plan, if any.

2.3 Method of Sharing Information

(1) The Hospital will provide to the Researcher the Shared Information via **[specify manner of information sharing such as provision of a computer tape, computer disk, hard copy, electronic data interchange, etc.)]**.

(2) Such transmission of Shared Information will take place on **[specify frequency of sharing]**.

(3) Such transmission of Shared Information will **[describe the measures that will be taken to ensure that the Shared Information will be protected against loss and unauthorized access during transfer]**.

2.4 Accuracy, Completeness and Currency of Shared Information

The Hospital may conduct audits in accordance with an information quality framework and may follow up with the Researcher concerning the maintenance of appropriate technical standards for information quality, integrity and security in order to seek to ensure the accuracy, completeness and currency of the Shared Information. The Researcher shall fully cooperate with the Hospital in this regard. **[If this provision is not appropriate in the circumstances, describe what steps will be taken to ensure the accuracy, completeness and currency of the Shared Information before it is disclosed to the Researcher]**.

2.5 Access to the Shared Information

The Researcher shall refer individuals seeking access to their own personal health information that forms part of the Shared Information to the Hospital. The Researcher will cooperate with the Hospital and these individuals in providing access to this information.

2.6 Security of Shared Information

(1) The Researcher shall comply with the Act and all statutes, regulations, rulings and orders relating to the collection, use and disclosure of personal

health information in respect of the Shared Information, as the same may apply or be amended from time to time.

(2) The Researcher shall implement the following security safeguards in handling the Shared Information:

[Insert appropriate provisions. The following provisions are examples of best practices. You should try to include all of these provisions in your agreements; however, it is likely that the Researcher will resist some of these high standards. Consult your lawyers when negotiating these agreements.]

(a) The Researcher shall not disclose the Shared Information, except as permitted by this Agreement or required by law;

(b) The Researcher shall give access to the Shared Information, in a form in which the individual to whom it relates can be identified, only to the Researcher's staff members listed in Schedule D (the "Named Staff"). The Named Staff are responsible for encrypting identifying numbers, linking files, storing and retrieving files from safes that are located in secure rooms and for destroying information in accordance with Section 2.6(2)(m);

(c) Identifying information, including names and numbers, forming part of the Shared Information will be encrypted immediately after the applicable computer program first links the Shared Information;

(d) The Researcher's working files will not contain any identifying information about an individual but will contain the encrypted number;

(e) Other than the Named Staff, staff members of the Researcher will access the working files only in an anonymized form and will produce analyses required for reports from such files;

(f) All of the Researcher's staff members, including the Named Staff, shall sign a confidentiality agreement in a form acceptable to the Hospital;

(g) The Researcher shall take appropriate disciplinary action against any Named Staff member who breaches the terms of his or her Confidentiality Agreement in relation to the Shared Information and shall deny such individual any further access to the Shared Information;

(h) The Researcher shall keep the Shared Information in a physically secure manner at all times **[Consider adding details of physical security.];**

(i) The Researcher shall monitor access to the Shared Information to ensure security;

(j) The Researcher shall allow the Hospital to inspect the Researcher's security arrangements at any time upon reasonable notice and shall notify the Hospital of any material changes to these practices;

(k) The Researcher shall present only aggregated information in its reports so as to prevent any identification of individuals, whether direct or indirect. The Researcher shall ensure that each cell has at least five observations, unless express written authorization for fewer cells is provided by the Hospital;

(l) The Researcher shall not contact any individual to whom the Shared Information relates without the Hospital's prior approval **[The Hospital must ensure that it has the individual's consent to being contacted by the Researcher before giving its approval.]**;

(m) The Researcher shall retain the Shared Information for as long as necessary to fulfill the purposes identified in Section 2.2. The parties will review the Researcher's information retention practices as required;

(n) The Researcher shall destroy, in a secure manner, information that is no longer required to fulfill the purposes identified in Section 2.2. Such information shall be permanently erased, rendered anonymous or destroyed in such a way that it cannot be reconstructed or retrieved. The Researcher shall provide the Hospital with confirmation in writing of the destruction and manner of destruction of the Shared Information; and

(o) The Researcher shall notify the Hospital in writing immediately upon becoming aware that any of the terms or conditions of this Agreement has been breached.

