AGENDA
MIDDLESEX-LONDON BOARD OF HEALTH
Governance Committee

Microsoft Teams
Thursday, February 17, 2022 at 6 p.m.

1. **ELECTION OF CHAIR, GOVERNANCE COMMITTEE**

2. **DISCLOSURE OF CONFLICTS OF INTEREST**

3. **APPROVAL OF AGENDA –** February 17, 2022

4. **APPROVAL OF MINUTES –** November 18, 2021

5. **NEW BUSINESS**

   5.1. 2022 Governance Committee Reporting Calendar (Report No. 01-22GC)
   5.2. Governance Policy By-law Review (Report No. 02-22GC)
   5.3. Annual Privacy Program Update (Report No. 03-22GC)
   5.4. MLHU Risk Management Plan (Report No. 04-22GC)

6. **OTHER BUSINESS**

   The next meeting of the Governance Committee will be on Thursday, April 14, 2022.

7. **ADJOURNMENT**

PUBLIC MINUTES
GOVERNANCE COMMITTEE
Microsoft Teams
Thursday, November 18, 2021 6:00 p.m.

MEMBERS PRESENT: Mr. Bob Parker (Chair)
Ms. Aina DeViet
Ms. Maureen Cassidy
Mr. Mike Steele

OTHERS PRESENT: Ms. Carolynne Gabriel, Executive Assistant to the Board of Health and Communications Coordinator (Recorder)
Ms. Stephanie Egelton, Senior Executive Assistant to the Medical Officer of Health / Associate Medical Officer of Health
Ms. Emily Williams, Director, Healthy Organization/Interim CEO
Ms. Kendra Ramer, Manager, Strategy, Risk and Privacy
Dr. Alexander Summers, Acting Medical Officer of Health/Acting Secretary-Treasurer

Chair Bob Parker called the meeting to order at **6:01 p.m.**

DISCLOSURES OF CONFLICT OF INTEREST

Chair Parker inquired if there were any disclosures of conflict of interest. None were declared.

APPROVAL OF AGENDA

It was moved by **Ms. Maureen Cassidy, seconded by Mr. Mike Steele,** *that the **AGENDA** for the November 18, 2021 Governance Committee meeting be approved.*

Carried

APPROVAL OF MINUTES

It was moved by **Ms. Aina DeViet, seconded by Mr. Steele,** *that the **MINUTES** of the October 21, 2021 Governance Committee meeting be approved.*

Carried

RECEIPT OF SUB-COMMITTEE MINUTES

It was moved by **Mr. Steele, seconded by Ms. Cassidy,** *that the **MINUTES** of the October 19, 2021 CEO and MOH Performance Review Committee meeting be received.*

Carried

NEW BUSINESS

Governance By-Law and Policy Review (Report No. 23-21GC)

This report was introduced by Ms. Emily Williams, Director, Healthy Organization / CEO (Interim). Discussion on this report included the following policies:

Policy G-180: Financial Planning and Performance

- Zero-based budgeting will start in 2022 with the Healthy Living Division whose programming has been largely paused or reduced during the COVID-19 pandemic. This will provide an opportunity for the division to do an in-depth review with the Finance Team to review programs and build a robust budget. The concept of zero-based budgeting was added to the policy.
- Program Budgeting Marginal Analysis (PBMA) is a separate part of the budgeting process from zero-based budgeting and is used to determine how to adjust program budgets.
- Legislative impact is an integral part of the PBMA process and ensures programs which are delivered by the Health Unit meet requirements laid out in the *Health Protection and Promotion Act*.
- Amend language in the "Audited Financial Statements" section of the policy to read "These program audit reports are also included in the main audited statements for MLHU" instead of "These programs are also reported in the main audited financial statements of MLHU…"

Policy G-200: Approval and Signing Authority

- Appendices A and B will be amended such that "Board of Health" will be changed to "Board of Health Chair or Vice-Chair."

G-320: Donations

- The policy will be amended to remove "as well as with family members" from the sentence "MLHU will encourage donors to consult with professional advisors of their choice, as well as with family members, prior to making a donation to ensure that the donor will not be disadvantaged by the donation."

It was moved by **Ms. DeViet, seconded by Mr. Steele** that the Governance Committee recommend to the Board of Health to*:*

1) Receive Report No. 23-21GC re: "Governance By-law and Policy Review" for information; and
2) Approve the governance policies appended to this report, as amended.

Carried

Ms. Williams introduced Ms. Kendra Ramer, Manager, Strategy, Risk and Privacy who extended gratitude and thanks to the Governance Committee members for doing a significant amount of work to review the policies and update the governance manual. She advised that there are three policies due to be reviewed and recommended that they go to both the members of the Governance Committee and the Finance and Facilities Committee for review in the coming weeks in preparation for approval at the December Board of Health meeting as they have financial implications. The three remaining policies are: Policy G-220: Contractual Services, Policy G-230: Procurement, and Policy G-250: Reserve and Reserve Funds.

OTHER BUSINESS

Next meeting is TBD in 2022.

ADJOURNMENT

At **6:30 p.m.,** it was moved by **Ms. Cassidy, seconded by Ms. DeViet,** *that the meeting be adjourned.*
Carried

ROBERT PARKER
Chair

ALEXANDER SUMMERS
For Christopher Mackie,
Secretary-Treasurer

MIDDLESEX-LONDON HEALTH UNIT

REPORT NO. 01-22GC

TO: Chair and Members of the Governance Committee

FROM: Emily Williams, Chief Executive Officer

DATE: 2022 February 17

GOVERNANCE COMMITTEE REPORTING CALENDAR & MEETING SCHEDULE

Recommendation

It is recommended that the Governance Committee:

1) ***Receive Report No. 01-22GC re: "Governance Committee Reporting Calendar & Meeting Schedule"; and***
2) ***Recommend that the Board of Health approve the 2022 Governance Committee Reporting Calendar (Appendix B).***

Key Points

- The 2022 Governance Committee Reporting Calendar (Appendix B) provides a framework for activities to be undertaken in the current year.
- New quarterly reporting on the MLHU Risk Management program will commence and has been added to the Reporting Calendar.
- It is recommended that the Governance Committee meet five times in the calendar year to ensure all legislative accountabilities of the Board of Health are fulfilled.

Background

In accordance with Policy G-290 Standing and Ad Hoc Committees, the Governance Committee is authorized by the Board of Health to serve a specific purpose set out in the Terms of Reference (Appendix A). The Terms of Reference was amended to reflect the separation of Medical Officer of Health and Chief Executive Officer roles in accordance with Policy G-030 MOH and CEO Position Descriptions.

The Reporting Calendar delineates the regular activities required of the Committee each calendar year in compliance with applicable statutes. Further, it serves as an account of the Committee's proactive approach to Board of Health governance, performance, and accountability.

At its meeting on January 20, 2022, the Board of Health approved the Governance Committee Terms of Reference, which is reviewed every two (2) years. The Reporting Calendar (Appendix B) is reviewed and approved annually.

Amendments to the Reporting Calendar

In 2021 the Governance Committee met five (5) times per year with additional meetings occurring as needed at the call of the Chair of the Committee. It is recommended that the Committee maintain this meeting schedule in 2022 to allow for new quarterly reporting of MLHU's Risk Management program and receive regular status updates on the Provisional Plan.

An additional change to the 2022 Reporting Calendar includes Board Orientation proceeding for the first half of the year, followed by a focus on Board Development during the second half of 2022.

Next Steps

The Governance Committee has the opportunity to review the appended Reporting Calendar and meeting schedule for 2022.

Once the Governance Committee is satisfied with its review, the Reporting Calendar will be forwarded to the Board of Health for approval.

This report was prepared by the Healthy Organization Division.

Emily Williams, BScN, RN, MBA, CHE
Chief Executive Officer

BUREAU DE SANTÉ DE MIDDLESEX-LONDON HEALTH UNIT
www.healthunit.com

GOVERNANCE COMMITTEE
TERMS OF REFERENCE

PURPOSE

The Governance Committee serves to provide an advisory and monitoring role. The committee's role is to assist and advise the Board of Health, the Medical Officer of Health (MOH) and Chief Executive Officer (CEO) in the administration and risk management of matters related to Board membership and recruitment, Board self-evaluation, and governance policy.

REPORTING RELATIONSHIP

The Governance Committee reports to the Board of Health of the Middlesex-London Health Unit. The Chair of the Governance Committee, with the assistance of MOH and CEO, will make reports to the Board of Health following each of the meetings of the Governance Committee.

MEMBERSHIP

The membership of the Governance Committee will consist of a total of five (5) voting members. The members will include the Chair and Vice-Chair of the Board of Health and in total, the membership will contain at least one Middlesex County Board member, one City of London Board member and two provincial Board members.

The Secretary and Treasurer will be ex-officio non-voting members.

Staff support includes:

- CEO;
- Manager, Strategy, Risk and Privacy; and
- Executive Assistant (EA) to the Board of Health and/or EA to the MOH.

Other Board of Health members may attend the Governance Committee but are not able to vote.

CHAIR

The Governance Committee will elect a Chair at the first meeting of the year to serve for a one or two-year term. The Chair may be appointed for additional terms following the completion of an appointment to enhance continuity of the Committee.

TERM OF OFFICE

At the first Board of Health meeting of the year the Board will review the Governance Committee membership. At that time, if any new appointments are required, the position(s) will be filled by majority vote. The appointment will be for at least one year, and where possible, staggered terms will be maintained to ensure a balance of new and continuing members. A member may serve on the Committee as long as they remain a Board of Health member.

DUTIES

The Governance Committee will seek the assistance of and consult with the MOH and CEO for the purposes of making recommendations to the Board of Health on the following matters:

1. Board member succession planning and recruitment;
2. Orientation and continuing education of Board members;

BUREAU DE SANTÉ DE MIDDLESEX-LONDON HEALTH UNIT
www.healthunit.com

3. Assessment and enhancement of Board and Board committee performance;
4. Performance indicators that are reported to the Board;
5. Compliance with the Board of Health Code of Conduct;
6. Performance evaluation of the MOH and CEO;
7. Governance policy and by-law development and review;
8. Compliance with the Ontario Public Health Standards;
9. Strategic planning;
10. Privacy program;
11. Risk management;
12. Human resources strategy and workforce planning; and
13. Occupational health and safety.

FREQUENCY OF MEETINGS

The Governance Committee will meet five (5) times per year or at the call of the Chair of the Committee.

AGENDA & MINUTES

1. The Chair of the committee, with input from the MOH and CEO, will prepare agendas for regular meetings of the committee.
2. Additional items may be added at the meeting if necessary.
3. The recorder is the EA to the Board of Health or the EA to the MOH.
4. Agenda and minutes will be made available at least five (5) days prior to meetings.
5. Agenda and meeting minutes are provided to all Board of Health members.

BYLAWS:

As per Section 19.1 of Board of Health By-Law No. 3, the rules governing the proceedings of the Board shall be observed in the Committees insofar as applicable. This will include rules related to conducting of meetings; decision making; quorum and self-evaluation.

REVIEW

The terms of reference will be reviewed every two (2) years.

BUREAU DE SANTÉ DE MIDDLESEX-LONDON HEALTH UNIT
www.healthunit.com

2022 Governance Committee Reporting Calendar

Q1 (Jan 1 to Mar 31)	Q2 (Apr 1 to Jun 30)
Meeting: February	**Meetings: April & June**
• Approve Reporting Calendar • Initiate Terms of Reference Review (every two years) • Annual Declarations – Confidentiality and Conflict of Interest • Initiate Board of Health Orientation • Report on Privacy Program • Report on Provisional/Strategic Plan and Performance • Report on Board of Health Risk Management • Review Governance By-laws and Policies	• Initiate Medical Officer of Health and Chief Executive Officer Performance Appraisal • Initiate Board of Health Self-Assessment (every 2 years) • Report on Board of Health Self-Assessment (every 2 years) • Complete Board of Health Orientation • Report on Occupational Health and Safety Program • Report on Provisional/Strategic Plan and Performance • Report on Board of Health Risk Management • Review Governance By-laws and Policies
Q3 (Jul 1 to Sep 30)	**Q4 (Oct 1 to Dec 31)**
Meeting: September	**Meeting: November**
• Initiate Board of Health Development • Report on Public Health Funding and Accountability Agreement Indicators • Report on Provisional/Strategic Plan and Performance • Report on Board of Health Risk Management • Review Governance By-laws and Policies	• Complete Board of Health Development • Report on Provisional/Strategic Plan and Performance • Report on Board of Health Risk Management • Review Governance By-laws and Policies

Annual Declarations

In accordance with Ontario privacy laws and the Ontario Public Health Standards, Board of Health members are accountable for maintaining the confidentiality and security of personal information, personal health information, and other confidential information that they gain access to for the purpose of discharging their duties and responsibilities as a member of the

Board. As such, Board members will sign an annual confidentiality attestation. (Refer to Policy G-100 Privacy and Freedom of Information and Policy.)

