Guide to

Information Security for the Health Care Sector

Information and Resources for

Complex Organizations

Ontario

eHealth Ontario

Acknowledgements

Numerous representatives from the health care community were consulted during the development of this guide. Representatives included physicians, the continuing care sector, laboratories, pharmacies, hospitals, LHINS and vendors of health care and health care related technology.

eHealth Ontario would like thank the following participants for their effort, time and contribution to the development of the guide:

Judy Ash, Ontario Association of Medical Laboratories (OAML)
Peter Berwick, Canadian Medical Association (CMA)
Peter Catford, Centre for Addiction & Mental Health (CAMH)
Jeff Curtis, Sunnybrook Health Sciences
Lyndon Dubeau, Formerly of Community Care Access Centre (CCAC)
Brian Forster, OntarioMD (OMD)
Sunny Loo, Ontario Pharmacy Association (OPA)
Mary McKeen, Ministry of Health and Long-Term Care (MOHLTC)
Steve Milling, Ministry of Health and Long-Term Care (MOHLTC)
Scott Mitchell, Canadian Mental Health Association (CMHA)
Martha Murray, Ontario Hospital Association (OHA)
Fraser Ratchford, Formerly of Ontario Health Information Standards Council (OHISC)
Harley Rodin, OntarioMD (OMD)
Ben Rodrigues, Gamma Dynacare (LAB)
Igor Sirkovich, Standards (SMBI)
Bobby Singh, eHealth Ontario
Martin Green, eHealth Ontario
Ireen Birungi, eHealth Ontario
Marc Stefaniu, eHealth Ontario

Table of Contents

1. Introduction

The privacy and security of information is of prime importance to all individuals, government agencies and private sector organizations. Nowhere is the protection of information a more sensitive issue than in the health care sector. Like many other industries, health care is becoming more efficient in delivering clinical results and more cost effective through the use of Information Technology (IT), including computers, applications, electronic networks and related technologies.

However, the use of these technologies and the increasing exchange of health information among health providers also pose a privacy and security risk to personal information (PI) and personal health information (PHI). Health information that is disclosed to unauthorized individuals, accessed incorrectly, tampered with, or lost could result in devastating impacts on patient health or even life.

All health care providers should take measures to protect the confidentiality, integrity and availability of PI and PHI. This means protecting this information from unauthorized access, collection, use, disclosure, destruction and modification.

- Remember, if PHI or PI is compromised, the consequences for a patient may be life threatening
- Health care institutions may violate PHIPA and PIPEDA requirements
- Reputation of health care institutions could be negatively impacted
- Health care institutions may face costs such as fines and legal fees

In 2007 the Ontario Health Informatics Standards Council (OHISC) approved the development of an information security guide based on the internationally recognized standards ISO 17799:2005[1] and ISO 27001:2005, as Ontario's minimum requirements to support the implementation of the province's eHealth vision.

This guide focuses on two priorities:

- Building an information security program
- Setting up a risk management program

Recognizing that the documentation framework and the action plan for implementing these security priorities need to be adapted to the size and complexity of various health care organizations, it was decided that the guide should be developed in two versions:

- Guide to Information Security for the Health Care Sector – Information and Resources for Community-based and Private Medical Offices (Guide #1)
- Guide to Information Security for the Health Care Sector – Information and Resources for Complex Organizations (Guide #2)

This document is Guide #2. It is of interest for individuals responsible for the information security program and for managing security risks. The intended audience may include but is not limited to:

- Hospitals
- Clinics
- Continuing Care Sector
- Laboratories
- Public Health Units
- Pharmacies
- Local Health Integration Networks (LHINS)
- Vendors of health care technologies

1 ISO/IEC is the single largest sponsor of globally recognized standards. As of July 1, 2007 ISO 17799:2005 has been officially renamed to ISO/IEC 27002 2005. However, no content within the standard has changed. The name change is to maintain consistency and alignment with the ISO/IEC 27000 series standards numbering convention.

By developing a security program and setting up a risk management program, health care organizations will be better prepared to:

- Protect their reputation and maintain the trust and confidence of patients
- Reduce liability as implementation of a security program demonstrates due diligence
- Comply with legal requirements based on PHIPA and PIPEDA
- Streamline operations by clarifying roles and responsibilities

Note however that there are several areas of the ISO security standards that are not covered in this guide. Health care institutions are encouraged to adopt ISO subject areas not covered by this guide, where practical and possible, as this will improve their overall ability to secure PI and PHI.

The subject areas not covered within this guide include:

- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications & Operations
- Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

The following Navigation Guide provides a quick way to view what is included in the guide. Click on the topic description or the name of sample document and templates to navigate directly to the area of interest.

Case Study : Laptop with Patient Data Stolen

In Dallas, an employee of Baylor Health Care was fired for losing her laptop which contained the personal health information of 100,000 patients. The laptop, which was taken from the employee's car, contained medical records, Social Security numbers and billing records. Baylor Health Care is offering free credit monitoring services to the patients whose information was stored in the laptop, as well as a $1,000 reward for the return of the laptop which would have soon been upgraded to include tracing capabilities. A representative of Baylor Health Care stated the employee was fired for breaking company protocol by leaving her laptop unattended in the car and assured breaches are taken "very seriously".

Source: "Baylor Health Care says laptop with patient data stolen".
http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/stories/110508dnbusbaylordatatheft.91bf7e.html

2. Navigating the Guide

Major Topic	Supporting Documents	What's In the Document
Information Security Program	**Information Security Policy**	Guide to developing an enterprise information security policy: objectives of the policy, key policy requirements and internal processes leading to policy approval.
	• Information Security Policy Checklist	High level information security policy requirements for complex health care organizations.
	• Sample Information Security Policy	Sample policy that sets security objectives, assigns responsibilities and demonstrates the organization's commitment to protecting health information.
	Roles & Responsibilities	Description of various organizational roles that have a subset of security responsibilities.
	• Sample Information Security Roles & Responsibilities	High level list of security responsibilities that should be part of typical IT roles in an organization.
	Confidentiality Agreements	Role and benefits of using confidentiality agreements in protecting health information.
	• Employee Confidentiality Agreement Checklist	List of requirements that should be included in a Confidentiality Agreement between the health organization and employees.
	• Third Party Confidentiality Agreement Checklist	List of requirements that should be included in a Confidentiality Agreement between the health organization and third parties such as consultants or service providers.
	Program Assessment	Guide to assessing the strengths and weaknesses of a complete security program.
	• Information Security Program Assessment Checklist	List of recommended components of a comprehensive, standard-based information security program.
Information Security Risk Management	**Risk Management Methodology**	Definition of risk and description of a structured approach to identifying and assessing risk and implementing controls for the treatment and ongoing monitoring of risk.
	Risk Assessment	Guide to identifying risks and assessing risk magnitude.
	• Sample Assets and Assets Categories	List of common physical and logical (informational) assets that can be found in a complex health care organization.
	• Assets Registry - Template	Template spreadsheet to identify and keep track of physical and logical informational assets; examples included.
	• Threat / Vulnerability Catalogue	Catalogue of common security threats and vulnerabilities that may create information security risks.
	Risk Treatment	Guide on management options in responding to identified risks.
	• Sample Risk Treatment Planning Template	Sample spreadsheet tool to identify action items planned to reduce risk, responsible parties and timeframe for execution.
	Risk Monitoring	Guide on continuous monitoring of the environment to ensure proactive detection of risks and implementation of preventive safeguards.
Additional Material	**Quick Reference Guide**	A simplified guide to security best practices that cover key components of an enterprise information security program. Contains best practices both for end users and for information security managers.
	Secure Destruction of PI / PHI	Fact Sheet created by Information and Privacy Commissioner of Ontario, providing best practices on destruction of personal information.

3. Information Security Program

The Information Security Program is a framework that ensures measures are implemented to protect the privacy and security of PI and PHI and to broadly educate the organization about applicable laws and regulations governing information management, security and privacy. The benefits of implementing a security program are: improved organization, management support and improved understanding of information security goals.

The program accomplishes this by establishing:

- An Information Security Policy
- Information security roles and responsibilities
- Selection and implementation of safeguards
- Periodic information security program assessments

The following section provides a minimum set of controls that must be implemented in the development of an Information Security Program.

3.1 Establishing a Policy

The information security policy is a document that defines the expected behaviours, responsibilities and rules that the organization must follow and enforce for the safeguarding of information. The policy communicates management support for security activities and sets the tone for information security practices within the organization.

Refer to Appendix A for an example of an Information Security Policy. If you plan to develop your own, consider the checklist in Appendix B, Information Security Policy Checklist - for requirements that should be included in the policy.

Benefits:

- Improved protection of PI and PHI
- Alignment of information security with business strategy and drivers
- Consistent messages, guidance and accountability for information security
- Compliance with legislative, regulatory (e.g., PHIPA and PIPEDA) and contractual requirements
- Reduction of risk impact
- Better allocation and management of resources
- Increased awareness of the importance of information security throughout the organization

3.1.1 Supporting Standards, Guidelines and Procedures

Once the policy is written, supporting standards, guidelines and procedures need to be developed to support the policy at a more detailed and specific level. The detail and depth of the standards and guidelines will depend upon the complexity and size of the organization and its information systems. Typically the supporting standards, guidelines and procedures should address the key control areas of the ISO standard. All supporting documents must be reviewed regularly (yearly) to ensure completeness and relevance to the organization.

3.1.2 Stages of Policy Development

Information Security Policy development can be a difficult process because it is a complex task that must balance business objectives, technology objectives, relevant laws and regulations, security requirements and human behaviour. Using a process that includes many reviews, revisions and stakeholder engagements is key to developing a policy that can be successfully implemented.

A key benefit of following this process is that stakeholders within the organization will not be surprised with unattainable security requirements, requirements will be well vetted and aligned to the organization's business and technology objectives and buy-in and support for the policy will be improved.

Diagram 1: Stages of Policy Development

1. Obtaining Executive Support

Engage senior management at the beginning of developing the policy to obtain their support and commitment for the development of the policy and its implementation.

2. Drafting & Engagement

When drafting the policy, ensure that those within your organization that will be impacted by the policy or who can offer subject matter expertise or insight from their area of the organization are engaged and review the content of the draft. These individuals are known as stakeholders. In some cases, stakeholders outside of the organization such as vendors, suppliers, or patients may need to be consulted.

3. Review

The draft policy should be reviewed with stakeholders and management and necessary revisions should be made. This may result in a number of versions being created before an acceptable draft is ready for approval and publication.

4. Approval

Executive management and any other required approving body should formally approve the policy and communicate to the organization the necessity to comply with it.

5. Implementation

Identify areas in the organization that must comply with the policy. Create and document an action plan to reach compliance and monitor for completion.