(3) If a Named Staff member no longer has access to the Shared Information in a form in which the individual to whom it relates can be identified, the Researcher shall so notify the Hospital in writing. The Researcher shall be entitled to substitute another individual for that Named Staff member by notice in writing to the Hospital. After the Hospital has been given such

written notice, the substituted individual shall be deemed to be a Named Staff member under this Agreement.

(4) In the event that the Hospital has concerns about the Researcher's compliance with the provisions of this Agreement, the Hospital shall provide the Researcher with written notice of such concerns and its reasons for them. The Researcher shall, within five days of receipt of the notice, investigate the matter and provide the Hospital with a report stating the cause of the deficiency, if any, and the steps taken to prevent a recurrence, if required.

(5) If the Researcher becomes aware that a person has obtained access to the Shared Information other than in accordance with this Agreement through the Researcher's breach of this Agreement, or the Researcher or the Researcher's staff members have used or disclosed the Shared Information other than in accordance with this Agreement, the Researcher shall immediately notify the Hospital in writing and meet any requirements prescribed by law.

(6) The Researcher shall keep the Hospital appraised of any changes to its policies and procedures followed in respect of the Shared Information.

(7) Each party undertakes to give the other written notice of any changes in legislation, regulations or policies governing or regulating it that are likely to affect the parties' rights and obligations under this Agreement.

(8) Upon expiration or termination of this Agreement, the Researcher shall continue to protect the Shared Information in accordance with Section 2.6.

2.7 Term and Termination

(1) This Agreement shall start on **[insert start date]** and shall end on **[termination date]**, unless ended earlier in accordance with Section 2.7(2) or if the parties agree in writing to extend it. **[State whether the proposed information sharing will be a one-time occurrence, time-limited, or ongoing.]**

(2) This Agreement may be terminated in any of the following ways:

(a) by written agreement of the parties;

(b) by either party, if written notice of termination is given to the other party, because:

(i) the other party fails to perform or comply with any term or condition of Section 2.6 and such failure to perform or comply is not remedied within **[five]** days of written notice to do so; or

(ii) the other party fails to perform or comply with any material term or condition of this Agreement (other than a term or condition contained in Section 2.6) and such failure to perform or comply is not remedied within **[ten]** days of written notice to do so.

(3) Notwithstanding the termination of this Agreement for any reason, a research project of the type referred to in Section 2.2 may be completed provided that the Researcher has obtained written authorization from the Hospital to do so and the Researcher continues to comply with the terms and conditions contained in this Agreement in respect of that research project.

2.8 Indemnity

In addition to any other protections from liability available to the Hospital at law, the Researcher shall indemnify and hold harmless the Hospital and its directors, officers, employees, agents and medical staff members against any and all third party civil or administrative actions, claims or proceedings, including reasonable legal fees, incurred by the Hospital in connection with any failure by the Researcher or any person for whom it is responsible at law to perform its obligations under this Agreement.

SECTION 3 - GENERAL

3.1 Entire Agreement

This Agreement constitutes the entire agreement between the parties concerning the information sharing described in this Agreement.

3.2 Amendments

This Agreement may be amended only by written agreement of the parties.

3.3 Severability

Each provision contained in this Agreement is distinct and severable. Any declaration by a court of competent jurisdiction of the invalidity or unenforceability of any provision or part of a provision will not affect the validity or enforceability of any other provision of this Agreement.

3.4 Waiver

The failure of either party to insist upon strict performance of any terms and conditions or to exercise any of its rights set out in this Agreement shall not constitute a waiver of these rights, and these rights shall continue in full force and effect.