Board of Health members also have a duty to avoid conflicts of interest – situations where financial, professional or other personal considerations may compromise, or have the appearance of compromising, a Board member's judgment in carrying out his/her fiduciary duties as a Board of Health member. As such, Board members will sign an annual conflicts of interest declaration. (Refer to Policy G-380 Conflicts of Interest and Declaration.)

Board of Health Orientation and Development

In accordance with the Ontario Public Health Standards, the Board of Health must ensure that members are aware of their roles and responsibilities by ensuring the development and implementation of a comprehensive orientation plan for new board members and a continuing education and development program for all board members. (Refer to Policy G-370 Board of Health Orientation and Development.)

Board of Health Self-Assessment

In accordance with the Ontario Public Health Standards, the Board of Health must complete a self-assessment at least every other year and provide recommendations for improvements in Board effectiveness and engagement. (Refer to Policy G-300 Board of Health Self-Assessment.)

Governance By-laws and Policies

By-laws and policies establish the governing principles, practices and accountability frameworks for the Board of Health. The Ontario Public Health Standards set out by-laws and policies that must be in place for Board operation and require that these are reviewed at least every two years. (Refer to Policy G-000 By-laws, Policy and Procedures.)

Medical Officer of Health and Chief Executive Officer Performance Appraisals

The Medical Officer of Health and Chief Executive Officer (MOH and CEO) performance appraisals will be conducted annually with a report coming to the Governance Committee on the results. (Refer to Policy G-050 MOH and CEO Performance Appraisals.)

Occupational Health and Safety Program

The Board of Health has statutory duties in accordance with the *Occupational Health and Safety Act* to maintain a safe and healthy workplace. The Board shall be informed of all significant health and safety activities including employee incidents and investigations through an annual report summarizing the health and safety program. (Refer to Policy G-080 Occupational Health and Safety.)

BUREAU DE SANTÉ DE MIDDLESEX-LONDON HEALTH UNIT
www.healthunit.com

Privacy Program

The Board of Health must ensure there is a privacy program in place to monitor compliance with governance accountabilities and legislative requirements with respect to privacy and the confidentiality and security of personal information and personal health information. (Refer to Policy G-100 Information Privacy and Confidentiality.)

Public Health Funding and Accountability Agreement Indicators

The Public Health Funding and Accountability Agreements provide a framework for setting specific performance expectations and establishing data requirements to support monitoring of these performance expectations.

Reporting Calendar

The reporting calendar ensures the Committee's requirements to assist and advise the Board of Health on matters outlined in the Committee Terms of Reference. (Refer to Appendix A.)

Risk Management

The Ontario Public Health Standards require the Board of Health to have a formal risk management framework in place that identifies, assesses, and addresses risks. (Refer to Policy G-120 Risk Management.) In accordance with the Ontario Public Health Standards and the Public Health Funding and Accountability Agreement, the Board of Health will report to the ministry the high risks that are being managed by the Board.

Strategic Planning

The organization's strategic plan is developed in consultation with the Board of Health, staff, and other key stakeholders as appropriate, and is subject to final approval by the Board of Health. The strategic plan is reviewed annually by management and the Board of Health. (Refer to Policy G-010 Strategic Planning.)

Terms of Reference

The Governance Committee Terms of Reference set out the parameters for how authority is delegated to the Committee and how the Committee is accountable to the Board of Health. It is incumbent upon the Governance Committee to review the Terms of Reference every two years to ensure that components (purpose, reporting relationship, membership, chair, term of office, duties, frequency of meetings, agenda and minutes, by-laws and review) are still relevant to the needs of the committee. (Refer to Policy G-290 Standing and Ad Hoc Committees).

MIDDLESEX-LONDON HEALTH UNIT

REPORT NO. 02-22GC

TO: Chair and Members of the Governance Committee

FROM: Emily Williams, Chief Executive Officer

DATE: 2022 February 17

GOVERNANCE BY-LAW AND POLICY REVIEW

Recommendation

It is recommended that the Governance Committee recommend that the Board of Health:

1) Receive Report No. 02-22GC re: "Governance By-law and Policy Review" for information; and
2) Approve the governance policies appended to this report (Appendix B).

Key Points

- It is the responsibility of the Board of Health to review and approve governance by-laws and policies.
- Appendix A details recommended changes to the by-laws and policies that have been reviewed by the subcommittees of the Board and outlines the status of all documents contained within the Governance Manual.
- There are two (2) policies that have been prepared for review by the Governance Committee (Appendix B) and three (3) policies that are coming up for review in Q1 2022.

Background

In 2016, the Board of Health (BOH) approved a plan for review and development of by-laws and policies based on a model that incorporates best practices from the Ontario Public Health Standards and advice obtained through legal counsel. Refer to Report No. 018-16GC. The Governance Committee has been actively reviewing the overdue policies throughout the year and there were three (3) remaining policies identified for review by the end of 2021.

Policy Review

There are 2 (two) by-laws/policies included as Appendix B that have been prepared for approval by the Board of Health:

- G-000 Bylaws, Policy and Procedures
- G-100 Privacy and Freedom of Information

Appendix A to this report details the recommended changes for the above by-laws/policies as well as the status of all documents contained within the Governance Manual. There are three (3) policies that are coming up for review in Q1 2022.

Next Steps

It is recommended that the Board of Health approve the policies as outlined in Appendix B.

This report was prepared by the Manager, Strategy, Risk and Privacy, Healthy Organization Division.

Emily Williams, BScN, RN, MBA, CHE
Chief Executive Officer

Governance By-law and Policy Review Status and Recommendations

December 1, 2021

Document Name	Last Review	Status	Recommended Changes	For Review at Governance Committee Meeting
G-000 Bylaws, Policy and Procedures	17/06/2021	Reviewed	Replaced Appendix A with the approved review process for Governance Policies (Appendix A1) and Administrative Policies (Appendix A2).	February 17, 2022
G-010 Strategic Planning	17/06/2021	Current		
G-020 MOH/CEO Direction	02/27/2020	Current	To be circulated to the Governance Committee on March 1, 2022.	April 21, 2022
G-030 MOH and CEO Position Descriptions	10/16/2021	Current		
G-040 MOH/CEO Selection and Succession Planning	10/19/2017	On Hold Review Pending		
G-050 MOH and CEO Performance Appraisal	10/16/2021	Current		
G-080 Occupational Health and Safety	09/16/2021	Current		
G-100 Information Privacy and Confidentiality	03/21/2021	Reviewed	Minor changes highlighted in yellow.	February 17, 2022
G-120 Risk Management	10/16/2021	Current		
G-150 Complaints	04/15/2021	Current		
G-160 Jordan's Principle	17/06/2021	Current		

Document Name	Last Review	Status	Recommended Changes	For Review at Governance Committee Meeting
G-180 Financial Planning and Performance	11/18/2021	Current		
G-190 Asset Protection	11/18/2021	Current		
G-200 Approval and Signing Authority	11/18/2021	Current		
G-205 Borrowing	04/15/2021	Current		
G-210 Investing	11/18/2021	Current		
G-220 Contractual Services	12/09/2021	Current		
G-230 Procurement	12/09/2021	Current	Recommendation from the Board of Health meeting on December 9, 2021: Staff review this policy in parallel with the administrative Policy 4-140 Approval and Signing Authority by March 31, 2022. Appendix A – all references to Director, Healthy Organization has been replaced with CEO and separation of roles highlighted.	
G-240 Tangible Capital Assets	11/18/2021	Current		
G-250 Reserve and Reserve Funds	12/09/2021	Current		
G-260 Governance Principles and Board Accountability	04/15/2021	Current		
G-270 Roles and Responsibilities of Individual Board Members	01/20/2022	Current	This policy was amended and approved at the Board of Health meeting on January 20, 2022.	

Document Name	Last Review	Status	Recommended Changes	For Review at Governance Committee Meeting
G-280 Board Size and Composition	10/16/2021	Current		
G-290 Standing and Ad Hoc Committees	02/27/2020	Current	To be circulated to the Governance Committee on March 1, 2022.	April 21, 2022
G-300 Board of Health Self-Assessment	10/16/2021	Current		
G-310 Corporate Sponsorship	11/18/2021	Current		
G-320 Donations	11/18/2021	Current		
G-330 Gifts and Honoraria	11/18/2021	Current		
G-340 Whistleblowing	06/18/2020	Current		
G-350 Nominations and Appointments to the Board of Health	10/16/2021	Current		
G-360 Resignation and Removal of Board Members	09/16/2021	Current		
G-370 Board of Health Orientation and Development	10/16/2021	Current		
G-380 Conflicts of Interest and Declaration	02/27/2020	Current	To be circulated to the Governance Committee on March 1, 2022.	April 21, 2022
G-400 Political Activities	06/17/2021	Current		
G-410 Board Member Remuneration and Expenses	10/16/2021	Current		

Document Name	Last Review	Status	Recommended Changes	For Review at Governance Committee Meeting
G-430 Informing of Financial Obligations	04/15/2021	Current		
G-470 Annual Report	10/16/2021	Current		
G-480 Media Relations	10/16/2021	Current		
G-490 Board of Health Reports	10/16/2021	Current		
G-B10 By-law No. 1 Management of Property	10/16/2021	Current		
G-B20 By-law No. 2 Banking and Finance	10/16/2021	Current		
G-B30 By-law No. 3 Proceedings of the Board of Health	01/20/2022	Current	This by-law was amended and approved at the Board of Health meeting on January 20, 2022.	
G-B40 By-law No. 4 Duties of the Auditor	10/16/2021	Current		

BUREAU DE SANTÉ DE MIDDLESEX-LONDON HEALTH UNIT
www.healthunit.com

Policy G-000

BY-LAWS, POLICY AND PROCEDURES

PURPOSE

The Middlesex-London Health Unit (MHLU) is committed to providing a consistent approach to effective, open, and supportive systems of governance and management. The purpose of this policy is to outline the process for the development and review of the policies contained within the Health Unit's Governance and Administration Manual.

POLICY

All by-laws and policies at the Middlesex-London Health Unit must:

- Reflect the goals and values of MLHU and the Board of Health;
- Comply with relevant legislation and regulations;
- Be specific and clearly worded;
- Be relevant to the current and future needs of the MLHU and the Board of Health;
- Follow the prescribed ~~development and~~ review process (Appendix A);
- Be published according to MLHU policy standards (Appendix B); and
- Undergo annual/biannual review.

PROCEDURE

Middlesex-London Health Unit Governance and Administration Manual shall include:

Governance By-laws and Policies

The Board of Health is responsible for the Health Unit's governance by-laws and policies. These represent the principles that set the direction, limitations and accountability frameworks for MLHU. Governance by-laws relate to management of property, banking and finance, proceedings of the Board of Health, and duties of the auditor. Governance policies relate to strategic direction, leadership and Board management, program quality and effectiveness, financial and organizational accountability, Board effectiveness, and communications and external relations.

Administrative Policies & Procedures

The Senior Leadership Team is responsible for the Health Unit's administrative policies. These policies align the procedures for managing MLHU and establish efficiency, consistency, responsibility, and accountability. Administrative policies relate to general administration, property, finance, human resources, records and privacy, information technology, health and safety, and communications.