6. Maintenance & Review

The policy should be reviewed and updated on a periodic basis or upon significant changes to business objectives, environment, technology, legislation. The challenges and issues regarding the policy, as expressed to the organization by its staff, patients and their partners and care givers, researchers and governments (e.g. privacy commissioners) can also be considered.

3.2 Establishing Roles & Responsibilities

When developing an Information Security Program, the organization will need to put an information security management structure in place by assigning roles and responsibilities for security throughout the organization.

Benefits

- **Accountability for security within the organization is established and there is clear understanding of who does what, when and where.**
- **Ensures that information security activities are organized effectively and efficiently and staff are aware of their security duties and have adequate training and skills.**

It is important to note that:

Each organization will have its own unique requirements. Smaller organizations may choose to combine multiple responsibilities into a single role, while medium to larger organizations may choose to separate an area of responsibility into multiple roles.

The concept of segregation of duties (see Glossary) should be applied when developing and assigning these roles and responsibilities. In cases where segregation of duties may not be possible or practical in all situations, the principle should be applied as much as possible.

If the organization is small and unable to implement segregation of duties, other controls should be implemented to offset the risk. Controls may include audit mechanisms, independent reviews, logical controls, or additional manual controls.

Refer to Appendix C for examples of common security roles and responsibilities in a complex health care organization.

3.3 Program Assessment

All health care institutions should review (assess for gaps) their Information Security Program at planned intervals or when changes to the security program occur.

Benefits:

- **Actual or potential security weaknesses, which could put the organization or patient at risk, are identified to reduce potential harm.**
- **Allows the organization to proactively prioritize and plan for improvements, thus reducing the risk and ensures the continuing suitability, adequacy and effectiveness of the Information Security Program.**

Without assessing the program, an organization will not know where they have weaknesses and where resources, time and effort should be focused. As a result, valuable resources may be spent or used securing areas that do not require it. Assessments of the Information Security Program should be initiated by management.

The review should identify opportunities for improvement and the need for changes to security, including the policy and other security control areas. Refer to the ISO standard 27001 for more in security control areas.

It is highly recommended that the program assessment be done by third party auditors or by someone other than the person who is responsible for implementing the information security policy. Individuals carrying out these reviews should have the appropriate skills and experience. The results of the independent review should be documented and reported to management.

If the independent review finds that an organization's information security is inadequate or not compliant with the direction in the information security policy, management should take corrective actions.

Refer to Appendix D for a list of recommended components of a comprehensive, standard-based Information Security Program.

3.4 Confidentiality Agreements

A Confidentiality Agreement is a contract that requires one party, usually an employee or contractor, not to reveal confidential information that they acquire while working for the employer.

Benefits:

- **Clearly communicates to employees their responsibility and accountability for protecting confidential information.**
- **May also help the organization demonstrate due diligence in the event of a confidentiality breach.**

Employees should sign a Confidentiality Agreement when they are hired that states their obligation to avert unauthorized use or disclosure of confidential information during and after employment.

All agreements should be signed, dated and the original should be received by the organization before the person is granted access to confidential information.

Employees should review Confidentiality Agreements when there are changes or when they are due to leave the business or when contracts terminate. This will remind the employee of their obligations, some of which may extend beyond employment. Temporary staff and third parties should also be required to sign a Confidentiality Agreement.

Confidentiality Agreements must comply with all applicable laws and regulations for the jurisdiction to which they apply, be easy to read and understand and be accompanied by frequently asked questions (FAQs) to help the signatories (those who sign the document) to understand their ongoing obligations of confidentiality.

The following checklist includes elements that are recommended for an organization when implementing s confidentiality agreement. You can use this checklist to assess your use of Confidentiality Agreements.

Checklist:

Confidentiality Agreements should include:

- ☐ A definition of the information to be protected (e.g. confidential information)
- ☐ The responsibilities and actions required of signatories to avoid disclosure of information in an unauthorized manner
- ☐ A legal representative who drafts the agreement or provides a template for the agreement
- ☐ The permitted use of confidential information, and rights of the signatory to use the information
- ☐ Expected actions in case of a breach of the agreement
- ☐ Required actions when an agreement is terminated

Most agreements should also include, where appropriate, one or more of the following:

- ☐ Requirements for information to be returned or destroyed when the agreement is terminated
- ☐ The process for reporting unauthorized disclosure
- ☐ Ownership of information, trade secrets and intellectual property and how this relates to the protection of confidential information
- ☐ The expected duration of the agreement, including cases where confidentiality might need to be maintained indefinitely
- ☐ The right to audit and monitor activities that involve confidential information

3.5 Third Party Agreements

Most health care institutions require, to some degree, the assistance of third parties who may have access to information through physical means (office, filing cabinets, laboratories, etc.), or through logical means (databases, applications, information systems or an Intranet).

A third party agreement is a type of Confidentiality Agreement used when an organization is planning to disclose confidential or proprietary information to a third party.

Similar to the employee Confidentiality Agreement, it ensures that the third party is aware and accepts responsibility and accountability for protecting confidential information. It also demonstrates due diligence and may give the organization legal recourse if the third party breaches the agreement.

- It is important that third parties accept their responsibility for safeguarding the confidentiality, integrity and availability of information
- Demonstrate their ability to undertake and maintain security and privacy responsibilities
- Third-party agreements should be signed and dated; the original should be received by the organization before the third party is granted access to confidential information

The following checklist includes elements that are recommended for an organization to implement. Use this checklist to assess your use of third party agreements.

Checklist:

Third-party agreements should include:

- ☐ The organization's policy on information security
- ☐ The organization's policies about asset protection
- ☐ A description of the service that the third party is to provide – written in clear English - which both parties agree is a comprehensive description of the service
- ☐ Verifiable performance criteria and a clear statement on the process for monitoring and reporting
- ☐ The target level of service and a definition of unacceptable service
- ☐ The prospective liabilities of the parties to the agreement
- ☐ Legal responsibilities (e.g. information protection in accordance with PHIPA, PIPEDA)
- ☐ Intellectual property rights, copyright and protection of rights in any collaborative work
- ☐ The right to audit contractual responsibilities or to have a third party carry out such an audit
- ☐ The escalation process for dispute resolution

Have/Has:

- ☐ All third parties employed by the organization been identified?
- ☐ Legal representatives drafted the agreement or the agreement template?
- ☐ Third party access to information been based on formal third party agreements?

Contracts could also include:

- ☐ Provision for the transfer of staff and any associated costs
- ☐ Protection against poaching staff
- ☐ Access control agreements covering:
  - Permitted access methods, control and use of passwords and user IDs and the process by which these are surrendered at the end of the contract
  - The authorization process for user access and privileges
  - A requirement that the third party maintains an up-to-date list of which personnel have been given what level of authorization
- ☐ The right of the host organization to monitor user activity and revoke user rights
- ☐ Responsibilities regarding hardware and software installation and maintenance
- ☐ The reporting structure and reporting formats, so that third party staff know who within the organization is responsible for what and to whom they have to report on those issues
- ☐ The required change management process
- ☐ Any physical controls that are required
- ☐ Training that is required around methods, procedures and security
- ☐ Controls against malicious software and viruses
- ☐ Involvement with any sub-contractors

4. Risk Management

Information Security Risk Management is the coordinated direction and control of activities to ensure that security risks are identified, analyzed, understood, addressed and are consistent with business goals and objectives.

These activities include the identification, assessment and appropriate management of current and emerging security risks that could cause loss or harm to persons, business operations, information (including PI and PHI), systems or other assets.

Benefits:

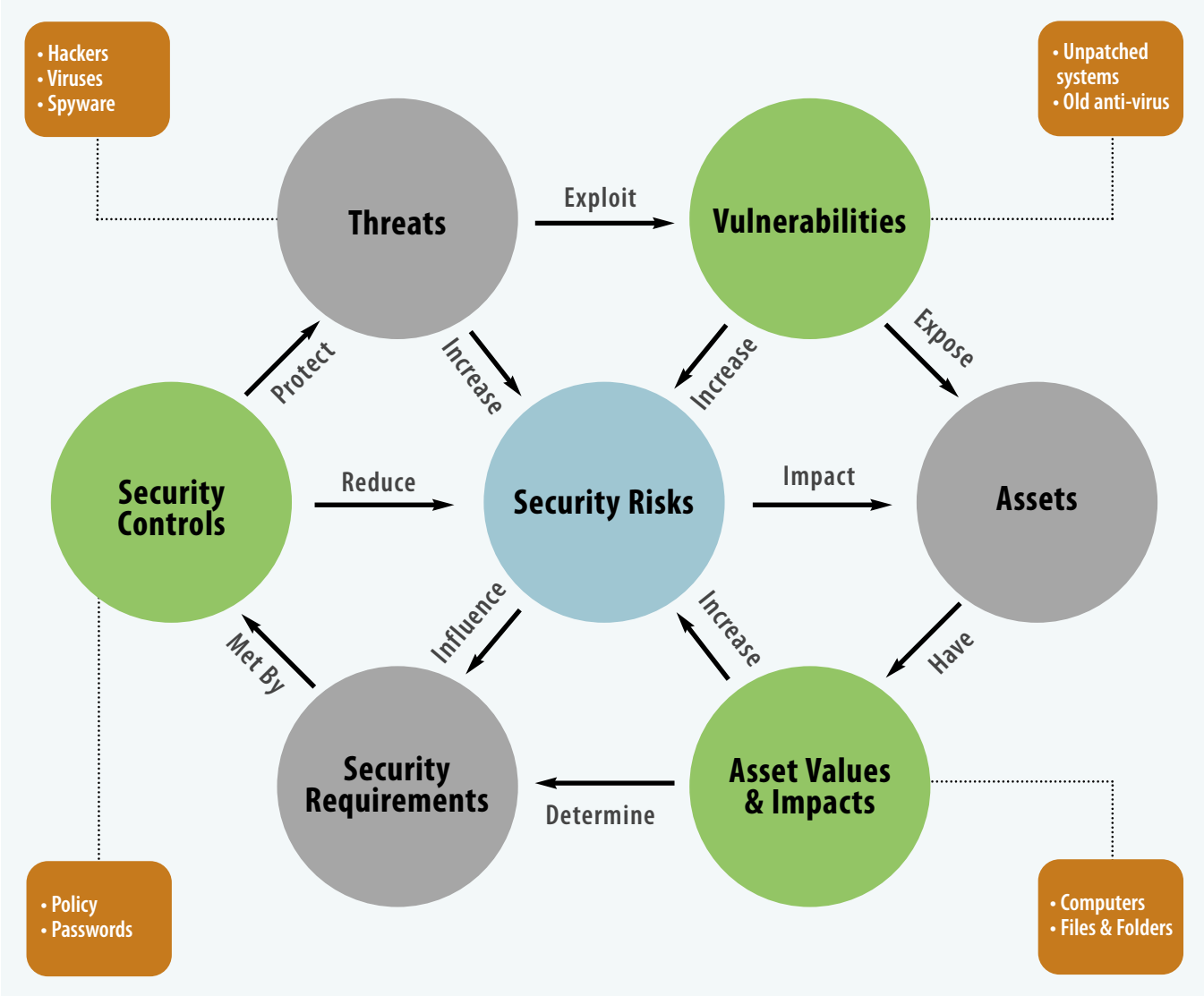
- Minimize liabilities caused by security incidents, weaknesses or other adverse impacts on business operations by identifying, prioritizing and addressing risks proactively.
- Reduce the risk that breaches in information confidentiality take place or go unnoticed.
- Enhanced support for privacy legislation.