3.5 Assignment and Enurement

The Researcher may not assign the Researcher's rights or obligations under this Agreement without the prior written consent of the Hospital. This Agreement enures to the benefit of and binds the parties and their respective successors and permitted assigns.

3.6 Survival

Sections 2.5, 2.6 and 2.7(3) shall survive the expiration or termination of this Agreement indefinitely.

3.7 Delivery by Fax and in Counterparts

This Agreement may be executed and delivered by fax and in any number of counterparts, each of which when executed and delivered is deemed an original but all of which when taken together constitute one and the same instrument.

3.8 Governing Law

This Agreement is governed by, and is to be construed and interpreted in accordance with, the laws of the Province of Ontario and the laws of Canada applicable in the Province of Ontario. Each of the parties irrevocably submits to the non-exclusive jurisdiction of the courts of the Province of Ontario.

The parties have executed this Agreement.

[INSERT NAME OF HOSPITAL]

By: _____

Name: ●

Title: ●

[If the Researcher is an individual, use the following signing lines]

SIGNED, SEALED AND DELIVERED in the presence of:

_____
Witness

By: _____
Name: **[Insert name of Researcher]**
Title: ●

[INSERT NAME OF CORPORATION]

By: _____
Name: ●
Title: ●

Schedule A – Research Plan

[Attach the Research Plan, which has been approved by a research ethics board and which describes in detail:

- the name, affiliation, roles and qualifications of everyone working on the research and accessing personal health information,
- adequate justification for disclosing personal health information to these persons,
- the nature of the research,
- the particular research objectives and related research questions,
- the duration of the research,
- the anticipated public and scientific benefit of the research,
- the required personal health information,
- the sources of the personal health information,
- the use of personal health information, including details on information linkage (if any),
- adequate justification for using the personal health information,
- adequate justification for linking the personal health information,
- adequate consent process/form OR adequate justification for proceeding without consent,
- the reasonably foreseeable harms and benefits of the information use,
- adequate explanation of how foreseeable harms will be addressed,
- adequate privacy and security safeguards,
- how long the information will remain identifiable and why,

- how and when the information will be destroyed or returned to source,
- details on research funding,
- details on whether the researcher has applied for other research ethics board approval and its response or the status of the application,
- details on the researcher's conflicts of interest, and
- details on any additional matters the law or ethical guidelines and conventions may require.]

Schedule B – Shared Information

[List all elements of personal health information that will be disclosed to the Researcher for the specified research objectives and related research questions. Only those components of personal health information that are absolutely necessary to achieve the research objectives and to answer the related research questions should be disclosed.]

Schedule C – Research Ethics Board Approval

[Attach a copy of the written decision of the Research Ethics Board. The entire decision, with conditions, if any, must be attached.]

Schedule D – Named Staff

[List appropriate individuals. Limit these individuals to a small number.]

SAMPLE CONSENT FORM FOR STUDY PARTICIPANT

Note to User: This Sample Consent Form is intended to be used for retrospective research. It is not appropriate to use it for clinical trials.

Study Title: ●

Primary Investigator: ●

Sponsor: ●

Background: **[Insert details about the study.]**

What is involved? ●

Benefits and Risks: ●

Voluntary: Participation in this study is completely voluntary. You can refuse to sign this consent form and to participate in the study. You can also withdraw your consent any time by writing to ●. Your care at ● will not be affected by your decision.

Confidentiality: **[Insert details about collection, use, disclosure, storage and disposal of personal health information.]**

You have had this study explained to you and had an opportunity to ask questions. You have been given a copy of this Consent Form. If you have any additional questions about the study, please contact ● at ●. If you have any additional questions about your privacy, please contact ● at ●.

Participant Consent

I agree to participate in this study.

I also permit ● to collect, use and disclose health information about me for the purposes of this study.

Name of Participant (print)	Signature of Participant
Investigator's Signature	Signature of Substitution Decision-Maker (if required)
Date	