Policy	Brief statement(s) that clearly set out Board of Health and/or Health Unit principles and rules with respect to a particular matter to provide the organization with a specific direction.
Procedure	Clear, high-level description of responsibilities and steps to implement the policy. Separate from program guidelines, plans and/or manuals. Note: often legislation will require the employer to create both a policy and a program to address a specific issue (e.g., fit testing). Program details are best outlined separate from written policy and made available to staff on the intranet or in standards, protocols or guidelines.

Standards, Protocols and Guidelines

Where the policy and/or procedure does not provide sufficient detail to be operationalized across the organization, division or team standards, protocols and guidelines may be developed to ensure that the policy and/or procedure is enacted and practiced across the organization. The Middlesex-London Health Unit Governance and Administration Manual does not include standards, protocols or guidelines that further operationalize policies and procedures at the divisional or team level. These are developed at the sole discretion of Directors and Program Managers who are responsible for the standards, guidelines and protocols that apply specifically to the work of their divisions and team. These must align with all established administrative policies, procedures, standards, protocols and guidelines.

Standards	Establishes the acceptable level of quality with quantifiable low-level mandatory controls.
Protocols	A step by step descriptive guideline to achieve completion of a task and is to be followed in letter and spirit in all circumstances.
Guidelines	Provide additional recommended guidance to implement programs and services or to adhere to administrative policies and procedures.

Medical Directives

The Middlesex-London Health Unit Governance and Administration Manual does not include medical directives which apply to a specific patient population who meet specific criteria. A medical directive is role-specific (e.g., Nurse Practitioner, Registered Dietician, Registered Nurse), not person-specific and users within the role must possess the necessary knowledge, skills, and judgment before implementing a medical directive. Specifically, a directive:

- Is given in advance to enable an implementer to act under specific conditions without a direct assessment by the physician. Implementers are not ordering a procedure when they implement a directive; rather they are implementing a physician's order.
- Must have the integrity of a direct order, thus physicians potentially responsible for the order must approve it.
- Is approved only when all affected regulated professionals and relevant administrators participate in their development.
- Is always written and has essential components.

Policy Development

Governance policy development can be initiated by the Board of Health. The Senior Leadership Team may also provide recommendations regarding governance policies to the Board of Health for consideration.

Administrative policy development can be initiated by the Medical Officer of Health, ChiefExecutive Officer and/or the Senior Leadership Team. Additionally, an administrative policy development and revision form (Appendix C) can be submitted by a member of the Management Leadership Team for consideration and direction from the Senior Leadership Team.

For both governance and administrative policy development, the Senior Leadership Team will determine the assignment of responsibility for development of the policy, the consultation process and timelines. The consultation and development process will include input from the Manager of Strategy, Risk and Privacy, the policy sponsor(s), content expert(s) and additional stakeholders, as required.

Standard, protocol and guideline development can be initiated in response to a specific need. It is recommended that standards, protocols and guidelines align with administrative policies and serve as appendices to organization-wide policies rather than stand-alone documents.

Policy Review

Policies contained within the Administration Manual will be reviewed at a minimum of every two years (biannually) or as needed, based on changing legislation or organizational needs.

The Manager of Strategy, Risk and Privacy is responsible for the biannual review and will coordinate policy workgroups (where appropriate) to ensure that review of each policy occurs according to this cycle.

Review and revision of governance policies can be initiated at any time by the Board of Health or, as recommended to the Board of Health by the Senior Leadership Team.

Administrative policy review and revision can also be initiated at any time by a member of the Senior Leadership Team or the Management Leadership Team. Review and revision from the Management Leadership Team should be submitted through a policy development and revision form (Appendix C) to the Manager of Strategy, Risk and Privacy who will then submit it to the Senior Leadership Team.

For both governance and administrative policy development, the Senior Leadership Team will determine the assignment of responsibility for development of the policy, the consultation process and timelines. The consultation and development process will include input from the Manager of Strategy, Risk and Privacy, the policy sponsor(s), content expert(s) and additional stakeholders, as required.

All changes to policy should be tracked in the development and revision form (Appendix C) to streamline consideration and approval.

The most recent review date will be listed on each policy in addition to the original implementation date. Each revision date is listed after the previous revision date(s).

Policy Approval

Governance policies can only be approved by the Board of Health. New or revised policies will be ratified by the signature of the current Board of Health Chair.

The Senior Leadership Team will approve all new or revised administrative policies that pertain to the operational management of the Health Unit, except where Board of Health approval is also required. New or revised policies will be ratified by signature of the Medical Officer of Health and Chief Executive Officer.

Standards, protocols and guidelines will be approved and ratified by signature of Divisional Directors and are to be reviewed regularly for alignment with organizational policies.

Policy Distribution and Retention

The Manager of Strategy, Risk and Privacy is responsible for ensuring the Governance and Administration Manuals are managed and accessible in an automated policy management software program. All new policies and revisions are communicated to staff.

Withdrawn Policies

The Manager of Strategy, Risk and Privacy, in consultation with sponsors and/or content experts will recommend policies to be withdrawn from the agency manual to the appropriate approval body. The Manager of Strategy, Risk and Privacy will maintain a copy of withdrawn policies including their withdrawal date, the reason for withdrawal, and the appropriate signature.

Governance and Administrative Policy Manual Archiving

The Manager of Strategy, Risk and Privacy will ensure that each change to the policy manuals are tracked and that copies of each revision are kept to protect against potential future litigation.

The process for managing policies (e.g. distribution, policy withdraws, and archiving) can be found in Appendix D.

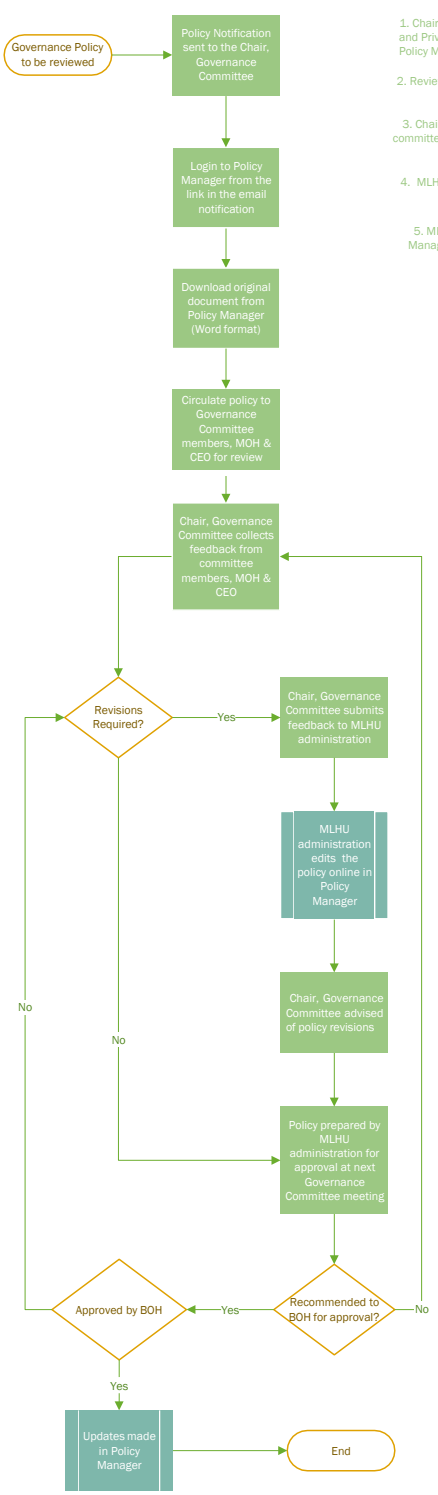
APPENDICES

Appendix A1 – Governance Policy Review and Approval Process
Appendix A2 – Administrative Policy Development, Review and Approval Process
Appendix B – Policy Development and Review Checklist
Appendix C – Development and Revision Form
Appendix D – Management of Policies in PolicyManager

APPLICABLE LEGISLATION AND STANDARDS

Health Protection and Promotion Act, R.S.O. 1990, c. H.7
Ontario Public Health Organizational Standards

APPENDIX A1
To Policy G-000



Notes

1. Chair, Governance Committee and Manager, Strategy, Risk and Privacy assigned to the "Governance Committee" team in Policy Manager and designated as a reviewer.

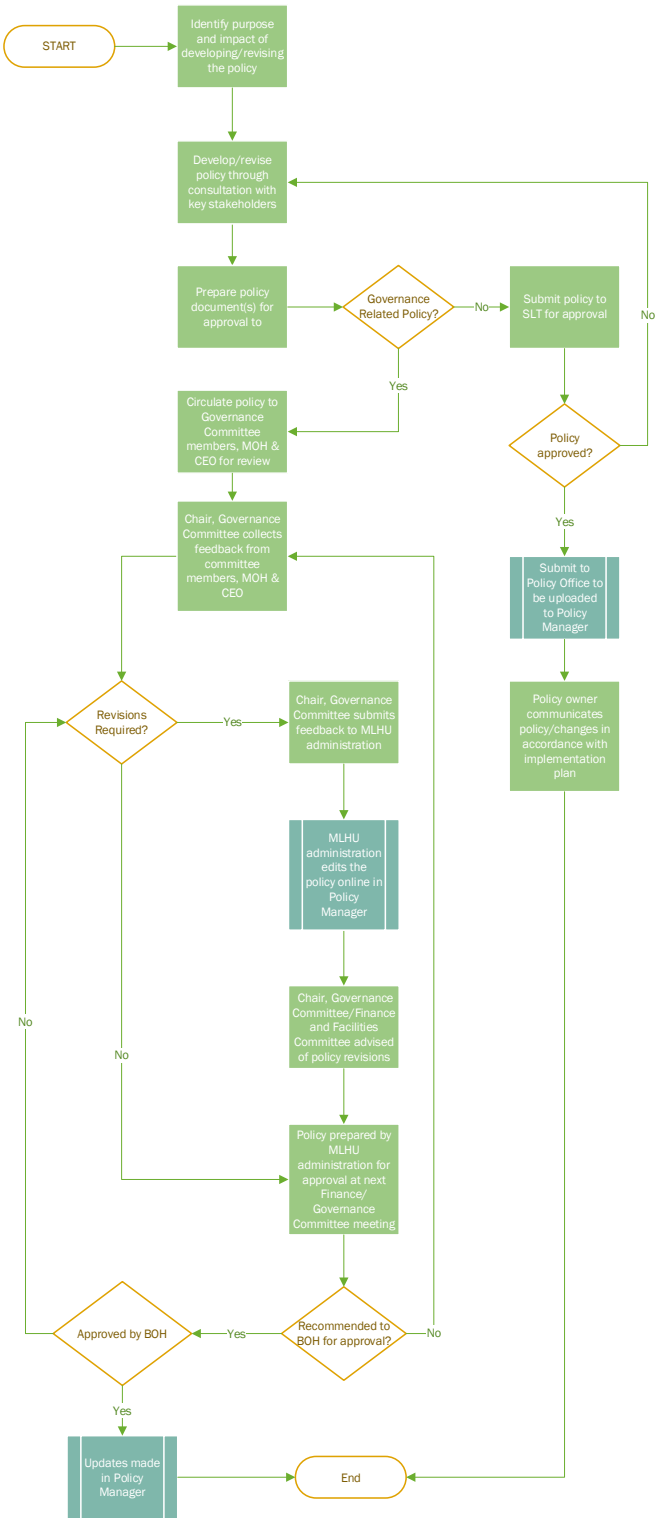
2. Reviewers receive notifications when policies are due for review on the 25th of every month.

3. Chair, Governance Committee will circulate the policy to other committee members via email and collect feedback by the 1st of the month.

4. MLHU administration includes the Manager, Strategy, Risk and Privacy.

5. MLHU administration is responsible for the edits in Policy Manager and oversees the publishing of all approved policies.

APPENDIX A2
To Policy G-000



APPENDIX B
To Policy G-000

POLICY DEVELOPMENT AND REVIEW CHECKLIST

Purpose

1. Do all review members understand the policy goal?
2. Is it clear to whom and what the policy applies?
3. Will the policy be uniformly applied and enforced in all Service Areas?
    a. If not, ensure Service Area identifies how it will be applied and/or enforced.