Definitions

Risk	The combination of the probability of an event and its consequence.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk Management	Coordinated activities to direct and control an organization with regard to risk.
Threat	A threat is someone or something that can take advantage of (exploit) the vulnerability, thus causing harm to an asset or to the organization. Information security is concerned primarily with three types of potential harm to information: confidentiality, integrity and availability of information. Threats could impact on any of these three attributes. Examples of security threats include: hackers, viruses, spyware, fires and others.
Assets	Assets are anything that has value for an organization. Assets include not only physical, tangible items, such as furniture and IT equipment, but also logical items such as data or information. Many of these assets have tremendous value or may merely be sensitive in nature, such as PI or PHI. Examples of assets include: computers, files and folders, databases, software applications and others.
Vulnerability	A vulnerability is a weakness in an asset which could be exploited by a threat to cause harm to an asset. Examples of vulnerabilities include unpatched systems, outdated anti-virus, weak passwords and poor physical security.
Security Requirements	Security requirements describe business objectives with regard to protection of assets and information. A good understanding of what are the desired business outcomes allows security advisors to select an appropriate set of security controls.
Security Controls	Security controls, also referred to as safeguards, are means of managing risk, intended to protect assets by limiting threats or reducing or, if possible, eliminating vulnerabilities. Examples of security controls include: policies, practices, organizational structure and others.

The relationship between these concepts is illustrated in Diagram 2. Refer to the Glossary for additional information about security concepts.

Diagram 2: Concept Relationships



Information security risk management[2] typically involves three core activities, which can be subdivided into separate phases. The methodology and the associated phases are described in detail in section 4.2 Risk Assessment.

2 For detailed procedures consult risk assessment best practices such as ISO/IEC 27005:2008 – Information technology -- Security techniques -- Information security risk management and AS/NZS 4360:2004 Risk Management.

4.1 Risk Management Methodology

The objective of a risk assessment is to identify, prioritize and assess information security risks to which the organization's assets are exposed so that the appropriate safeguards can be selected and implemented. Risk assessments are a snapshot of a point in time and should, therefore, be conducted on a regular basis to ensure that changes in the business and technical environments are captured.

Without performing risk assessments, an organization will not have accurate information pertaining to areas of strengths and weaknesses, which will increase the likelihood of a security incident(s).

Typically, risk assessments are performed when:

- New projects and initiatives are started
- Major changes are made to existing processes, personnel and/or systems
- A security incident has occurred
- Changes to the threat landscape are identified

4.2 Risk Assessment

4.2.1 Phase 1: Establish the Context

A. Define Scope and Objective

The objective of conducting risk assessments should be clearly documented. The objective may be to fulfil policy, regulatory or legislative requirements (e.g., PHIPA and PIPEDA). The scope may be the whole organization, part(s) of the organization or only a specific information system. Definition of the scope needs to take into account the dependencies that the risk assessment has with other parts of the organization, other organizations, third party suppliers or with any entity outside the information security program.

B. Define Risk Tolerance

Prior to starting the risk analysis for a particular department, project or system, the organization's tolerance for risk should be identified and approved by management. An understanding of risk tolerance will help define the criteria for risk acceptance - the circumstances under which the organization is willing to accept the risks.

For a sample risk tolerance matrix, refer to Table 5.

The tolerance line provides management guidance on how risks should be treated. Risks which fall below the tolerance line may be acceptable to the organization and may not require special treatment. Accepting a certain amount of risk is a management prerogative and will typically reflect priorities in delivering certain projects or initiatives faster or keeping a lead on costs or satisfying other business objectives. Risks which are assessed to be above the risk tolerance line will require risk treatment plans which involve security controls intended to reduce the risk below the tolerance line.

4.2.2 Phase 2: Asset Identification & Valuation

A. Asset Identification

As part of conducting a risk assessment, it is important to identify all the assets that are relevant to the business and assign a relative value to each of those assets. This process makes it easier to decide which assets should be protected.

A list of assets that are likely to be found in a complex health care organization is provided in Appendix E: Asset Categories. If there are too many assets to manage, grouping similar or related assets into manageable categories can help make the risk assessment process easier.

The following list provides an example of the kind of asset information that should be collected:

- Asset Category: assets can be grouped by category if there are too many assets to manage individually (e.g., information, software, physical, personnel, intangible)
- Asset Name: the name of the asset
- Asset Description: a brief description of what the asset is (e.g., computer, health records, x-rays, etc.)
- Asset Custodian and Email Address: information that will help locate the custodian of the asset
- Asset Type: the medium in which the asset exists (e.g., paper, physical/hardware, software, people)
- Asset Location - both the physical and electronic location of the asset (e.g., filing cabinet, location on network, etc.)
- If there is more than one copy of the asset – some assets have multiple copies (e.g. computers, patient records, etc.)

Table 1 provides an example of an Asset Registry spreadsheet, populated with sample information that can be used to track assets. For an Asset Registry template in Excel file-format, it is available online.

Accountability for assets helps ensure that adequate information security is maintained. A custodian should be identified for each of the identified assets and the responsibility for the maintenance of the appropriate security controls should be assigned by the custodian. Regular reviews of the Asset Registry are part of the security risk assessment methodology.

Table 1: Asset Registry Examples

Asset Category[1]	Asset Name	Asset Description	Asset Custodian & Email Address	Asset Type[2]	Asset Location[3]
Physical	Cardiac monitoring machinery	Portable and in-hospital heart monitoring equipment	John Smith jsmith@company.com	Physical / Hardware	Patient room A
Physical	X-ray machines	X-ray for radiology	Jane Doe jdoe@company.com	Physical / Hardware	Patient room B
Physical	PCs	There are now 4 PCs in this office: one for each employee and one for John Smith. These PCs are used for patient appointments, billing invoices and storing patient information.	Adam Smith asmith@company.com	Physical / Hardware	Employees' work stations
Information Asset	Patient health information and records	This includes all patient related health information that has been disclosed.	Dave Martin dmartin@company.com	Electronic / Paper	
Information Asset	Employee records	This includes all employee related records (address, employment information, training records, other relevant personal information, signed agreements, contracts, etc.)	James Morris jmorris@company.com	Electronic	
Information Asset	Operating policies and procedures	This includes the operating policies and procedures used by the organization.	Steve Jackson sjackson@company.com	Electronic	
Information Asset	Third party contracts	This includes contracts with all third party organizations.	Kate Hall khall@company.com	Electronic / Paper	
Personal Asset	Employees	These are the three employees employed by the organization.	Dave Hill dhill@company.com	People	
Information Asset	System documentation	This is the system documentation for the PCs in this office, the PC for John Smith's office and the server.	John Smith jsmith@company.com	Paper	Filing cabinet of server

1 Asset categories include: information assets, software assets, physical assets, personal assets, intangible assets
2 Example asset types: electronic, paper, physical / hardware, software, people
3 Refers to the physical and / or electronic location

B. Asset Valuation

Asset valuation is assigning a relative business value to each of the identified assets.

It is important to note that business value is not only the monetary value of the asset but also includes the potential business impact due to the loss of this asset (e.g., losing PHI causing non-compliance to PHIPA). These values (often called soft values) are all part of the importance of the assets to the organization. Any legal and/or contractual requirements related to each of the assets and to the organization should also be identified.

The goal of asset valuation is to assign impact values to the assets in the context of confidentiality, integrity and availability. The impact value should be based on worst case scenarios, using a scale appropriate for the organization.

Items to consider when assessing the potential impact include:

- What is the potential impact to patient care?
- What is the impact to service delivery?
- What is the impact to the organization's reputation?
- What is the potential privacy/legal/regulatory impact?
- What is the potential financial impact on the organization?

Tools such as the Business Impact Matrix can help in valuing the assets.

Table 2 provides an example of a Business Impact Matrix. Note the level and areas of impact are for illustrative purposes only. Each organization should develop their own impact model and scale for asset valuation, appropriate for the size, complexity and business priorities of the organization.

Table 2: Sample Business Impact / Asset Value Matrix

		Area of Impact				
		Service Delivery	**Reputation**	**Privacy Infringement**	**Failure to Meet Legal Obligations**	**Financial Obligations**
Value	Low	Normal	Minimal impact to reputation	No PHI revealed	Minimal impact	Minimal impact
	Medium	Degraded: Minor functions not available or minority of users affected	Contained within company	External breach of personal information	Civil suit > $10K damage	<$50K*
	High	Down: Service completely unavailable	Unfavourable widespread press interest	Detrimental effect on person and personal life	Custodial sentence imposed	<$250K**

* The financial loss is for illustrative purposes only and is the maximum fine for an individual found guilty of an offence under PHIPA

** The financial loss is for illustrative purposes only and is the maximum fine for a corporation found guilty of an offence under PHIPA

The final output of this step is a list of assets and their values, taking into account the potential impact on confidentiality, integrity, availability and replacement cost.

C. Identification of Existing or Planned Safeguards

It is important to identify existing and/or planned safeguards. The risk assessment process may indicate that existing safeguards are not sufficient and new ones need to be introduced to reduce the risk to acceptable levels. The final output of this step should be a list of all existing and planned safeguards.

Refer to ISO27002:2005 for a complete list of safeguards available to reduce security risks.

4.2.3 Phase 3: Threat & Vulnerability Assessment

Vulnerability assessment is the process of identifying weaknesses that may be exploited by threats to cause harm to the assets and to the business they support. An identified vulnerability will not, in itself, cause harm unless there is a threat present to exploit it. Safeguards need only be implemented if an identified vulnerability can be exploited by a corresponding threat. However, all vulnerabilities should be recognized and monitored for changes over time.

A. Identify threats and vulnerabilities

A key part of risk assessment is to identify all the threats from the physical or electronic environment in which the organization operates and to recognize the people, process or technology related vulnerabilities that may be exploited by these threats.

Refer to Appendix F: Threat and Vulnerability Catalogue for a sample list of information security threats and vulnerabilities that are likely to exist in a health care organization.