Risk, Best-Practice and Impact

1. If appropriate, have policies from other Boards of Health been examined for comparison?
    a. If yes, list the Boards of Health that were examined.
2. If appropriate, have policies from similar institutions been examined for comparison?
    a. If yes, list the institutions that were examined.
3. If appropriate, has applicable legislation been identified and reviewed to ensure adherence?
    a. Ensure applicable legislation is identified in policy.
4. Have proposed major practice changes been reported to and/or discussed with stakeholders so that they are aware of the implications of any potential change?
    a. If yes, does this policy affect the organization's reporting, service delivery or planning cycles?
    b. If yes, list stakeholders that were engaged.
5. Are the responsibilities under this policy assigned to a person(s), in a way that is compatible with organizational roles?

Alignment

1. Does the document align with the Middlesex-London Health Unit Vision, Mission and Values?
2. Does the document align with the Middlesex-London Health Unit Code of Conduct?
3. Is there another policy with the same or a similar intent?
    a. If yes, can these be integrated?
    b. If yes, are appropriate references included to related policies?
    c. If yes, is it clear when each policy will apply?

Implementation

1. Will there be any training or professional development requirements associated with the development, implementation or monitoring of this policy?
    a. If yes, ensure these are explicit in the policy?
2. Is there a defined implementation date (the date the policy comes into force)?
3. Is there a unique proposed review date?

Structure & Appropriateness

1. Does the document follow our policy template?
2. Do all logos and/or images follow our graphics standards?
3. Has appropriate formatting been used (e.g., bullets, numbered-lists, headings, etc.)
4. Is the “purpose” section clearly distinct from the “policy” section?
5. Have all procedures been separated from the “policy” section?
6. Does the document consider diversity, accessibility or equal opportunity?
7. Does the document employ gender-neutral and inclusive language?
8. Have all references in the draft policy been verified as accurate and current?

Clarity

1. Are key terms (and any new terms) adequately defined?
2. Is terminology consistent across all documents?
3. Is the policy written in a manner that can be understood by a wide audience (i.e., plain language)?

IMPLEMENTATION CHECKLIST

Administrative Manual

1. Approved document(s) sent to Policy Office with the Policy Development and Revision form (Appendix C).
2. Approved policy document(s) uploaded to Policy Management software (“Policy Manager”).

Implementation

1. Develop plan to inform all staff of the relevant policy changes (refer to Appendix C)

APPENDIX C
To Policy G-000

POLICY DEVELOPMENT AND REVISION FORM

Review Type:		Indicate if this is a new by-law/policy or under revision.
Title:		Indicate the title of the document
Section:		List the section that best applies.
Sponsor:		Person responsible for the by-law or policy. Mandatory for all documents.
Policy Owner:		Identify the person responsiblefor the by-law or policy.
Associated Documents:		Enter all associated documents.
Keywords:		Enter 10 keywords for ease of searching.

Purpose

Issue or need tobe addressed:	•	State the problem, issue or need that the by-law or policyis intended to address. Does this by-law or policy applyto a specific division, program, collective agreement, etc.?
Consultation Plan & Stakeholder List:	•	Stakeholders to be consulted –list name and title; If Committees/Groups: list name of committee, group, department, etc.
Summary of Changes:	•	To be completed before approval. Provide a summary of all changes made.

Implementation

How will staff be made aware of the policy and/or changes:	•	Consider communication plan and whether it will include All Staff email, presentation to MLT, presentation at town hall, etc.
What requirements are in place for staff:	•	Detail any specific instructions to be followed before or after the policy comes into effect.

APPENDIX C1
To Policy G-000

SAMPLE POLICY UPDATE EMAIL COMMUNICATION

Please be advised of the following policy update from _____:

Note: *If you are not already logged into PolicyManager, you will be prompted to log in when you select the links below. As soon as you log in, using the same user name and password you use to log into your computer, you will be redirected to the policy or appendix. There are no attestations to complete for this update.*

Policy	***Summary of Key Changes***	***Effective Date***	***Audience***	***Requirements***	***Policy Lead(s)***	***Policy Manager Link***

For further information regarding MLHU Administrative Policies or supplemental resources, please visit PolicyManager.

For additional questions or feedback, please discuss with your leader and feel free to email policy@mlhu.on.ca.

APPENDIX D
To Policy G-000

MANAGEMENT OF POLICIES IN POLICYMANAGER

All governance policies are managed electronically in an automated policy management software program called PolicyManager. By maintaining the policies electronically, it is not necessary to keep a hard copy of the Governance Policy Manual. PolicyManager also provides version control and archiving abilities.

Governance policies can be accessed without a log in by Board of Health members as well as the public through the Middlesex-London Health Unit (MLHU) website. There is a direct link to PolicyManager located on the website under the Board of Health section. Employees of MLHU may use the website or can log into PolicyManager to see the Governance Policy Manual.

Adding a new policy

1. After approval by the Board of Health, the new policy is emailed to the Program Administrative Assistant (PA) for Strategic Projects, Privacy, Risk and Governance who is also a System Administrator for PolicyManager.
2. The policy is uploaded to PolicyManager with appropriate meta data to ensure that the program is able to notify the PA when the policy is next ready for review.
3. The policy is then published to PolicyManager by the PA and can be viewed by everyone.

Replacing a current policy with a revised policy

1. After approval by the Board of Health, the revised policy is emailed to the Program Administrative Assistant (PA) for Strategic Projects, Privacy, Risk and Governance who is also a System Administrator for PolicyManager.
2. The PA opens the current policy in PolicyManager and replaces it with the revised policy and ensures the meta data is updated.
3. The policy is automatically published to PolicyManager and becomes available to everyone.
4. All previous versions of the policy are saved in PolicyManager.

Retiring a policy

1. After approval by the Board of Health, the retired policy is emailed to the Program Administrative Assistant (PA) for Strategic Projects, Privacy, Risk and Governance who is also a System Administrator for PolicyManager.
2. The PA opens the current policy in PolicyManager and selects it to be retired. At this time a note may be added describing the reason the policy is being retired.
3. Once a policy is retired, all circulations and internal links associated with the policy will be removed.
4. The retired policies will be displayed within a specific area in PolicyManager called Retired Documents.
5. Policies may also be unretired at any time.

BUREAU DE SANTÉ DE MIDDLESEX-LONDON HEALTH UNIT
www.healthunit.com

Policy G-100

PRIVACY AND FREEDOM OF INFORMATION

PURPOSE

To facilitate the Board of Health's (Board) compliance with governance accountabilities and legislative requirements with respect to privacy and freedom of information.

To outline the confidentiality obligations of Board members.

POLICY

The Board recognizes its legal and ethical obligation to protect the privacy of individuals with respect to their personal information (PI) and personal health information (PHI), and is committed to ensuring the confidentiality and security of the PI and PHI under the custody and control of the Middlesex-London Health Unit (MLHU), as set out in the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act* (PHIPA).

The Board further recognizes its obligation to provide a right of access to information under its control, as set out in MFIPPA, and is committed to openness, transparency and accountability.

Board members are further accountable for maintaining the confidentiality and security of PI, PHI and other confidential information that they gain access to for the purpose of discharging their duties and responsibilities as a member of the Board.

The Board shall be informed of all significant privacy risks and significant privacy breaches.

PROCEDURE

1. Board of Health Accountabilities Under MFIPPA

1.1. The Board designates from among its members the Board Chair to serve as the "head" of the institution for the purposes of meeting the requirements outlined in this Act (s. 3).

1.2. The Board Chair delegates the duties and responsibilities of the head to the Chief Executive Officer (CEO). Appendix A describes duties and powers of the head with respect to freedom of information and protection of individual privacy. The day-to-day administration and management of MLHU's privacy program will be operationalized by MLHU's Privacy Officer, who reports to the CEO.

1.3. The Board Chair maintains authority to delegate responsibility to external counsel to advise and/or respond to access requests filed under MFIPPA and/or PHIPA.

2. Board of Health Accountabilities Under PHIPA

2.1. The Medical Officer of Health of a Board of Health within the meaning of the Health Protection and Promotion Act serves as the health information custodian (HIC) for the purposes of PHIPA (s. 3 (1)).

2.2. In accordance with the requirements set out in the Ontario Public Health Standards, the Board of Health shall ensure that the Medical Officer of Health, as the designated HIC, maintains information systems and implements policies/procedures for privacy and security, data collection and records management. Appendix B describes required practices to protect PHI.

3. Board of Health Member Confidentiality Attestation

3.1. Board members shall confirm understanding of their confidentiality obligations under applicable privacy legislation and governance policies, and their agreement to honour these obligations, by signing an Annual Confidentiality Attestation (Appendix C).

New Board members shall provide initial attestation upon orientation to the Board and according to the annual schedule thereafter.

DEFINITIONS

"**Agents**", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated (PHIPA s. 2).

"**Collection**" means to gather, acquire, receive or obtain the information by any means from any source.

"**Confidentiality**" means the nondisclosure of PI or PHI except to another authorized person or where disclosure is permitted by law. Confidentiality also refers to the ethical and fiduciary duty and obligation of individual Board members to safeguard confidential information.

"**Confidential Information**" means personal information, personal health information and/or information regarding the organization which is not publicly disclosed by the organization, this information may include, but is not limited to:

- Matters including personal information and personal health information;
- Personnel matters relating to an employee of the health unit;
- The security of the property of the Board of Health;
- Proposed or pending acquisition of land, assets, or services for Board of Health purposes;
- Labour relations or employee negotiations;
- Litigation or potential litigation, including matters before administrative tribunals, affecting the Board;
- Advice that is subject to solicitor-client privilege, including communications necessary for that purpose;
- Matters related to other Acts that may be closed for discussion by the Board of Health;
- Matters that relate to requests under the Personal Health Information Protection Act or the Municipal Freedom of Information and Protection of Privacy Act.

"**Disclosure**" means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information.

"**Head**" means the individual designated, in writing, by the Board from among themselves, to act as head of the institution for the purposes of MFIPPA.

"**Health Information Custodian**" means a person or organization as defined and described in PHIPA who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties.

"**Identifying Information**" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual (PHIPA s. 4 (2)).

"**Institution**" means a board of health (MFIPPA, s. 2 (1)).

"**Personal Health Information**" means 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 Home Care and Community Services Act, 1994 for the individual;
(d) Relates to payments or eligibility for health care, or eligibility for coverage 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;
(f) Is the individual's health number; and/or
(g) Identifies an individual's substitute decision-maker. (PHIPA, s. 4 (1))

"**Personal Information**" means recorded information about an identifiable individual, 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 if 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/or
(h) The individual's name if 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. (MFIPPA, s. 2(1))

"**Privacy**" means the qualified right of individuals to exercise control over the collection, use and disclosure of their personal information and personal health information, unless the collection, use and/or disclosure of the information is permitted or required by law.

"**Privacy Breach**" means the theft, loss unauthorized use or disclosure of personal information, personal health information or other confidential information.

"**Privacy Officer**" means the individual designated by the Chief Executive Officer to administer and manage MLHU's privacy program.

"**Records**" means any record of information in any form or in any medium, whether in oral, written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record (MFIPPA s. 2 and PHIPA, s. 2).

"**Security**" means a system of safeguards and precautions established to preserve confidentiality. These means may be legislative, administrative/procedural and/or technical.

"**Use**" means to view, handle or otherwise deal with the information.

APPENDICES

Appendix A – MFIPPA: Duties and Powers of the Head Related to Freedom of Information and Protection of Individual Privacy
Appendix B – PHIPA: Practices to Protect Personal Health Information
Appendix C – Annual Confidentiality Attestation

APPLICABLE LEGISLATION AND STANDARDS

Municipal Freedom of Information and Protection of Privacy Act
Personal Health Information Protection Act
Regulated Health Professions Act
Ontario Public Health Standards: Requirements for Programs, Services, and Accountability, 2018

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Duties and Powers of the Head Related to Freedom of Information and Protection of Individual Privacy

APPENDIX A
To Policy G-100

MFIPPA Section	Summary of Duties and Powers
Part I – Freedom of Information	
Right of access 4 (1)	4 (1) Every person has a right of access to a record or a part of a record in the custody or under the control of an institution unless, a) the record or the part of the record falls within one of the exemptions under sections 6 to 15; or b) the head is of the opinion on reasonable grounds that the request for access is frivolous or vexatious.
Severability of the record 4 (2)	4 (2) If an institution receives a request for access to a record that contains information that falls within one of the exemptions under sections 6 to 15 and the head of the institution is not of the opinion that the request is frivolous or vexatious, the head shall disclose as much of the record as can reasonably be severed without disclosing the information that falls under one of the exemptions. 1996, c. 1, Sched. K, s. 13.
Measures to ensure preservation of records 4.1	4.1 Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put into place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution. 2014, c. 13, Sched. 6, s. 3.
Obligation to disclose 5 (1)	5 (1) Despite any other provision of this Act, a head shall, as soon as practicable, disclose any record to the public or persons affected if the head has reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard to the public.
Notice 5 (2)	5 (2) Before disclosing a record under subsection (1), the head shall cause notice to be given to any person to whom the information in the record relates, if it is practicable to do so.
Part II – Protection of Individual Privacy	
Notice [of collection] to individual 29 (2) and (3)	29 (2) If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,

MFIPPA Section	Summary of Duties and Powers
	(a) the legal authority for the collection; (b) the principal purpose or purposes for which the personal information is intended to be used; and (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection. R.S.O. 1990, c. M.56, s. 29 (2). Exception (3) Subsection (2) does not apply if, a) the head may refuse to disclose the personal information under subsection 8 (1) or (2) (law enforcement), section 8.1 (Civil Remedies Act, 2001) or section 8.2 (Prohibiting Profiting from Recounting Crimes Act, 2002); b) the Minister waives the notice; or c) the regulations provide that the notice is not required. R.S.O. 1990, c. M.56, s. 29 (3); 2001, c. 28, s. 23 (3); 2002, c. 2, ss. 16 (3), 19 (10); 2007, c. 13, s. 45 (3).
Right of access to personal information 36 (1) and 38	36 (1) Every individual has a right of access to, (a) any personal information about the individual contained in a personal information bank in the custody or under the control of an institution; and (b) any other personal information about the individual in the custody or under the control of an institution with respect to which the individual is able to provide sufficiently specific information to render it reasonably retrievable by the institution. 38 A head may refuse to disclose to the individual to whom the information relates personal information, if the record or the part of the record falls within one of the exemptions under section 38.

Personal Health Information Protection Act (PHIPA)
Health Information Custodian Practices to Protect Personal Health Information

APPENDIX B
To Policy G-100

PHIPA Section	Requirement
Information practices 10 (1), (2) and (3)	10 (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations. 2004, c. 3, Sched. A, s. 10 (1). (2) A health information custodian shall comply with its information practices. 2004, c. 3, Sched. A, s. 10 (2). (3) A health information custodian that uses electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any. 2004, c. 3, Sched. A, s. 10 (3).
Collection 11.1	11.1 A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information is not collected without authority. 2016, c. 6, Sched. 1, s. 1 (3).
Security 12 (1)	12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).
Notice of theft, loss, etc. 12 (2) and (3)	Notice to individual 12 (2) Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall, (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI. 2016, c. 6, Sched. 1, s. 1 (4). Notice to Commissioner (3) If the circumstances surrounding a theft, loss or unauthorized use or disclosure referred to in subsection (2) meet the prescribed requirements, the health information custodian shall notify the Commissioner of the theft or loss or of the unauthorized use or disclosure. 2016, c. 6, Sched. 1, s. 1 (4).

Handling of records 13 (1)	13 (1) A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any. 2004, c. 3, Sched. A, s. 13 (1).
Contact person 15 (1) and (3)	15 (1) A health information custodian that is a natural person may designate a contact person described in subsection (3). 2004, c. 3, Sched. A, s. 15 (1). (3) A contact person is an agent of the health information custodian and is authorized on behalf of the custodian to, (a) facilitate the custodian's compliance with this Act; (b) ensure that all agents of the custodian are appropriately informed of their duties under this Act; (c) respond to inquiries from the public about the custodian's information practices; (d) respond to requests of an individual for access to or correction of a record of personal health information about the individual that is in the custody or under the control of the custodian; and (e) receive complaints from the public about the custodian's alleged contravention of this Act or its regulations. 2004, c. 3, Sched. A, s. 15 (3).
Written public statement 16 (1) and (2)	16 (1) A health information custodian shall, in a manner that is practical in the circumstances, make available to the public a written statement that, (a) provides a general description of the custodian's information practices; (b) describes how to contact, i. the contact person described in subsection 15 (3), if the custodian has one, or ii. the custodian, if the custodian does not have that contact person; (c) describes how an individual may obtain access to or request correction of a record of personal health information about the individual that is in the custody or control of the custodian; and (d) describes how to make a complaint to the custodian and to the Commissioner under this Act. 2004, c. 3, Sched. A, s. 16 (1). (2) If a health information custodian uses or discloses personal health information about an individual, without the individual's consent, in a manner that is outside the scope of the custodian's description of its information practices under clause (1) (a), the custodian shall, (a) inform the individual of the uses and disclosures at the first reasonable opportunity unless, under section 52, the individual does not have a right of access to a record of the information; (b) make a note of the uses and disclosures; and

	(c) keep the note as part of the records of personal health information about the individual that it has in its custody or under its control or in a form that is linked to those records. 2004, c. 3, Sched. A, s. 16 (2).
Agents and information 17 (1) and (3)	17 (1) A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if, (a) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be; (b) the collection, use, disclosure, retention or disposal of the information, as the case may be, is necessary in the course of the agent's duties and is not contrary to this Act or another law; and (c) the prescribed requirements, if any, are met. 2004, c. 3, Sched. A, s. 17 (1); 2016, c. 6, Sched. 1, s. 1 (5). (3) A health information custodian shall, (a) take steps that are reasonable in the circumstances to ensure that no agent of the custodian collects, uses, discloses, retains or disposes of personal health information unless it is in accordance with subsection (2); and (b) remain responsible for any personal health information that is collected, used, disclosed, retained or disposed of by the custodian's agents, regardless of whether or not the collection, use, disclosure, retention or disposal was carried out in accordance with subsection (2). 2016, c. 6, Sched. 1, s. 1 (7).
Notice to governing College 17.1 (2)	17.1 (2) Subject to any exceptions and additional requirements, if any, that are prescribed, if a health information custodian employs a health care practitioner who is a member of a College, the health information custodian shall give written notice of any of the following events to the College within 30 days of the event occurring: 1. The employee is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee. 2. The employee resigns and the health information custodian has reasonable grounds to believe that the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee. 2016, c. 6, Sched. 1, s. 1 (8)

ANNUAL CONFIDENTIALITY ATTESTATION
BOARD OF HEALTH MEMBERS

APPENDIX C
To Policy G-100

I,

_____,

Printed Name of Board Member

understand that as a member of the Board of Health for the Middlesex-London Health Unit (MLHU), I may have access to:

- Confidential information (as defined within Policy G-100)
- Personal information (PI) (as defined by MFIPPA)
- Personal health information (PHI) (as defined by PHIPA)

This information could be related to MLHU clients and their families; MLHU employees, students and volunteers; members of my own family, friends or associates; and/or MLHU business, financial and management matters.

I understand that I will only be provided access to such information for the purpose of discharging my duties and responsibilities as a member of the Board of Health. Therefore, due to the highly sensitive nature of this information, I will:

1. Safeguard all confidential information including, but not limited to, PI and PHI, from unauthorized access, use or disclosure in accordance with Policy G-100.
2. Not collect, use or disclose any confidential information including, but not limited to, PI and PHI, without authorization; nor will I discuss, divulge, or disclose such information to others, unless it is necessary to fulfill my duties and responsibilities. Specifically, I will not:
    a) Reveal to anyone the name or identity of a client, employee, student or volunteer that is disclosed through information provided to me in the course of my duties.
    b) Repeat to anyone any statements or communications made by or about confidential MLHU business, financial or management matters, or about an MLHU client, client's family or associates.
    c) Reveal to anyone any information that I learn about an MLHU client, client's family or associates as a result of discussions with others providing care to the client, client's family or associates.
    d) Write, publish, or contribute to any articles, papers, stories or other written materials, or speak with members of the media with respect to information disclosed to me in the course of my duties as a member of the Board of Health, which has been deemed confidential by the Board of Health, Medical Officer of Health or Chief Executive Officer, or would be reasonable to consider confidential or sensitive given the type of information disclosed and the context in which such disclosure is made to the Board of Health, including without limitation, the names or identities of any client, client's family or associates who can be discerned, unless such disclosure is authorized by the Board of Health.
3. Obtain authorization from the Board Chair and/or the Secretary and Treasurer prior to disclosing any confidential information including, but not limited to, PI and PHI.

I have read this statement and understand my obligation to maintain confidentiality. I agree to honour that obligation during my term as a member of the Board of Health and thereafter. I understand that any contravention of the Board of Health/MLHU privacy and confidentiality policies could result in financial penalties, legal liability and other consequences and assessments as deemed appropriate or relevant which could be initiated by the MLHU, another governing body or otherwise.

Signature	Signature of Witness
Name (Please PRINT)	Name of Witness (Please PRINT)
Date	Date

DEFINITIONS

Confidential Information" means personal information, personal health information and/or information regarding the organization which is not publicly disclosed by the organization, this information may include, but is not limited to:

- Matters including personal information and personal health information;
- Personnel matters relating to an employee of the health unit;
- The security of the property of the Board of Health
- Proposed or pending acquisition of land, assets, or services for Board of Health purposes;
- Labour relations or employee negotiations;
- Litigation or potential litigation, including matters before administrative tribunals, affecting the Board;
- Advice that is subject to solicitor-client privilege, including communications necessary for that purpose;
- Matters related to other Acts that may be closed for discussion by the Board of Health
- Matters that relate to requests under the Personal Health Information Protection Act or the Municipal Freedom of Information and Protection of Privacy Act.

"**Personal Health Information**" means identifying information about an individual in oral or recorded form, if the information:

(h) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
(i) 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;
(j) Is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual;
(k) Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual;
(l) 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;
(m) Is the individual's health number; and/or
(n) Identifies an individual's substitute decision-maker. (PHIPA, s. 4 (1))

"**Personal Information**" means recorded information about an identifiable individual, including:

(i) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
(j) 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;
(k) Any identifying number, symbol or other particular assigned to the individual;
(l) The address, telephone number, fingerprints or blood type of the individual;
(m) The personal opinions or views of the individual except if they relate to another individual;
(n) 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;
(o) The views or opinions of another individual about the individual; and/or
(p) The individual's name if 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. (MFIPPA, s. 2(1))

MIDDLESEX-LONDON HEALTH UNIT

REPORT NO. 03-22GC

TO: Chair and Members of the Governance Committee

FROM: Emily Williams, CEO; Dr. Alexander Summers, Acting Medical Officer of Health

DATE: 2022 February 17

ANNUAL PRIVACY PROGRAM UPDATE

Recommendation

It is recommended that the Governance Committee recommend that the Board of Health receive Report No. 03-22GC re: "Annual Privacy Program Update" for information.

Key Points

- The Middlesex-London Health Unit (MLHU) has obligations under provincial privacy legislation to ensure the rights of individuals with respect to privacy, access and correction of records of their personal information and personal health information, as well as the right to access general records that pertain to MLHU operations and governance.
- MLHU's Privacy Program supports compliance with these obligations through education, policy and procedure development, assessment and management of privacy risks, facilitation of access and correction requests, and management of potential and actual breaches that may occur.
- MLHU completes annual statistical reporting to the Information and Privacy Commissioner of Ontario in accordance with requirements set out in the *Personal Health Information Protection Act (PHIPA), O. Reg. 329/04* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*.

Background

MLHU is a 'health information custodian (HIC)' in accordance with section 3 of the *Personal Health Information Protection Act (PHIPA)*, and an 'institution' in accordance with section 2 of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*. Under these legislation MLHU and the Middlesex-London Board of Health have obligations to ensure the rights of individuals with respect to privacy, access and correction of records of their personal information and personal health information, and access to general records that pertain to MLHU operations and governance.