B. Determine Likelihood

A threat has the potential to cause a negative impact to the organization. For all threats, the threat source (who/what could cause the threat) and the threat target (what assets would be affected) should be determined and the likelihood of occurrence (defined here as the probability of an undesired event occurring in the future) should be assessed. This should take into account:

- The threat frequency (how often it might occur, according to experience, statistics, etc.)
- The motivation, the capabilities (both perceived and necessary), resources required and available to possible attackers and the perception of attractiveness and vulnerability of the IT system assets to the possible attacker
- Geographical factors such as proximity to chemical or petroleum factories, the possibility of extreme weather conditions and factors that could influence human errors and equipment malfunction (for accidental threat sources).

The following is a sample scale, which can be used to determine the likelihood of a threat:

Very Low	The event has not yet occurred but could occur at some time (once every 10 or more years), (e.g., an earthquake damaging the building, or meteors striking the office).
Low	The event has 6% to 20% probability of occurring in the next two years (e.g., Avian bird flu, power grid failure impacting the operations of the data centre).
Medium	The event has 21% to 50% chance of occurring in the next two years (e.g., attempted theft of patient records, identity theft, failure to restore backed up data).
High	The event has happened in the past and has 51% to 80% probability of occurring in the next two years (e.g., theft of computers; misdirected FAX transmissions; unauthorized access to PHI files, folders or databases).
Very High	The threat has higher than 80% probability of occurring in the next two years (e.g., a virus attack).

C. Determine the impact

The following is a sample scale, which can be used to determine the potential impact to the business if the vulnerability is exploited:

Very Low	Minimal impact on patient care or the business (e.g., localized virus infection that impacts email transmission for one hour, access to purchasing system delayed for a couple of hours, receipts cannot be printed for a couple of hours, wait time for non-critical patients extended by a few minutes).
Low	No impact at all on health care delivery to patients. Negligible impact on the business (e.g., telephone services not operating for an hour or internal memos or telephone numbers disclosed by accident to an unintended external audience).
Medium	Moderate impact to the patient or business that will negatively impact reputation, patient confidence and/or budgets (e.g., theft of medical equipment or of an office computer, online reports not accessible for an hour).
High	Severe impact to the patient or business that may cause operations to cease for a period of time. There will be some loss of reputation, patient confidence and/or income (e.g., loss of a laptop containing unencrypted personal health information; unauthorized access to patient information, transmission of PHI by fax or email to a wrong destination).
Very High	The most severe type of impact to the patient or the business that will cause loss of reputation, patient confidence, embarrassment and/or income. It may even be life threatening. Recovery may take an extended period of time (e.g., the integrity of patient information is compromised, resulting in an incorrect diagnosis or incorrect medication).

Tables 3 and 4 offer a model for threat likelihood and impact categories.

Table 3: Likelihood Categories

	Probability of occurrence in the near future*	Likelihood Description
Very High	> 80%	This event will probably occur in the near future*.
High	51% to 80%	This event is likely to occur in the near future*.
Medium	21% to 50%	This event may occur in the near future*.
Low	6% to 20%	This event is possible but highly unlikely to occur in the near future*.
Very Low	0% to 5%	This event is not expected to occur in the near future*.

* 'Near future' is defined in this instance as over the next two years.

Table 4: Impact Categories

	Delivery	Budgetary	Timeline	Operational	Reputation
Very High	Will not be able to meet business unit objectives	> 40% deviation from budget	> 20% time increase to delivery timelines	Major outage of critical systems	Potential for reduction of company mandate
High	Major shortfalls in meeting business unit objectives	20% to 40% deviation from budget	10% to 20% time increase to delivery timelines	System becomes unavailable for a significant period of time / SLA targets are not met	Serious adverse attention from clients, media, medical establishment and/or public
Medium	Minor shortfalls in meeting business unit objectives	10% to 20% deviation from budget	5% - 10% time increase to delivery timelines	Major degradation in operational performance / system becomes unavailable for a brief period of time	Some loss of reputation among clients / partners
Low	A few shortfalls in meeting business unit objectives	< 10% deviation from budget	< 5% time increase to delivery timelines	Minor degradation in operational performance	Internal loss of reputation
Very Low	Business unit should still meet defined objectives	Insignificant deviation from budget	Insignificant time increase to delivery timelines	Little interference on internal operations	Insignificant effect on reputation

D. Risk Analysis

The combination of threat likelihood and size of impact give rise to several levels of risk. Table 5 illustrates a model based on five levels of risk.

Table 5: Sample Risk Tolerance Matrix

Impact					
Very High	4	4	4	5	5
High	3	3	3	4	5
Medium	2	-2	3	3	4
Low	1	2	2	3	4
Very Low	1	1	2	2	3
	Very Low	Low	Medium	High	Very High
	Likelihood				

Level	Risk Levels
5	Very High Risk
4	High Risk
3	Medium Risk
2	Low Risk (Tolerable)
1	Very Low Risk (Tolerable)

Default Risk Tolerance Line

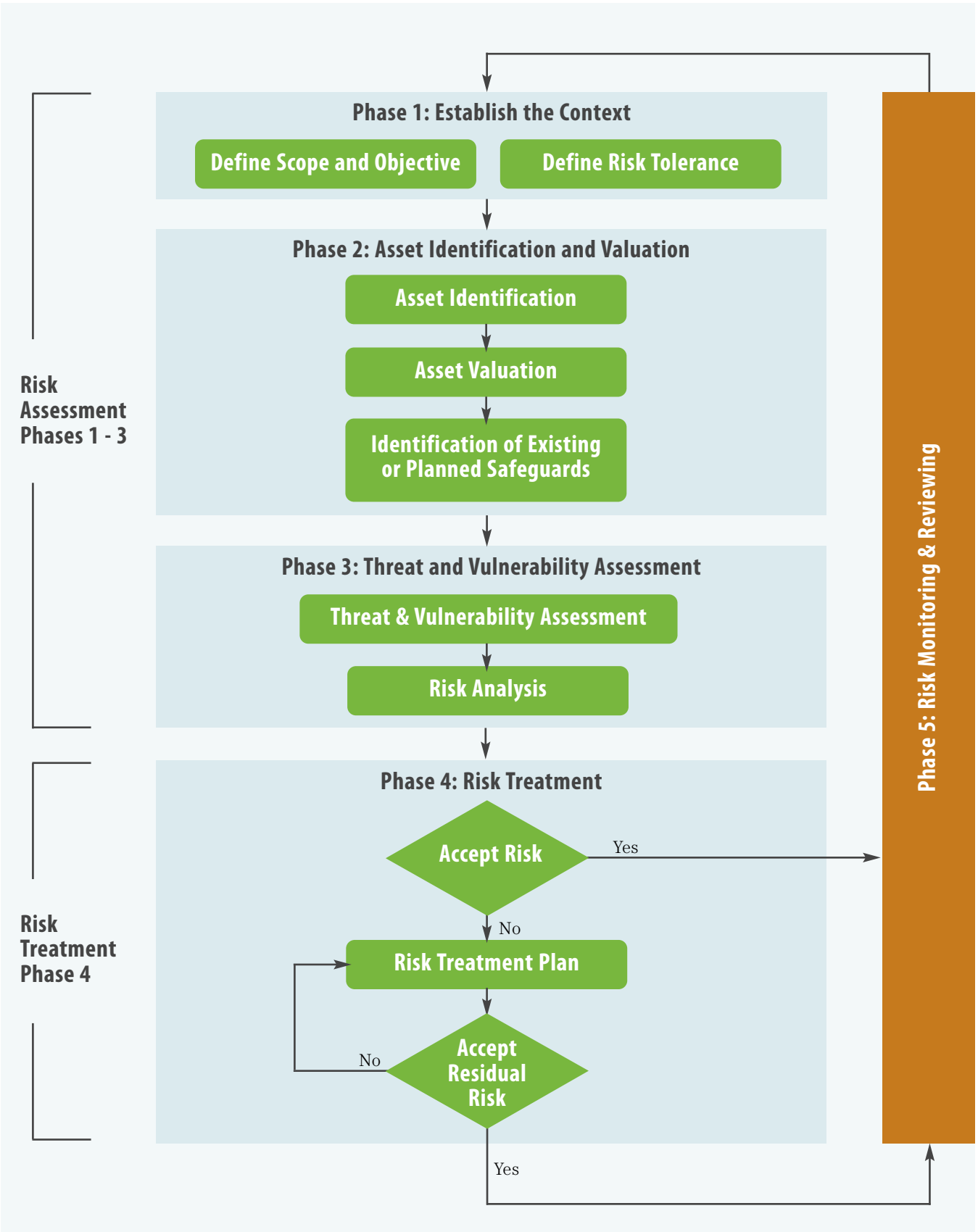
Table 5 is a suggestion only and is not the only method an organization can use to assess risk. How the two contributing factors (the impact and the likelihood) are combined to determine the risk depends upon the organization and the particular risk assessment method chosen.

The decision on final risk level should take into account:

- the real monetary or intangible value of the assets at risk
- the likelihood of threats occurring to cause the potential adverse business impacts
- the ease of exploitation of the vulnerabilities by the identified threats
- any existing or planned safeguards which might reduce the risk

This will help prioritize the risk treatment plan and identify the strength and urgency of the required safeguards.

Diagram 3: Risk Methodology



4.3 Risk Treatment

Once the Risk Assessment has been completed, identified risks must be reviewed and a decision criteria must be determined on how to address the risks. There are four possible risk treatment strategies to choose from:

Risk Mitigation:

The risk is limited by implementing controls that minimize the adverse impact of a threat exploiting a vulnerability. More often than not, risk mitigation is the approach taken by most organizations. Risk mitigation can be achieved through a multitude of preventative and/or detective controls. For example, it may include development of clear and practical security policies and procedures, employee training and awareness, encryption of sensitive information on databases, use of security tokens for strong authentication, development of a security architecture that places sensitive information behind one or more layers of protection, i.e., a firewall.

Risk transfer:

The risk or its impact is transferred to another party such as a supplier, through contracts, insurance and other mechanisms to limit the severity of consequences to the organization or affected stakeholders. This is normal practice where it is most practical due to the difficulty and/or high cost of reducing the magnitude of potential harm. Note: Risk transfer through insurance is still rare in the IT industry and is usually limited to insurance against equipment failure, but not against information loss.

Risk Avoidance:

The risk is avoided by changing the business scope, technical characteristics or usage of the information or system determined to be at risk. An example of this option would be a decision to not give local system administration privileges to novice computer users (e.g., office administrative staff, assistant medical practitioners). The user may be inconvenienced by the inability to download and install software or applications that require administrative privileges, however, this limitation on their system permissions has the advantage of avoiding risks related to downloading potentially malicious software applications, such as keyboard loggers, spy-ware, viruses, etc., which may in turn, impact the confidentiality and integrity of the network and/or stored PI/PHI.

Risk Acceptance:

The risk is accepted as is and operation of the system continues, perhaps with a plan to reduce it in the future by implementing controls to lower the risk to an acceptable level. Risk acceptance is a common practice when identified risks fall below the risk tolerance line defined by management practice when identified risks fall below the risk tolerance line defined by management.

Once a decision has been made on how to treat the risks, a corrective action plan should be put into place outlining what must be done, by whom and by when. The action plan must be monitored for progress and completion.

4.3.1 Phase 4: Risk Treatment

In many situations the risk level identified in the Risk Analysis phase will be deemed unacceptable and a risk treatment plan will be put in place.

A. Risk Treatment Plan

A typical risk treatment plan outlines the following information:

- Threat/vulnerability combination causing the risk
- Risk level
- Selected risk treatment options
- Reasons for selecting those options
- Reduced projected risk level
- Person assigned to deal with the risk
- Expected completion date of the risk treatment
- Status
- Risk category

The plan shows how each identified risk will be treated, the safeguards that are already in place, the additional safeguards to be applied, the timeframe for implementing them and the person responsible for implementing the safeguard. Once the Risk Treatment Plan has been approved, resources can be allocated and activities initiated.

Table 6 provides an example of a Risk Treatment Plan in a spreadsheet format, populated with sample information that can be used to document the plan. The Risk Treatment Plan template in Excel file-format is available online.

Table 6: Risk Treatment Plan Example

Risk Category	Threat / Vulnerability Combination Causing Risk	Risk Level	Observation Comment	Risk Treatment	Reduced Risk Level	Assigned to	Expected Completion Date of Risk Treatment	Status of Risk Treatment
Legal & Compliance	Non-compliance to legislation or contractual obligations / No restriction of access to personal information	High	No restriction for staff that does not require access to personal health information	Management support on restriction of personal health information to staff Develop procedures and standards on restriction of personal health information and communicate throughout organization	Low	John Smith	June 31st, 2007	March 31, 2007 Management meeting to communicate the need to restrict access to personal health information April 3, 2007 Build draft of procedures on restricting access to personal health information
Productivity Loss	Security breaches due to ineffective security management / Employees are not aware of their security responsibilities	High	Many practitioners are unaware of PHIPA requirements		Low	John Smith	June 31st, 2007	In progress
Network Security	Breaches due to weakness in network security / Out of date firewall software/patches	Medium	Firewalls have been not been updated in the last four months	Update all firewalls with software/patches	Low	John Smith	June 31st, 2007	In progress

B. Analyze Residual Risk

No system can be absolutely secure. There will always be some residual risks, i.e. risk remaining even after risk treatment. Residual risk should be assessed and categorized as either 'acceptable' or 'unacceptable'. It will be up to management to decide whether the residual risk can be accepted or whether additional safeguards should be implemented. These decisions should be based upon the organizations risk tolerance.

If management chooses not to implement additional safeguards to further reduce the residual risks, the resulting residual risk is deemed ‘acceptable’ and must be documented and approved by management.

C. High Risk Acceptance

In a number of cases a project team may determine that risks remain high, even after the application of some risk mitigation solutions, however additional changes to further reduce the risk may not be practical. Planning, procuring and implementing additional safeguards to further reduce the risk may impact the project delivery dates, may require substantial redesign, may require specialized staff training, or may require additional funding. In such cases project teams have the option to present the higher than desired risk to senior management and get approval to move into or continue IT production operations despite the elevated level of risk. In these situations the standard practice is to document the senior management approval of the accepted high risk level and to schedule a review of the risk level at a later time.

A sample High Risk Acceptance form, which documents the risks and includes management approval is found in Appendix G. Each organization can develop their own form and process for risk acceptance, using this sample as a model.

4.4 Risk Monitoring & Reviewing

Programs and processes will change, as can the political, social and legal environment and goals of the organization. It is necessary to continually monitor risks, the effectiveness of the risk treatment plan and the management of the implemented safeguards. An ongoing review is essential to ensure that the plan remains relevant. Factors which may affect the likelihood and impact (consequences) of a threat may change over time, as may the factors which affect the suitability or cost of the various risk treatment solutions.

The benefit of monitoring and periodically reviewing risk is that the changes listed above are captured in the risk management program and the program remains up to date. Otherwise, the program will be dated and new/different risks will go unnoticed and unaddressed. This could lead to potentially severe security and privacy incidents.

Monitoring and reviewing is an essential step for:

- Managing risks
- Monitoring the effectiveness of the corrective action plans
- Monitoring the strategies and management systems that have been set up to control the implementation of the risk treatments
- Monitoring and reviewing establishes risk assessments as a vital part of business processes.

Case Study : Stolen Information

At Toronto's Hospital for Sick Children (SickKids,) a laptop computer containing the personal health information of 2,900 patients of the hospital was stolen. The personal health information stored on the stolen laptop included patients' names and numbers as well as information relating to patients' medical conditions. In some cases, very sensitive information was included, such as drug therapy and HIV status. The only security measure on the laptop was a login password. The incident caused Ontario's Information and Privacy Commissioner Ann Cavoukian to order SickKids to introduce privacy safeguards, specifically the need to encrypt any personal data taken out of the hospital on a laptop or other remote computing device.

"All health information custodians", said Commissioner Cavoukian, "should invest in proactive measures to protect personal health information stored on mobile computing devices. In the event that such a device is lost or stolen, this would save custodians time and money by allowing them to avoid the notification requirements of PHIPA, as well as protecting individuals from the undue stress of knowing that their personal health information was lost or stolen. It will also prevent the potentially irreparable damage to a custodian's reputation resulting from the loss or theft of health information from their hospital or office."

Source:

"Identify Theft Revisited: Security is Not Enough". http://www.ipc.on.ca/images/Resources/idtheft-revisit.pdf

"Stolen laptop sparks Order by Commissioner Cavoukian requiring encryption of identifiable data: Identity Must be Protected". http://www.ipc.on.ca/images/Resources/up-2007_03_08_ho_004.pdf

Appendix A:

Information Security Policy

The following is a sample Information Security Policy. It includes common areas typically included in an information security policy. Use it as a guide for creating an Information Security Policy that suites your organization or use it to verify that your existing policy is compliant

Document Control

The electronic version of this document is recognized as the only valid version.

Document Location:	< Where the policy is accessible >
Review Frequency:	This document will be reviewed every_____ years.
Document Prime*: *Enquiries relating to this document should be referred to the responsible document prime.	< Name and contact information of the individual >
Document Sensitivity:	< Sensitivity level of the document >

Approval History

Approver(s)	Title	Approved Date
< Authority or approving body >	< Title of approving body or individual >	< Date of approval >

Revision History

Version No.	Version Date	Summary of Change	Changed By
< 0.01>	<YYYY-MM-DD >		

1 Purpose

[Organization Name] relies upon the confidentiality, integrity and availability of its information and technology-based systems to conduct business and provide patient care. It is essential that information and technology-based systems are continuously protected and utilized in a secure and controlled manner.

Legislation, regulatory directives and industry practices require *[Organization Name]* to exercise due diligence in information security. Patients expect and trust that *[Organization Name]* will protect the confidentiality, privacy and integrity of their information and that *[Organization Name]* services will be available when needed. Meeting these expectations is essential to promoting patient safety and retaining patient trust and loyalty.

This information security policy assigns the responsibilities for security as well as for reporting and oversight.

2 Objective

Information security is a means through which security-related risks can be managed to appropriate levels and the informed trust of relying parties can be gained and maintained. It is not possible or even desirable, to eliminate all risks. Information security serves the specific objectives of reducing the uncertainty and controlling the likelihood, nature and consequences of potential unwanted events, thereby limiting harm, preserving existing value and enabling enhanced value to be derived from information, information technology and associated services.

Security mechanisms and practices will be implemented to appropriately protect information collected, used, stored, transmitted, disclosed, or exchanged by *[Organization Name]* and to assure the continued delivery of services through the use of information systems.

3 Scope and Applicability

This information security policy is meant to provide the highest level guidance from senior management of the organization on *[Organization Name]*'s approach to information security. The information security policy can be supported by topic-specific policies, standards and operating procedures.

This information security policy applies to all activities and employees within *[Organization Name]* and to all third parties including suppliers and vendors of services to *[Organization Name]* that involve access to or handling of any of *[Organization Name]*'s or patients' health information.

4 Information Security Principles

An information security principle provides a statement of value, operation, or belief for the organization as a whole, on *[Organization Name]*'s approach to information security. It must be applicable and enforceable.

The intent of the information security policy is to achieve the following:

1. Compliance with Laws and Regulations – All necessary steps must be taken to be aware of and address all legal, regulatory and contractual requirements pertaining to security and privacy of information and technology-based systems.
2. Safeguarding of Information Assets – All participants must be responsible for safeguarding the privacy and confidentialityof information in all forms, whether created by the organization or entrusted to the organization by patients, partners or suppliers.
3. Ethical Practices- Information and technology-based systems must be used and the administration of information security practices must be executed, with the highest priority given to the preservation of the integrity of personal and personal health information.
4. Accountability - Individual accountability and responsibility for information security must be clearly and consistently defined and acknowledged.
5. Integration – Strategies, policies and standards for managing information security must be closely co-ordinated and integrated with the vision, objectives and plans of the organization as a whole.
6. Awareness - Participants must be aware of the need for the security of information and technology-based systems and they must know what they can do to maintain security.
7. Responsibility - All participants are responsible for the security of information and technology-based systems.
8. Proactive Prevention and Response - Participants must act in a timely and co-operative manner to prevent, detect and respond to security incidents.
9. Risk management - Information security risks must be analyzed, treated and monitored throughout the organization.
10. Reassessment - The security of information systems and networks should be reviewed and reassessed at regular intervals so that appropriate modifications to security policies, standards, safeguards and procedures can be made.

5 Policy Statement

[Organization Name] shall:

- Protect the confidentiality, integrity and availability of information in accordance with legal obligations and the reasonable requirements of the parties that control the information (the information stewards, custodians and authorized users)
- Protect the integrity and availability of information technology-based services
- Hold individual users accountable for unauthorized or inappropriate access, disclosure, disposal, modification, or interference with sensitive information or services.

Information and associated services must be obtained secure in line with legal and business requirements throughout their life cycles, so as to optimize the combination of net value derived and risk incurred.

5.1 Information Security Program

Consistent with the above noted information, *[Organization Name]* will employ an information security management program that includes the following:

- Establishment of governance, strategy and a policy framework for information security
- Definition of an approach for the information security program, as well as for the processes that enable the ongoing operation of the program
- Definition of a training and awareness framework for information security
- Monitoring and reporting on the status of the information security program
- Guidance for information security operations.

5.2 Governance

A governance and policy framework must be established that allows for strong linkages between the governance elements. This framework must establish appropriate organizational structures, roles and responsibilities for establishing and implementing policies and guidelines.

- This information security policy must be reviewed every two years and updated as needed. The policy must be approved by the person who is responsible for the information security program
- Information security operating directives shall support the policy by defining the information security program and information security management system (ISMS) in greater detail, clarifying managerial accountabilities and responsibilities and specifying the required outcomes of management of information security.