MLHU Privacy Program

In accordance with Policy G-100 Privacy and Freedom of Information, the Medical Officer of Health (MOH) and Chief Executive Officer (CEO) have the delegated duties and powers of the head with respect to freedom of information and protection of individual privacy under MFIPPA. The MOH serves as the health information custodian (HIC) for the purposes of PHIPA (s. 3 (1)). Together, the MOH and CEO have the responsibility to maintain information systems and implement policies/procedures for privacy and security, data collection, and records management.

The day-to-day administration and management of MLHU's privacy program is operationalized by MLHU's Privacy Officer, and includes the following components:

- Education
- Policy development
- Privacy impact assessment and consultation
- Response to access and correction requests under PHIPA and MFIPPA

- Breach and complaint management

MLHU's Privacy Program is continually evolving in response to internal and external drivers, including, but not limited to, new legislation/regulations and case law, orders issued by the provincial and federal Privacy Commissioners, new technology, emerging best practices, and increasing awareness and expectations by the public with respect to privacy and access.

Successes over the past year include:

- MLHU staff are compliant in completing the annual online privacy education module implemented in 2021 to increase awareness and compliance with legislative requirements;
- Alignment of Privacy and Risk Management with the Strategy portfolio to support a consistent approach to effective, open and supportive systems of governance and management;
- Further assessment and mitigation of risks associated with new technologies and processes that support online collaboration and communication/information sharing among MLHU staff and with clients and external partners; and
- Completion of all formal written requests for access to records of personal information or personal health information or general records within the statutory time limits.

MLHU experienced a total of six (6) health information privacy breach incidents in 2021, none of which met the threshold for notification to the Information and Privacy Commissioner/Ontario (IPC). Corrective actions were taken following each incident to comply with legislative requirements under PHIPA and MFIPPA.

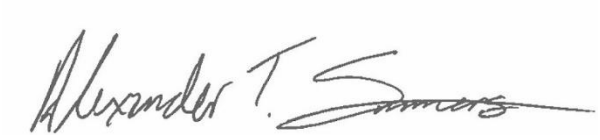
Provincial Oversight

MLHU is required to submit annual statistical reports to the IPC with respect to:

- Confirmed privacy breaches under PHIPA (attached as Appendix A);
- Access and correction requests under PHIPA (attached as Appendix B); and
- Access and correction requests under MFIPPA (attached as Appendix C).

All of these reports were submitted to the IPC within the required timelines.

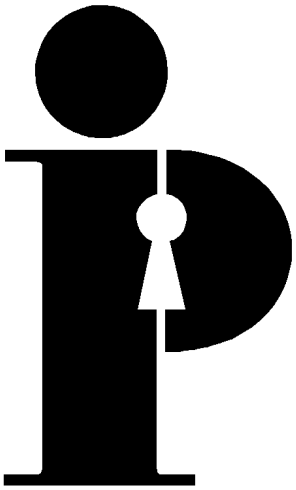
This report was prepared by the Manager, Strategy, Risk and Privacy, Healthy Organization Division.



Alexander Summers, MD, MPH, CCFP, FRCPC
Acting Medical Officer of Health

Emily Williams, BScN, RN, MBA, CHE
Chief Executive Officer

PHIPA BREACH STATISTICS



Statistical Report for the Information and Privacy Commissioner of Ontario

on

Personal Health Information Privacy Breaches

WORKBOOK AND COMPLETION GUIDE

Introduction

Use this Workbook and Guide as a "how to" tool to complete the annual report for the Information and Privacy Commissioner of Ontario (IPC) about privacy breach statistics, as required by section 6.4 of Ontario Regulation 329/04 made pursuant to the *Personal Health Information Protection Act, 2004* (*PHIPA*). We encourage you to use it to help you complete and submit your questionnaire online, especially if you are unfamiliar with it.

Health privacy breach statistics will be collected through the IPC's Online Statistics Submission Website from January to March 1 each year. For your convenience this Workbook and Guide is laid out in the same manner as the online questionnaire (section by section).

If there are any questions that have not been answered by this guide, there are two ways to receive additional information from the IPC:

- e-mail statistics.ipc@ipc.on.ca;
- call our main switchboard:
  Local calls 416 326-3333
  Long distance, use our toll-free line: 1-800-387-0073

Please note: Incomplete questionnaires may result in the custodian's submission being partly or entirely excluded from the statistics generated for the IPC's annual report.

Health information custodians are required to report statistics on health privacy breaches annually to the IPC**.**

If no privacy breaches under this Act occurred, **only health information custodians that are also institutions covered by the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) or the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) must still complete and submit Section 1.**

This workbook and guide is for your use in completing your questionnaire and should not be faxed or mailed to the Information and Privacy Commissioner in lieu of online submission. Faxed or mailed copies of this workbook and guide will NOT be accepted. Please submit your questionnaire online at: https://statistics.ipc.on.ca.

Note for coroners to whom Ontario Health provides personal health information that is accessible by means of the electronic health record: the requirement to submit a health privacy breach statistics report applies, with any necessary modification, to such coroners as if they were health information custodians.

Thank you for your co-operation!

SECTION 1: Identification

1.1 Please clearly indicate the name of the health information custodian, name of the contact person responsible for *PHIPA*, phone/fax numbers, mailing and e-mail addresses, name of the person to contact with any questions about the content of the report.

1.2 Are you a coroner to whom the prescribed organization provides personal health information under subsection 55.9.1 (1) of *PHIPA*?

☐ Yes. (If yes, please skip the next question)
☐ No. (If no, please continue)

1.3 Please indicate the type of health information custodian that is reporting. If the health information custodian is part of an institution under *FIPPA/MFIPPA* that has more than one type of health information custodian, please submit separate reports for each type of health information custodian.

1.4

☐	If your **health information custodian** experienced no privacy breaches**,** PLEASE STOP HERE AND SUBMIT ONLY SECTION 1 OF THE REPORT.
X	If your **health information custodian** experienced at least 1 privacy breach, PLEASE COMPLETE AND SUBMIT THE REST OF THE REPORT.

Background

Health information custodians are required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made pursuant to the *Personal Health Information Protection Act, 2004 Act,* as follows:

(1) On or before March 1 in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.

3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.
5. Personal health information was collected by the custodian by means of the electronic health record without authority. O. Reg. 224/17, s. 1; O. Reg. 534/20, s. 3 (1).

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner. O. Reg. 224/17, s. 1.

(3) A health information custodian that disclosed the information collected by means of the electronic health record without authority is not required to include this disclosure in its annual report. O. Reg. 534/20, s. 3 (2).

The remaining sections of the report ask for counts of privacy breaches that occurred in each of the above five categories. Do not count each incident more than once. If one incident includes more than one of the above categories, choose the one that best fits. For example, if an employee accessed personal health information without authority, and then disclosed the information, count that incident as either a use or a disclosure, but not both.

In completing the report, count a privacy breach in the year it was **discovered**, even if the breach occurred in a previous calendar year.

In this annual statistics report, you must include all thefts, losses, unauthorized uses or disclosures, or unauthorized collections by means of the electronic health record (EHR), even if you were not required to report them to the IPC under section 6.3 or section 18.3[1] of the Regulation.

Custodians will find it easier to provide the IPC with the information required at reporting time if they keep track of these statistics over the course of the preceding calendar year.

[1] Or, for coroners, clause 18.10(4)(b) of the Regulation.

SECTION 2: Total Number of Health Information Privacy Breaches

2.1	Enter the **total** number of health information privacy breach incidents experienced during the **reporting year** (January – December).	6

Enter this number into box 2.1 of the online questionnaire.

PLEASE NOTE:

Do NOT count each incident more than once. If one incident includes more than one of the following five categories (sections 3 through 7), choose the category that it best fits. For example, if an employee accessed personal health information without authority, and then disclosed the information, count that incident as either a use or a disclosure, but not both. The sum of boxes 3.1 + 4.1 + 5.1 + 6.1 + 7.1 must equal box 2.1.

SECTION 3: Stolen Personal Health Information

3.1 What was the total number of privacy breach incidents where personal health information **was stolen**? | 0 |

Enter this number into box 3.1 of the online questionnaire.

3.2 Of this total indicate the number of privacy breaches where:

Count each incident only once – the total on line 3.2.3 must equal line 3.1.

3.2.1	theft was by an **internal party** (such as an employee, affiliated health practitioner or electronic service provider).	
3.2.2	theft was by a **stranger**	
3.2.3	**Total** (should equal line 3.1)	0

3.3 Of the total on line 3.1 indicate the number of privacy breaches where:

Count each incident only once – the total on line 3.3.6 must equal line 3.1.

3.3.1	theft was the result of a ransomware attack	
3.3.2	theft was the result of another type of a cyberattack	
3.3.3	unencrypted portable electronic equipment (such as USB keys or laptops) was stolen	
3.3.4	paper records were stolen	
3.3.5	theft was a result of something else, by someone else or other items were stolen	

3.3.6	TOTAL INCIDENTS (3.3.1 to 3.3.5 = 3.3.6) Box 3.3.6 must equal Box 3.1	0

Enter the numbers in the table above into boxes 3.3.1 through 3.3.6 of the online questionnaire.

3.4 Of the total on line 3.1 indicate the number of privacy breaches where:

Count each incident only once – the total on line 3.4.6 must equal line 3.1.

3.4.1	one individual was affected	
3.4.2	2 to 10 individuals were affected	
3.4.3	11 to 50 individuals were affected	
3.4.4	51 to 100 individuals were affected	
3.4.5	over 100 individuals were affected	
3.4.6	TOTAL INCIDENTS (3.4.1 to 3.4.5 = 3.4.6) Box 3.4.6 must equal Box 3.1	0

Enter the numbers in the table above into boxes 3.4.1 through 3.4.6 of the online questionnaire.

SECTION 4: Lost Personal Health Information

4.1 What was the total number of privacy breach incidents where personal health information **was lost**? | 0 |

Enter this number into box 4.1 of the online questionnaire.

4.2 Of this total indicate the number of privacy breaches where:

Count each incident only once – the total on line 4.2.6 must equal line 4.1.

4.2.1	loss was the result of a ransomware attack	
4.2.2	loss was the result of another type of a cyberattack	
4.2.3	unencrypted portable electronic equipment (such as USB keys or laptops) was lost	
4.2.4	paper records were lost	
4.2.5	loss was a result of something else or other items were lost	
4.2.6	TOTAL INCIDENTS 4.2.1 to 4.2.4 = 4.2.5	0

Enter the numbers in the table above into boxes 4.2.1 through 4.2.6 of the online questionnaire.

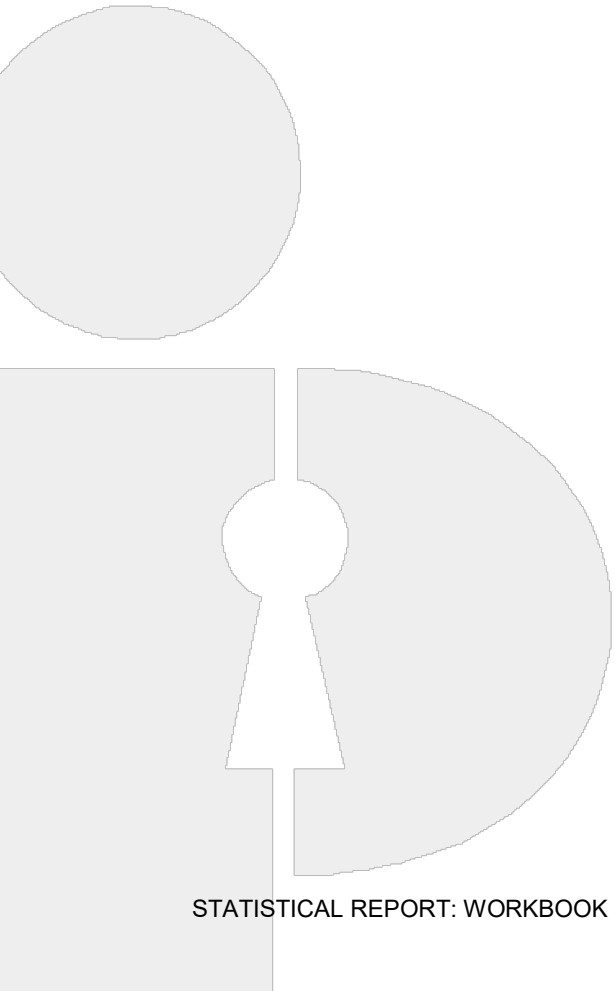
4.3 Of the total on line 4.1 indicate the number of privacy breaches where:

Count each incident only once – the total on line 4.3.6 must equal line 4.1.