5.3 Education and Awareness

Information security policies, standards and guidelines must be communicated to all employees and service providers, to ensure that they understand how their roles and responsibilities are affected by information security.

Awareness programs shall include standards, requirements, guidelines, responsibilities, related enforcement measures and consequences for non-compliance.

5.4 Information Classification

Management must routinely identify, valuate and document information assets and assign levels of sensitivity, criticality and ownership to them. All information custodians must appropriately control and manage their information assets with respect to integrity and availability. All personal and personal health information will be classified as confidential and treated with the highest level of sensitivity.

5.5 Transmission of Information

Standards and layered controls must be established to ensure that the communication and transmission of information as appropriate. This includes appropriate controls and monitoring over the exchange of information with related entities or service providers.

5.6 Access Control

Appropriate logical and physical controls must be established to balance access to information and technology-based systems against potential risks throughout the information lifecycle, from acquisition to destruction.

This includes the establishment of appropriate controls to authenticate and authorize users while providing access to information and technology-based systems, so that they may fulfil their roles and responsibilities.

5.7 Physical Security

Appropriate measures must be taken to ensure that physical access to information and technology-based systems is controlled.

5.8 Business Continuity Plans

Appropriate business continuity measures and plans must be developed and maintained in anticipation of significant disruptions of service. Consideration must be given to the risks and consequences associated with a disruption in service delivery.

The potential consequences of disasters, security failures and service disruptions must be analyzed to determine the criticality of services and supporting IT infrastructure components. Integrated plans must be developed, implemented and tested to ensure that all critical business services are either maintained or can be restored on a prioritized basis, to an acceptable level and within the required timeframes, in the event of failure. Business continuity commitments for critical services must be incorporated into Service Level Agreements with providers and clients.

5.9 Monitoring and Reporting

There are two distinct and important aspects of monitoring and reporting:

- Information security incidents (even if only suspected or resolved without impact) that have the potential for significant impact or consequences, or that involve service providers, must be reported to the appropriate personnel
- The utility and/or effectiveness of the organization's information security program must be measured and reported on, to provide a comprehensive strategic view of the information security program.

6 Roles and Responsibilities

Many areas or individuals (Board, Senior Management, Chief Information Security Officer, Employees, Information Security Group, Technology Group, etc.) play a role in a cohesive and comprehensive information security management program. The Roles and Responsibilities section includes the job titles and relevant departments that have specific roles within the information security management program. Each explicitly defined role has its associated responsibilities outlined.

In accordance with ISO, in every organization, regardless of size, the responsibility for managing the information security requirements needs to reside with at least one individual. All staff must be aware of the security responsibility undertaken by this nominated individual. This individual should ensure that there is clear direction and visible management support for security initiatives involving the security of health information.

6.1 The Board

- Provide guidance and oversight for security risk management program.

6.2 CEO

- Review and approve the Information Security Policy and appoint a Chief Privacy and Security Officer (CPSO) or Chief Security Officer.

6.3 Executive Leads

- Provide direction and oversight for management of security-related business risks within their areas of responsibility.
- Commit appropriate resources and adapt processes to integrate, embrace and support the Information Security Management Program.
- Ensure that all business operations and service delivery are in accordance with this Policy and <supporting standards>.
- Ensure that adequate procedures and training and awareness programs are implemented to make all employees, contractors and vendors' personnel aware of their obligations under PHIPA and that they sign an Acknowledgement of Confidentiality which clearly states their obligations in relation to access to Personal Information and Personal Health Information.

6.3.1 CPSO/CSO

- Develop and manage information security governance, the information security program and the necessary specialist staff resources, processes and technology.
- Champion and maintain enterprise-wide business continuity processes and plans.
- Commission external audits of the information security program.

7 Reference and Associated Documents

The following documents were referenced within this policy.

Reference
ISO/IEC 17799:2005 Information Technology – Code of Practice for Information Security Management
ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Management Systems – Requirements
ISO/DIS 27799 Health Informatics – Security Management in Health Using ISO/IEC 17799
Personal Health Information Protection Act, 2004 – Ontario
COACH - Guidelines for the Protection of Health Information, Dec 2006

Appendix B:

Information Security Policy Checklist

The following checklist includes high level information security policy requirements that are highly recommended for an organization to implement. Use this checklist to ensure that your policy fulfills these recommended elements.

☐	A written information security policy document exists.
☐	The information security policy has an owner.
☐	There is a defined process for reviewing the policy document.
☐	There are scheduled / periodic reviews of the policy.
☐	The policy has been distributed to all the employees and contractors to whom it applies.
☐	The policy defines the objectives and scope of information security for the organization.
☐	The policy contains and describes responsibilities for all aspects of information security.
☐	The policy contains a statement from management supporting the goals and principles of information security.
☐	The policy contains explanations of security policies, principles, standards and compliance requirements, including PHIPA and PIPEDA.
☐	The policy complies with contractual requirements.
☐	The policy addresses security education and awareness requirements.
☐	The policy addresses business continuity.
☐	The policy addresses the consequences of policy violations.

Appendix C:

Information Security Roles & Responsibilities

On the following page are examples of common types of roles and responsibilities in a medium to large organization. Use it as a guide to establish relevant roles and responsibilities in your own organization. You may need to adjust, combine, change, add to, or remove from it to develop an Information Security organization tailored to your organization. For additional roles and responsibilities related to the health sector, please refer to COACH's Guidelines for the Protection of Health Information (Dec 2006 version).

Role	Responsibilities
Information Security Management	• Assigned to an individual with Senior Business Management responsibility • Staff awareness and training of their responsibilities regarding information security • Developing the information security policy, objectives and strategy • Defining the scope of the information security management system (ISMS) • Carrying out the initial risk assessment and identifying risk • Getting agreement from senior management on the organization's approach to risk management and the risk treatment plan • Selecting security controls which will meet the business objectives • Recording and handling security incidents, including establishing their causes and determining appropriate corrective and/or preventive actions • Reporting to senior management on the progress of implementing the information security program, and on incidents, issues, security matters and current threats.
Compliance Officer	• Should be independent of the information security program • Monitoring and reviewing compliance with the information security policy and security best practices • Ensuring compliance with legislation and regulations (e.g., PHIPA and PIPEDA)
Information Technology Management	• Identifying system and network perimeter threats • Implementing selected system (e.g., passwords), network (e.g., firewalls) and physical (e.g., security cameras) security controls • Reporting technical vulnerabilities and incidents to senior management • Setting up security monitoring • Detecting and responding to threats • Planning for business continuity • Maintaining and testing disaster recovery plans • Ensuring that virus updates and system patches are applied as appropriate • Enforcing security requirements with external providers • Managing security for the computing facility
IT Users	• Follow the organization's security policy and procedures • Follow physical security procedures • Backup PC data (this is particularly important for notebook and PDA users) • Report security incidents • Understand your organization's Privacy and Security Professional Code of conduct. • Adhere to the security policies and make security part of everyday business.

Appendix D:

Assessment Checklist

1. Risk Assessment

- Has a risk assessment methodology been identified that is suited to the organization's information security program?
- Does the risk assessment have a clearly defined scope? (e.g. whole organization, parts of the organization, individual system, specific system components or services where practical)
- Have criteria for identifying the acceptable levels of risk been developed (i.e., a risk tolerance matrix)?
- Is a risk assessment process in place and being used in identifying risks?
  - Does this process identify the assets within the scope of the information security program and the custodians of the assets?
  - Does this process identify the threats to these assets and the vulnerabilities that might be exploited by those threats?
  - Does this process identify the impacts that losses of confidentiality, integrity, or availability may have on the assets?
- Are risk assessments performed periodically?
- Is the effectiveness of safeguards assessed?
- Is there a process to request acceptance and get management approval for high risk?
- Is the effectiveness of the selected safeguard measured to check if the risk is reduced to an acceptable level? Examples of factors to determine if risk is reduced to an acceptable level include:
  - Meeting organizational objectives
  - Meeting requirements and constraints of applicable legislation and regulations
  - The cost to implement safeguards, compared to the value of the assets
- Does the risk assessment process include a risk treatment plan that identifies the appropriate management action, responsibilities and priorities for managing risks?
- Does management continuously monitor, evaluate and improve the efficiency of the selected security safeguards?
- Are defined criteria in place to help identify effective risk treatment once the risk assessment is completed? Risk treatment options include:
  - Applying appropriate safeguards to reduce the risks
  - Avoiding the risk by avoiding the activity creating the risk
  - Transferring the risk or its consequences to another party
  - Knowingly and objectively accepting the risk

2. Information Security Policy

- Does a written information security policy document exist?
- Does the written information security policy have someone that is:
  - Accountable for the policy
  - Responsible for the policy
  - Managing the policy
- Is there a defined process for reviewing the policy document?
- Are there scheduled, periodic reviews of the following:
  - Nature, number and impact of recorded security incidents
  - Cost and impact of controls on business efficiency
  - Effects of changes to technology
- Has the policy been distributed to all employees and contractors for whom it is applicable?
- Does the policy contain a definition of the objectives and scope of information security?
- Does the policy contain definitions of specific and general responsibilities for all aspects of information security?
- Does the policy contain a statement of management intention, supporting the goals and principles of information security?
- Does the information security policy contain explanations of security policies, principles, standards and compliance requirements, including:
  - Compliance with legislative requirements (e.g. PHIPA, PIPEDA)
  - Compliance with contractual requirements
  - Security education requirements
  - Business continuity management requirements
  - Consequences of security policy violations

3. Organization of Information Security

- Is there a senior management forum with responsibility for reviewing information security?
  - Regular review of policy and standards.
  - Regular review of security responsibilities
  - Monitoring of significant changes in the exposure of information assets to major threats.
  - Regular review and monitoring of security incidents.
  - Regular review of exposure to threats.
  - Approval of initiatives for enhancing information security
- Is information security co-ordinated satisfactorily across the organization?
- Have all staff with access to confidential information been identified?
- Have responsibilities for the protection of individual assets and for carrying out specific security processes been explicitly defined and allocated?
- Have local responsibilities for individual physical and information assets and security processes, such as business continuity planning, been clearly defined?
- Have custodians of all information assets been identified, and have they all accepted those responsibilities?
- Is there a process to ensure that all purchases and installation of IT equipment and services are properly authorized and approved,to ensure that:
  - there is a clear business purpose
  - installation will not adversely affect existing security measures
  - the new equipment or services are provided with a

sufficient level of security

- Is the implementation of information security independently reviewed?
- Have the risks associated with third parties been identified and assessed with respect to:
  - Physical access (e.g., access to office, filing cabinets, laboratories, etc.)
  - Logical access (e.g., access to databases, intranet, etc.)
- Is third party access based on a formal contract, containing all the security requirements to ensure compliance with the information security policy?

4. Asset Management

- Are all major information and IT assets clearly identified and maintained in an inventory?
- Do all major information and IT assets have an identified custodian?
- Have the information custodians documented who is authorized to access their information?
- Have all information assets been labelled and classified in accordance with their sensitivity?

5. Human Resources Security

- Are all security roles and responsibilities assigned and included in staff job descriptions or performance objectives where appropriate?
- Are background checks made on all potential employees (including contractors, third parties and volunteers) who will have access to IT facilities handling sensitive information? These checks include:
  - At least two satisfactory character references
  - A check for completeness of the applicant's curriculum vitae
  - Confirmation of academic qualifications
  - A positive personal identification check
  - A Canadian Police Information Centre (CPIC) check for employment (for particularly sensitive jobs)
- Do the terms and conditions of employment:
  - State the employee's responsibility for information security?
  - State the action to be taken if the employee disregards the security requirements?
- Have All staff been required to sign the confidential agreement prior to employment?
- Are employees and relevant contractors and third party given security education when they join the organization?
- Do employees receive updates to information security training at least annually?
- Are there formal disciplinary proceedings for employees who have committed a security breach?
- Have access rights to information and information resources of all employees, contractors & third parties been removed upon termination of the employment and contract?
- Do all employees return all assets in their possession upon termination of their employment, contract, or agreement?

6. Physical & Environmental Security

- Are there controls to prevent unauthorized entry into secure areas and to restrict activities within them?
  - Visitors to secure areas are supervised
  - Visitors' entry and exit times are recorded and reviewed.
  - Logs of access should be reviewed at least weekly by management (a manager should be made responsible for each access-controlled area).
  - Visitors are only granted access for specific, authorized purposes.
  - Controls exist for personnel supplying or maintaining support services in secure areas - All authorized personnel display visible identification.
  - Appropriate physical barriers are in place (floor to ceiling)
  - Appropriate entry controls are in place.
- Has consideration been given to the need for additional protection (e.g., encryption, physical security and alternative routings) for exceptionally sensitive or critical systems?
- Is equipment protected from power failures and power surges?
- Are power and telecommunications cabling protected from interception or damage?
- Is a 'Clean Desk' policy in place?
  - Documents and magnetic media are stored in cabinets when not in use, especially outside working hours.
  - Confidential or critical patient information is locked away (ideally in fire and water resistant cabinets) when not in use especially when the facility is not occupied or when visitors are present.

7. Communications & Operations Management

- Have responsibilities and procedures for the management and operation of all computers and networks been clearly defined?
- Is an adequate change control process in place to prevent security exposures? This process should include:
  - Identification and recording of significant changes
  - Assessment of the potential impact of such changes
  - Formal approval procedure for proposed changes
  - Communication of change details to all relevant personnel
  - Procedures identifying responsibilities for aborting and recovering from unsuccessful changes.
- Are audit logs and similar evidence collected and secured for:
  - Internal problem analysis?
  - Use as evidence should litigation occur?
  - Negotiating for compensation from software and service suppliers?
- Are controls in place to reduce the risks associated with electronic mail? Consider the following:
  - Vulnerability of messages to unauthorized interception or modification
  - Vulnerability of messages to incorrect addressing or misdirection
  - Legal considerations (authenticity, proof of origin, etc.)
  - The implications of publishing directory entries
  - Implications of publishing externally accessible staff lists
  - Security measures to control remote user access

- Are there clear, complete, documented procedures for the correct and secure operation of the network and computers? Procedures must exist for:
  - The correct handling of data files
  - Scheduling requirements (job dependencies, start and end times, etc.)
  - Error handling
  - Support contacts in the event of problems
  - System restart and recovery
  - Start up and shutdown
  - Data backup
  - Equipment maintenance
  - Computer room management
  - Safety considerations
  - System monitoring
  - Recovery from individual component failure
  - Recovery from environmental and infrastructure failure (e.g. power, PTT, etc.)
- Are regular backups made in compliance with business units' and information custodians' business continuity plans?
- Are logs maintained of all operator actions, reported or detected faults and environmental monitoring?
- Are procedures in place for secure handling of computer media (removable computer media such as tapes, disks and paper reports) including storage, distribution and disposal?

8. Access Control

- Does an access control policy exist and take into account:
  - Security requirements for individual applications?
  - Identification of all information related to business applications?
  - Policies for information dissemination and authorization?
  - Consistency across different systems and networks?
  - Relevant legislation and any contractual obligations regarding protection of access?
  - Standard user access profiles for common categories of job?
  - Management of access rights, which recognizes all types of connections available?
  - The network and network services that are allowed to be accessed?
  - Authorization procedures for determining who is to be permitted access?
  - Management controls and procedures to protect unauthorized access?
- Are the allocations of user passwords securely controlled?
  - Users sign a statement, committing themselves to keep passwords secure
  - Users are required to change initial passwords at the first log on
  - Passwords are distributed in a secure manner - Users acknowledge receipt of passwords
  - Passwords are stored securely within the systems
  - Does access to IT services use a secure logon process?
  - System and application identifiers are not displayed until logon is complete
  - All systems carry a warning regarding authorized use only
  - The number of unsuccessful attempts to logon is limited (a limit of three attempts is recommended)
  - The maximum and minimum time for logon is limited
  - The date and time of the last successful logon is displayed following successful logon - Details of any unsuccessful attempts are displayed.

9. Information Systems Acquisition, Development & Maintenance

- Are security requirements identified and agreed to prior to the development or purchase of IT systems?
- Are appropriate security and data integrity controls designed into applications?
- Has encryption been considered for protecting the confidentiality of information?

10. Information Security Incident Management

- Are documented incident management procedures in place?
  - Analysis and identification of the cause of the incident
  - Recording of the incident, including collecting of evidence for problem analysis or litigation
  - Notification of business users, information custodians and others affected by or involved in the recovery
  - Actions required in correcting or recovering from security breaches or systems failures
  - Planning and implementation of remedies to prevent recurrence
  - Procedural coverage of all types of incidents including systems failure, errors resulting from incomplete or inaccurate data and confidentiality breaches.

11. Business Continuity Management

- Are business continuity plans in place to protect critical business processes from major failures or disasters?
- Have all business process owners identified their critical business processes and have they communicated their requirements for recovery of the processes?
- Are business continuity plans tested on a regular basis with the active involvement of owners and users?

Compliance

- Are all statutory, regulatory and contractual requirements discussed with the legal or privacy department/team?
- Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system?
- Have appropriate measures been implemented to protect essential records from loss, destruction, or falsification?
- Can adequate evidence be gathered which will conform with the rules of evidence according to the court, such as:
  - Admissibility of evidence?
  - Quality and completeness of evidence?
  - Adequate evidence that controls have operated correctly and consistently?

Appendix E:

Asset Categories

As part of the risk assessment process, an organization will be required to identify all the important assets it owns or is responsible for. Organizations should identify all the assets that are relevant to their business and assign a value to each one. This process will make it easier for organizations to determine which assets require protection. After the assets have been identified, an asset owner should be assigned to each asset. The asset owner will be accountable for safeguarding those assets according to their assigned value and potential risk. The following is a list of sample assets specific to the health care sector:

Category	Example Assets		
Information Assets	Accounting Ledgers Archived information Back up procedures Business continuity plans Contracts Corporate information Customer details Databases Disaster Recovery Plans Drawings Financial information Incident handling procedures Information services	Inventories Lab results Operational documents and procedures Organizational records Outsourcing contracts Paper documents Patient records Payment details Personal health information Personnel information Photographs Product information Research information	Sales/marketing information Service level agreements Slides Software documents System documentation Third party contracts Training material User manuals Video footage X-rays
Software Assets	Applications - developed in-house Applications - Standard (e.g., word processors, spreadsheet applications) Billing Systems Clinical Medical Systems	Communications software Encryption tools Development tools Financial systems Inventory systems HR systems Operating system software Software licenses	Special system software (e.g., special medical software) Utilities (e.g., antivirus software)
Physical Assets	Communications equipment: Answering machines Communications services Fax machines Mobile (cellular) phones Modems Network management centre Networks Routers/Hubs Tapes Telephones	Computing equipment: Cables Card devices CD-ROMs Computer rooms Computers CPUs/memory Discs DVDs Firewalls IC/chips Laptops Magnetic card readers Monitors/displays Operations centre Personal digital assistants (PDAs), etc.	Medical Equipment: Cardiac monitoring machinery Dialysis equipment X-ray machines, etc. General equipment: Air Conditioning Access badges Auxiliary power Buildings Furniture Heating/lighting Offices Photocopiers Power Standby generator Switches Water supplies, etc.
Personal Assets	Administrators (e.g. system admins) Receptionists Cleaning personnel Communications personnel Computer personnel Developers	Health care practitioners (e.g. doctors, nurses, pharmacists, etc.) Managers Network personnel	Security personnel Temporary personnel Third party staff
Intangible Assets	Brand names Confidence (in services offered by the organization)	Confidence (in the organization) Copyright Morale	Goodwill Reputation Trademarks Trust

Appendix F:

Threat & Vulnerability Catalogue

As part of the risk assessment process, an organization will need to identify threats and vulnerabilities for the identified assets. Organizations need to adopt risk assessment and risk management approaches that will appropriately address and identify the complete range of threats and vulnerabilities relevant to their business environment.

The following is a list of threats and vulnerabilities that should be considered by health organizations when assessing risks to the confidentiality, integrity and availability of health information and related business information systems. It is not an exhaustive list of threats and vulnerabilities and should only be taken as examples to illustrate the concepts.