4.3.1	one individual was affected	
4.3.2	2 to 10 individuals were affected	

4.3.3	11 to 50 individuals were affected	
4.3.4	51 to 100 individuals were affected	
4.3.5	over 100 individuals were affected	
4.3.6	TOTAL INCIDENTS (4.3.1 to 4.3.5 = 4.3.6) Box 4.3.6 must equal Box 4.1	0

Enter the numbers in the table above into boxes 4.3.1 through 4.3.6 of the online questionnaire.



SECTION 5: Used Without Authority

5.1 What was the total number of privacy breach incidents where personal health information **was used (e.g. viewed, handled) without authority**?

1

Enter this number into box 5.1 of the online questionnaire.

5.2 Of this total indicate the number of privacy breaches where:

Count each incident only once – the total on line 5.2.4 must equal line 5.1.

5.2.1	unauthorized use was through electronic records	1
5.2.2	unauthorized use was through paper records	
5.2.3	unauthorized use through other means	
5.2.4	TOTAL INCIDENTS (5.2.1 + 5.2.2 + 5.2.3 = 5.2.4) Box 5.2.4 must equal Box 5.1	1

Enter the numbers in the table above into boxes 5.2.1 through 5.2.4 of the online questionnaire.

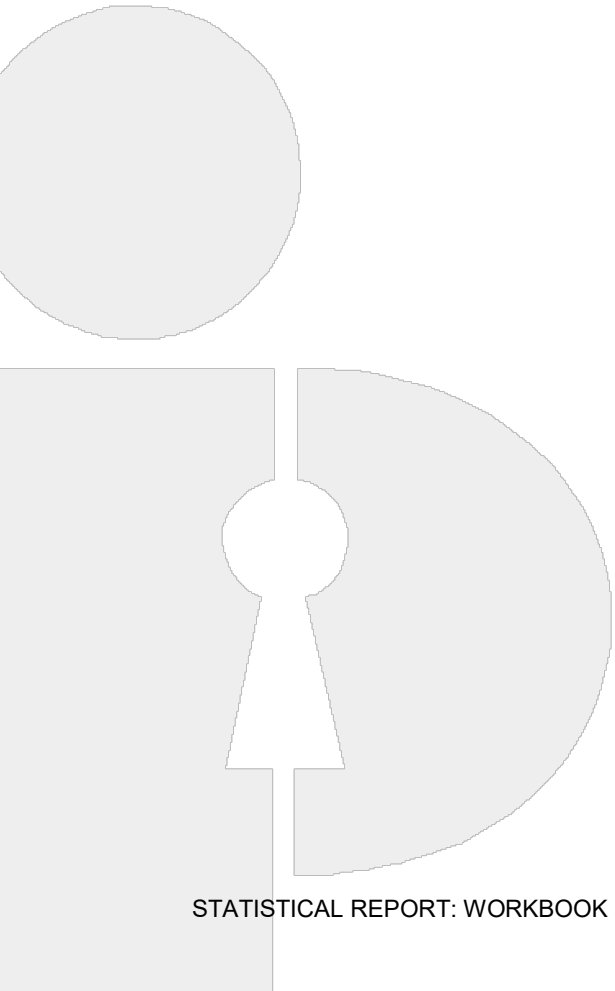
5.3 Of the total on line 5.1 indicate the number of privacy breaches where:

Count each incident only once – the total on line 5.3.6 must equal line 5.1.

5.3.1	one individual was affected	1
5.3.2	2 to 10 individuals were affected	
5.3.3	11 to 50 individuals were affected	
5.3.4	51 to 100 individuals were affected	

5.3.5	over 100 individuals were affected	
5.3.6	TOTAL INCIDENTS (5.3.1 to 5.3.5 = 5.3.6) Box 5.3.6 must equal Box 5.1	1

Enter the numbers in the table above into boxes 5.3.1 through 5.3.6 of the online questionnaire.



SECTION 6: Disclosed Without Authority

6.1 What was the total number of privacy breach incidents where personal health information **was disclosed without authority**?

5

Enter this number into box 6.1 of the online questionnaire.

6.2 Of this total indicate the number of privacy breaches where:

Count each incident only once – the total on line 6.2.4 must equal line 6.1.

6.2.1	unauthorized disclosure was through misdirected faxes	
6.2.2	unauthorized disclosure was through misdirected emails	3
6.2.3	unauthorized disclosure was through other means	2
6.2.4	TOTAL INCIDENTS (6.2.1 + 6.2.2 + 6.2.3 = 6.2.4) Box 6.2.4 must equal Box 6.1	5

Enter the numbers in the table above into boxes 6.2.1 through 6.2.4 of the online questionnaire.

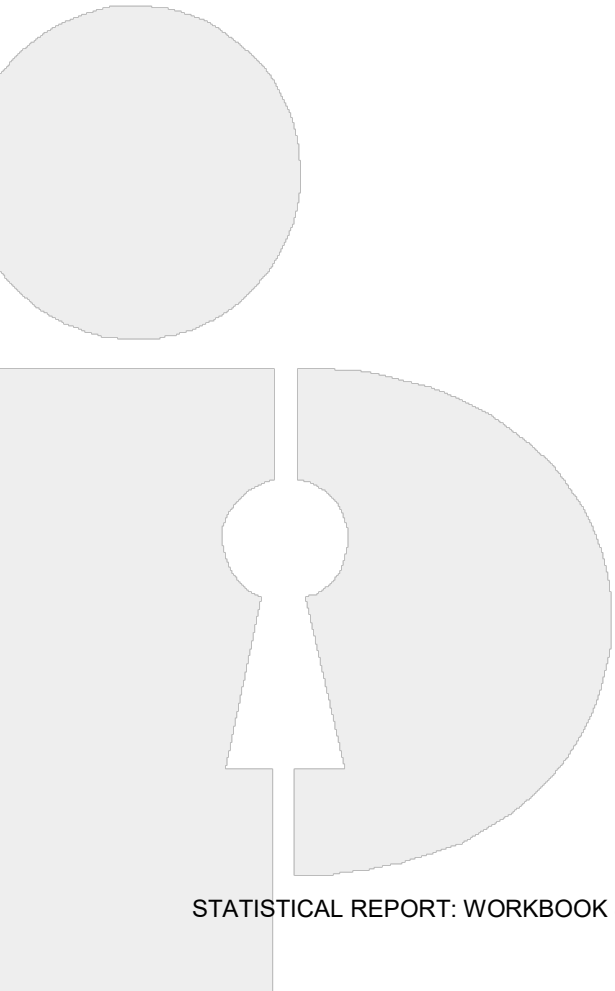
6.3 Of the total on line 6.1 indicate the number of privacy breaches where:

Count each incident only once – the total on line 6.3.6 must equal line 6.1.

6.3.1	one individual was affected	2
6.3.2	2 to 10 individuals were affected	3
6.3.3	11 to 50 individuals were affected	
6.3.4	51 to 100 individuals were affected	

6.3.5	over 100 individuals were affected	
6.3.6	TOTAL INCIDENTS (6.3.1 to 6.3.5 = 6.3.6) Box 6.3.6 must equal Box 6.1	5

Enter the numbers in the table above into boxes 6.3.1 through 6.3.6 of the online questionnaire.



SECTION 7: Collected Without Authority by means of the EHR

7.1 What was the total number of privacy breach incidents where personal health information was **collected by the custodian by means of the EHR without authority**?

Enter this number into box 7.1 of the online questionnaire.

7.2 Of this total indicate the number of privacy breaches where:

Count each incident only once – the total on line 7.2.6 must equal line 7.1.

7.2.1	One individual was affected	
7.2.2	2 to 10 individuals were affected	
7.2.3	11 to 50 individuals were affected	
7.2.4	51 to 100 individuals were affected	
7.2.5	Over 100 individuals were affected	
7.2.6	TOTAL INCIDENTS (7.2.1 to 7.2.5 = 7.2.6) Box 7.2.6 must equal Box 7.1	0

Enter the numbers in the table above into boxes 7.2.1 through 7.2.6 of the online questionnaire.

Completing and Submitting Your Questionnaire

This workbook and guide is for your use in completing your statistical report and should not be faxed or mailed to the Information and Privacy Commissioner in lieu of online submission. **Faxed or mailed copies of this workbook and guide will NOT be accepted.** Please submit your statistical report through the online questionnaire at: https://statistics.ipc.on.ca

Health Information Custodians

Health information custodians are required to submit an annual statistical report on health privacy breaches to the IPC using the Online Statistical Reporting System at https://statistics.ipc.on.ca. You will need a login id, with which you will set a password. Please request them via an email to statistics.ipc@ipc.on.ca and include the following:

- the name of your health information custodian
- the name and e-mail address of the person responsible for the content of the report (the management contact)
- the name, e-mail address, telephone and fax numbers and the mailing address of the person responsible for completing the report (the primary contact**)**
- your language preference (English or Français)

Health Information Custodians Reporting as Institutions under *FIPPA*/*MFIPPA*

As a Health Information Custodian who has also been reporting as an institution under *FIPPA/MFIPPA*, you should already have a login ID for the Online Statistical Reporting System.

If you have lost or forgotten it, you may request it via an email to statistics.ipc@ipc.on.ca indicating your institution name. If you have lost your password, you can reset it on the log-in page.

You have three different options for login and password:

- a single login id and password to submit all of your reports (for *FIPPA*/*MFIPPA* report, *PHIPA* access report and your *PHIPA* privacy breach statistics report).

  Having a single login id and password is convenient if the same person will be submitting all three reports;

- one login id and password for *FIPPA*/*MFIPPA* and a second login id and password for the two *PHIPA* reports;
- separate logins and passwords for each of the three reports.

The option you choose all depends on your organizational structure. Please indicate whether you want a single login id set or two or three separate ones.

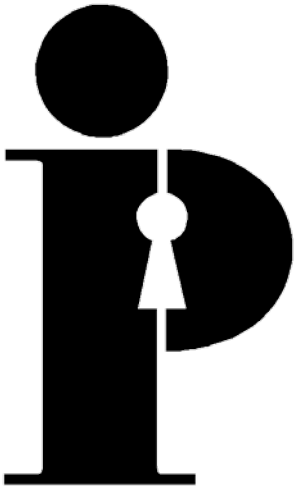
Once you have your login id and have completed this workbook, log on to the Online Statistical Reporting System at https://statistics.ipc.on.ca and enter your questionnaire data section by section. You may log off the system at any time and it will remember where you left off when you log on the next time. This means you do not have to complete and submit your questionnaire all in one session as long as you do complete and submit it before the deadline date. **The Online Statistical Reporting System will not be available after the deadline date**.

When you have completed entering your questionnaire, the system allows you to review your answers and make any necessary corrections before confirming and submitting your questionnaire. Once you have confirmed and submitted your questionnaire you are done, but should you discover that a correction is necessary after you have confirmed and submitted your questionnaire, you may log on to the Online Statistical Reporting System at any time before the deadline date and make the correction as needed. You will need to re-confirm your questionnaire and submit it again in order for the correction to be applied.

Changes to the type of questionnaire submitted may be made in the same manner. If, for example, you originally submitted a questionnaire stating that you had experienced no personal health information privacy breaches (a “zero report”), but then discovered that you indeed had experienced one or more such breaches, you may log on to the Online Statistical Reporting System at any time before the deadline date and simply change the questionnaire type selection on line 1.3 of Section 1. The system will take care of the rest and will take you to the appropriate sections of the questionnaire so you may complete them. Again, you will need to re-confirm your completed questionnaire and submit it again in order for the correction to be applied.

If you have specific questions that are not answered by this workbook and guide, please read our frequently asked questions, email **statistics.ipc@ipc.on.ca** or call the Information and Privacy Commissioner of Ontario’s main switchboard **416-326-3333**. If you are calling long distance, use our toll-free line: **1-800-387-0073**.