Threats

- acts of terrorism
- air conditioning failure
- airborne particles/dust
- bomb attack
- breach of legislation or regulations
- breaches of contractual obligations
- compromise of assets
- compromise of security
- damage caused by penetration tests
- damage caused by third parties
- destruction of records
- destruction of the business continuity plans
- deterioration of media
- disasters (natural or man-made)
- disclosure of information
- disclosure of passwords
- disruption to business processes
- illegal use of software
- industrial action
- information leakage
- information security incidents
- interception
- interference
- interruption to business activities and processes
- lightning
- loss of integrity
- loss of records
- loss of service
- maintenance error
- malfunctions of supporting utilities
- malicious code
- masquerading of user identity
- misuse of audit tools
- misuse of information processing facilities
- misuse of resources or assets
- network access by unauthorized persons
- operational support staff error
- power fluctuation
- security failure
- software failure
- system failure
- system misuse (accidental or deliberate)
- theft
- unauthorized access
- unauthorized access to audit logs
- unauthorized access to audit tools
- unauthorized modification of audit logs
- unauthorized or unintentional modification
- unauthorized physical access
- unauthorized use of software
- dust
- earthquake
- eavesdropping
- environmental contamination (and other forms of natural or man-made disasters)
- equipment failure
- errors
- failure of communications services
- failure of supporting utilities (such as electricity, water supply, sewage, heating, ventilation and air conditioning)
- falsification of records
- fire
- flooding
- fraud
- hardware failure
- hurricane
- introduction of unauthorized or untested code
- illegal import/export of software
- use of network facilities in an unauthorized way
- use of software by unauthorized users
- use of software in an unauthorized way
- user error
- vandalism
- violation of intellectual property rights
- willful damage

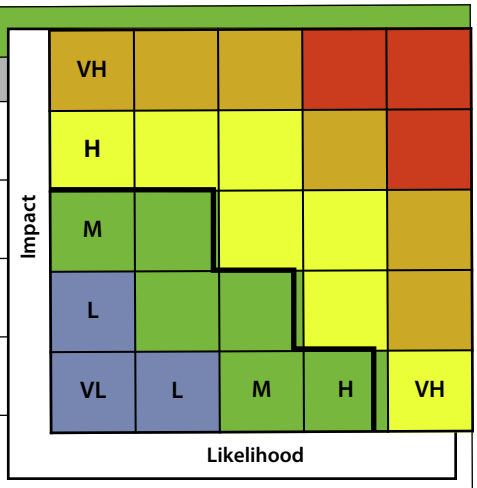
Vulnerabilities

- Disposable or reuse of storage media without proper erasure
- Failure to apply application security patches
- Inadequate or careless use of physical access control to buildings, rooms and offices
- Insufficient maintenance/faulty installation
- Insufficient security training
- Lack of backup procedures
- Lack of clear desk and clear screen policy
- Lack of identification and authentication mechanisms like user authentication
- Lack of networks monitoring from intrusion attempts
- Lack of encryption on mobile devices, i.e. laptops
- Lack of SPAM filters on email systems
- Lack of monitoring mechanisms to detect intrusion attempts, i.e. on networks, hosts, applications, physical space
- Lack of physical protection for the building, doors and windows
- Lack of periodic equipment replacement schemes
- Lack of policies for the correct use of telecommunications media and messaging
- Lack of updates to guard against malicious software, i.e. anti-virus, anti-spam
- Lack of security awareness
- Location in an area susceptible to natural disasters
- No or incorrect access control policy
- No “logout” when leaving the workstation
- No removal of access rights upon job termination
- No segregation of duties
- No procedure to ensure return of asset upon job termination
- Poor password management (easily guessable passwords, storing of passwords, insufficient frequency change)
- Susceptibility of equipment to humidity, dust, soiling
- Susceptibility of equipment to temperature variations
- Susceptibility of equipment to voltage variation
- Unstable power grid
- Unmotivated or disgruntled staff
- Unprotected storage
- Unprotected public network connections
- Unsupervised work by outside staff or staff working outside normal business hours

Appendix G:

High Risk Acceptance Form

Risk ID Number	Assigned by InfoSec
Risk Title	**Assigned by InfoSec**
Date Risk Identified	
Risk Owner (name / title)	
Project / Portfolio / Product	
Risk Description	
Risk Root Cause	
Risk Impact (text description)	



Impact (VL, L, M, H, VH)	Likelihood (VL, L, M, H, VH)	Risk Rating (VL, L, M, H, VH)
Assigned by InfoSec	**Assigned by InfoSec**	**Assigned by InfoSec**
Reason why risk cannot be reduced to an acceptable level?		
Information Security Recommendations		
Mitigating Controls (to be implemented)		
Period that the Acceptance is required (Maximum 1 year)		

High Risk Acceptance Signatures

The Risk Owner (executive sponsor) acknowledges accountability for this risk:

<print name>	<signature>
<title, organization name>	Date:

Privacy & Security approval of the Risk Acceptance:

<print name>	<signature>
<title, organization name>	Date:

Appendix H:

Glossary of Terms

Term	Definition
Asset	Anything that has value to the organization [ISO 27001:2005].
Asset Registry	A record of assets that helps identify assets within the organization.
Availability	The property of being accessible and usable upon demand by an authorized entity [ISO 27001:2005].
Compliance	Meeting the requirements of laws, regulations, policies and standards.
Confidential information	Sensitive information that needs to be protected in order to respect the privacy rights of the individual. Confidential information is typically disclosed only to authorized individuals, entities, or processes.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO 27001:2005].
Control	A means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be administrative, technical, managerial, or legal in nature [ISO 17799:2005].
Harm	Loss of or damage to an organization's or a person's right, property, business, reputation, or physical or mental well-being.
Identification	The process that enables unique recognition of one entity by another, generally by the use of names (e.g. user names, system names).
Integrity	The property that information is valid (authentic, consistent, complete, unmodified unless legitimately) and reliable.
Information management	The direction and control of production, use, transformation, exchange, protection and disposal of information by an organization.
Information security	The preservation of confidentiality, integrity and availability of information [ISO 17799:2005].
Information security guideline	A statement of advice concerning good business practice to retain a secure environment. A security guideline describes optional and additional security measures and procedures that can be followed to enhance security.
Information security management system (ISMS)	That part of the overall management system, based on business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security [ISO 27001:2005].
Information security policy	A statement of intent and guidance by senior management to the organization as a whole regarding the commitment, ownership, responsibilities, processes and other themes applicable to security. The security policy defines the expected behaviours, responsibilities and rules that are required to be enforced.
Information security standard	A requirement for compliance for a particular means of executing a security function resulting from a security policy. The security standard defines the methods and mechanisms that will be used to enforce the policy. In many cases a security policy and a security standard are combined and referred to as the security policy.
Integrity	The property of safeguarding the accuracy and completeness of assets [ISO 27001:2005].
ISO 17799	ISO/IEC 17799 was renamed to ISO/IEC 27002:2005
ISO 27001	ISO/IEC 27701:2005 Information Technology – Security Techniques – Information Management Systems – Requirements. International standard providing a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).

Term	Definition
ISO 27002	ISO/IEC 27002:2005 Information Technology – Code of Practice for Information Security Management. International standard for information security.
ISO 27799	ISO/DIS 27799 Health Informatics – Security Management in Health Using ISO/IEC 17799. International standard providing guidance to health care institutions and other custodians of personal health information on how to best protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27001 & ISO/IEC 27002.
Personal Health Information (PHI)	Identifying information about an individual in oral or recorded form, if the information, (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual, (c) is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual, (d) relates to payments or eligibility for health care in respect of the individual, (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, or (f) is the individual's health number (PHIPA).
Personal Information (PI)	Identifying information about an individual in oral or recorded form, including: (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual; (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; (c) any identifying number, symbol or other particular assigned to the individual; (d) the address, telephone number, fingerprints or blood type of the individual; (e) the personal opinions or views of the individual except where they relate to another individual; (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature and replies to that correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the individual; and (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual. (FIPPA)
Logical Controls	Safeguards for an organization's systems, including user ID and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.
PHIPA	The Personal Health Information Protection Act is a legislation that outlines privacy regulations for provincial health care information in Ontario, Canada. For a more comprehensive overview and guidance on complying with PHIPA, please consult the Community Mental Health and Addictions Privacy Toolkit – A Guide to Ontario's Personal Health Information Protection Act and Simplifying Privacy: A Tool Kit for Long-Term Care and Community Care.
PIPEDA	The Personal Information Protection and Electronic Documents Act is a Canadian federal law governing how private sector organizations collect, use and disclose personal information in the course of commercial business.
Residual risk	Risk remaining after risk treatment [BS 7799-3:2006].
Risk	The probability of an event and its consequence [BS 7799-3:2006].
Risk acceptance	The decision to accept risk [BS 7799-3:2006].
Risk analysis	Systematic use of information to identify sources and to estimate the risk [BS 7799-3:2006].
Risk assessment	The overall process of risk analysis and risk evaluation [BS 7799-3:2006].
Risk management	The coordinated activities by which risk is identified, assessed, measured, mitigated and monitored.
Risk tolerance	The degree of risk that the organization is willing to accept. Tolerance levels are typically determined by senior management.
Risk treatment	The process of the selection and implementation of measures to modify risk [BS 7799-3:2006].

Term	Definition
Risk treatment plan	A plan that defines the specific actions to be undertaken to implement the required safeguards to protect assets.
Risk management	Coordinated activities to direct and control an organization with regard to risk [BS 7799-3:2006].
Safeguard	A means of managing risk. Safeguards can include policies, guidelines, practices or organization structures, which can be administrative, technical, managerial, or legal in nature.
Segregation of Duties	Segregation of duties is a method of reducing the risk of accidental or deliberate system misuse. "Segregation of duties avoids the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner and in the normal course of business processes. Segregation of duties is an important means by which fraudulent and or malicious acts can be discouraged and prevented." The duties and responsibility for information security should be distributed across a number of people as a safeguard so that no one person can access, modify, or use sensitive assets without authorization or detection. The person who initiates an event should not be able to authorize it. When feasible, the organization should segregate the duties and areas of responsibility to reduce opportunities for unauthorized modification or misuse of personal health information.
Statement of applicability	A documented statement describing the controls (and the objectives of the controls) that are relevant and applicable to the organization's ISMS [ISO 27001:2005].
Temporary Employees	Employees whose work contract has a limited duration.
Third Parties	Third parties include individuals, groups and service providers that support the organization. Examples include; professional consultants, contractors, software and hardware vendors, students, intern placements, volunteers, cleaners, caterers and other support staff.
Threat	A threat is something that takes advantage of a vulnerability which will result in an incident. Threats can be people, process, or technology based.
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats [BS 7799-3:2006].

Appendix I:

References

Document
ISO/IEC 17799:2005 Information Technology – Code of Practice for Information Security Management http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=
ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Management Systems – Requirements http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40&ICS3=
ISO/DIS 27799 Health Informatics – Security Management in Health Using ISO/IEC 17799 (Not currently approved) http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41298&scopelist=PROGRAMME
HB 174-2003 Information Security Management – Implementation Guide for the Health Sector – Standards Australia
BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030125022&recid=1001
AS/NZS 4360:2004 Risk Management http://www.saiglobal.com/shop/script/Details.asp?DocN=AS0733759041AT
Nine Steps to Success – An ISO 27001 Implementation Overview – Alan Calder
Personal Health Information Protection Act, 2004 – Ontario
NIST Special Publication 800-100 – Information Security Handbook: A Guide for Managers
Simplifying Privacy: A Tool Kit for Long-Term Care and Community Care
Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals
Community Mental Health and Addictions Privacy Toolkit – A guide to Ontario's Personal Health Information Protection Act
COACH - Guidelines for the Protection of Health Information

eHealth Ontario

P.O. Box 148, 777 Bay Street,
Suite 701 Toronto, Ontario M5G 2C8
Tel: (416) - 586 - 6500
Fax: (416) - 586 - 4363

Toll free: 1 - 888 - 441 - 7742
Email: info@ehalthontario.on.ca
Web: www.ehealthontario.on.ca