PHIPA



Statistical Report for the Information and Privacy Commissioner of Ontario on

Personal Health Information Access Requests

WORKBOOK AND COMPLETION GUIDE

Introduction

Use this workbook and guide as a "how to" tool to complete the statistical report for the Information and Privacy Commissioner of Ontario about requests made under the *Personal Health Information Protection Act, 2004* (*PHIPA*). We encourage you to use it to help you complete and submit your questionnaire online, especially if you are unfamiliar with the reporting process.

For your convenience:

- this workbook and guide is laid out in the same manner as the online questionnaire (section by section)
- some sections which will appear in *italicized text* have been expanded to contain background information which may be helpful to you
- the **bold** text is defined in the glossary at the back of this guide
- the reconciliation chart is designed to help verify the figures in the questionnaire.

If there are any questions that have not been answered by this guide, there are two ways to receive additional information from the Information and Privacy Commissioner of Ontario:

- e-mail statistics.ipc@ipc.on.ca
- call our main switchboard: Local calls 416 326-3333, long distance, use our toll-free line: 1-800-387-0073

The questionnaire only includes access or correction requests made by an individual (or by the individual's substitute decision-maker) for their own personal health information. DO NOT include disclosures of personal health information to any other party, including health information custodians, even if the individual requested the disclosures. If no requests for access to personal health information or requests for correction of personal health information were received under this act, the health information custodian must still complete and submit Section 1 and 2.

This workbook and guide is for your use in completing your questionnaire and should **not** be faxed or mailed to the Information and Privacy Commissioner in lieu of online submission. Faxed or mailed copies of this workbook and guide will NOT be accepted. Please submit your questionnaire online at: https://statistics.ipc.on.ca

SECTION 1: Identification

1.1 Please clearly indicate the name of the institution, name of the contact person responsible for *PHIPA*, phone/fax numbers, mailing and e-mail addresses, name of the person to contact with any questions about the content of the report.

1.2 Please indicate the type of municipal or provincial institution that the **health information custodian** is either an agent of or is a part of (e.g. if the health information custodian is an ambulance service and is part of a municipality, the check mark would be placed in the box for municipal corporation). If the appropriate municipal type is not listed, check "other" and specify.

1.3 Please indicate the type of health information custodian that is reporting. Submit separate reports for each type of health information custodian.

SECTION 2: Uses or Purposes of Personal Health Information

2.1 Provide the number of uses or purposes for which personal health information was disclosed where the use or purpose is not included in the written public statement of information practices under the *Personal Health Information Protection Act* subsection 16(1).

0

Enter this number into box 2.1 of the online questionnaire.

	If your institution or **health information custodian received or completed no formal written requests for access or correction of personal health information** from individuals (or from the individuals' substitute decision makers), PLEASE STOP HERE AND SUBMIT ONLY SECTIONS 1 AND 2 OF THE REPORT.
	If your institution or **health information custodian** received or completed formal written requests for access to personal health information from an individual (or from their substitute decision maker), PLEASE CONTINUE TO SECTION 3.
	If your institution or **health information custodian** did not receive or complete any requests from individuals (or by the individuals' substitute decision makers) for access to their own **personal health information** but did receive (or carried forward from last year) or complete at least one request for correction of **personal health information**, PLEASE COMPLETE AND SUBMIT SECTION 9.

SECTION 3: Number of Requests

How Are Requests Counted?

*The following will assist you to determine how and when to count a **personal health information** request as being received.*

- *Any **personal health information** access request is counted as one request regardless of the number of records involved because it is about only one subject – "the person asking for the information."*

- *COUNT ONLY written requests made by individuals (or by the individuals' substitute decision makers) for their own personal health information.*

- *If you receive a request that requires clarification, DO NOT COUNT this as a request received until the requester provides you with all the information you need to complete the request.*

- *DO NOT COUNT a request to correct personal health information in this section (see section 9).*

3.1 - Enter the number of written requests made by individuals (or by the individual's substitute decision-makers) for access to their own personal health information that were received during the reporting year (January to December). 4

Enter this number into box 3.1 of the online questionnaire.

-

SECTION 4: Time to Completion

4.1–4.3 Enter the number of completed **personal health information** requests in the appropriate categories.

PLEASE NOTE:

*The response time to a requester may be extended to review and locate **records** and for consultation as described in subsection 54(3).*

How long did your institution take to respond to all requests for information? Enter the number of requests in the appropriate category.

4.1	1-30 days	4
4.2	Over 30 days with an extension	
4.3	Over 30 days without an extension	
4.4	TOTAL REQUESTS COMPLETED (4.1 to 4.3 = 4.4)	4

Enter the numbers in the table above into boxes 4.1 through 4.4 of the online questionnaire.

SECTION 5: Compliance with the *PHIPA*

The *PHIPA states that requests for access to **personal health information** should be completed within 30 days. In cases where there is a need to review or search numerous **records** or to conduct consultations, a **health information custodian** can extend the 30-day time limit for no more than an additional 30 days and remain in compliance with the PHIPA. This can be achieved by issuing a **Notice of Extension** (subsection 54(4)).*

*This section has been broken down into three different sections. Sections A and B are mutually exclusive and will be used to determine the number of requests that are in compliance or not in compliance with the statutory timelines under PHIPA. Section D deals with **expedited access requests** that are already included in Sections A and B.*

A. Notice of Extension Not Issued

5.1	Enter the number of requests completed within 30 days where no **Notice of Extension** was issued.	4
5.2	Enter the number of requests completed beyond the 30 days where no **Notice of Extension** was issued.	
5.3	Add boxes 5.1 and 5.2 to determine the total number of completed requests where no **Notice of Extension** was issued.	4

Enter the numbers in the table above into boxes 5.1 through 5.3 of the online questionnaire.

B. Notice of Extension (subsection 54(4)) Issued

5.4	Enter the number of requests completed within the time limit stipulated in the **Notice of Extension**.	
5.5	Enter the number of requests completed that exceeded the permitted time limit stipulated in the **Notice of Extension**.	
5.6	Add boxes 5.4 and 5.5 to determine the total number of completed requests where a **Notice of Extension** was issued.	0

Enter the numbers in the table above into boxes 5.4 through 5.6 of the online questionnaire.

C. Total Requests Completed (sections A and B)

5.7	Enter the overall total number of requests completed for the year by adding the totals from sections A and B (boxes 5.3 + 5.6 = 5.7). This total must equal the total number of requests shown in box 4.4.	4

Enter this number into box 5.7 of the online questionnaire.

D. Expedited Access requests (subsection 54(5))

5.8	Enter the number of completed requests from the total reported in box 5.7 that were requests for expedited access and completed within the requested time period.	
5.9	Enter the number of completed requests from the total reported in box 5.7 that were requests for expedited access and were completed in excess of the requested time period.	
5.10	Add boxes 5.8 and 5.9 to determine the total number of completed requests for expedited access.	0

Enter the numbers in the table above into boxes 5.8 through 5.10 of the online questionnaire.

SECTION 5(a): Contributing Factors

This section provides an opportunity for you to explain why the 30-day time line to complete requests could not be met. As well, it requests details on how to improve on the response rate in order to be compliant with the PHIPA.

Please outline any factors that may have caused you to not meet the 30-day time limit. If you anticipate circumstances that will improve your ability to comply with the *PHIPA* in the future, please provide details in the space below.

Enter the factors above into Section 5a of the online questionnaire.

SECTION 6: Disposition of Requests

*This section requests information about how each **personal health information** access request was handled.*

6.1 Enter the number of requests that resulted in full access to personal health information requested.

*6.2 Enter the number of requests where the **health information custodian** provided partial access to the requested information because **provisions** of PHIPA were used to deny access.*

*6.3 Enter the number of requests where the **health information custodian** provided partial access to the requested information because some of the records of personal health information do not exist or cannot be found.*

*6.4 Enter the number of requests where requested information was partially accessed because parts of the **record** exist outside of the PHIPA.*

*6.5 Enter the number of requests where no information was accessed and the **provisions** of PHIPA which were used to deny access.*

*6.6 Enter the number of requests where no information was accessed, because no **record** exists or none can be found.*

*6.7 Enter the number of requests where no information was accessed because the **record** is outside of the PHIPA.*

6.8 Enter the number of requests that were unfulfilled because they were withdrawn or abandoned by the requester.

6.9 Enter the number of requests from box 6.8 that were withdrawn or abandoned after a fee estimate was sent out.

6.10 Add the number of requests from boxes 6.1 to 6.8 to determine the disposition for the total number of requests. Do not include box 6.9 data in the total. This number should be greater than or equal to the total number of completed requests shown in box 4.4.

6.11 Add the number of requests in boxes 6.2 and 6.5 to determine the total number of requests where access to information was denied in whole or in part. This number should be less than or equal to box 7.12.

What course of action was taken for each of the requests completed? Please enter the number of requests into the appropriate category.

6.1	Full access provided	2
6.2	Partial access provided: provisions applied to deny access	2
6.3	Partial access provided: no record exists or cannot be found	
6.4	Partial access provided: record outside of *PHIPA*	
6.5	No access provided: provisions applied to deny access	
6.6	No access provided: no record exists or cannot be found	
6.7	No access provided: record outside of *PHIPA*	
6.8	Other completed requests, e.g. withdrawn or never proceeded with	
6.9	Number of requests from box 6.8 that were not pursued following a fee estimate	
6.10	TOTAL REQUESTS (EXCLUDING 6.9) (6.1 to 6.8 = 6.10) Box 6.10 must be greater than or equal to Box 4.4	4
6.11	TOTAL REQUESTS denied access in whole or part where a provision of PHIPA was applied (6.2 + 6.5 = 6.11) Box 6.11 must be less than or equal to Box 7.12	2

Enter the numbers in the table above into boxes 6.1 through 6.11 of the online questionnaire.

SECTION 7: REASONS APPLIED TO DENY ACCESS

*Box 6.11 of the previous section (Total Requests Denied Access in Whole or in Part) shows the total number of requests for which access to part or all of the requested information was denied based on **provisions** in PHIPA. In this section, you must apply one or more **provisions** to each request. The total must be greater than or equal to Box 6.11.*

For the TOTAL REQUESTS where a provision was applied to deny access in full or in part, how many times did you apply each of the following? (Please note that more than one provision may be applied to each request.)

7.1	Section 51(1)(a) – Quality of Care Information	
7.2	Section 51(1)(b) – Quality Assurance Program (Regulated Health Professions Act, 1991)	
7.3	Section 51(1)(c) – Raw Data from Psychological Tests	
7.4	Section 51(d) – Prescribed Research or Laboratory Information	
7.5	Section 52(1)(a) – Legal Privilege	
7.6	Section 52(1)(b) – Other Acts or Court Order	
7.7	Section 52(1)(c) – Proceedings that have not been concluded	
7.8	Section 52(1)(d) – Inspection, Investigation or Similar Procedure	
7.9	Section 52(1)(e) – Risk of Harm to or Identification of an Individual	2
7.10	Section 52(1)(f) – MFIPPA subsections 38(a) or (c) or FIPPA subsections 49 (a),(c) or (e) apply	
7.11	Section 54(6) – Frivolous or Vexatious	
7.12	TOTAL (7.1 to 7.11) (must be greater than or equal to Box 6.11)	2

Enter the numbers in the table above into boxes 7.1 through 7.12 of the online questionnaire.

SECTION 8: Fees

*This section concerns **fees** charged for access to **personal health information**.*

8.1	Number of requests for access to records of **personal health information** where **fees** were collected	0

*A **health information custodian** may waive all or part of a fee being charged if the custodian feels it is fair and equitable to do so.*

8.2	Number of requests where **fees were waived** – in full	
8.3	Number of requests where **fees were waived** – in part	
8.4	Total number of requests where **fees were waived** (8.2 + 8.3 = 8.4)	0

8.5	Total dollar amount of fees collected	0
8.6	Total dollar amount of **fees waived**	0

Enter the numbers in the table above into boxes 8.1 through 8.6 of the online questionnaire.

SECTION 9: Corrections and Statement of Disagreement

*If an individual believes that his or her record of personal health information held by a **health information custodian** is inaccurate or incomplete with respect to the purposes for which the **health information custodian** uses the information, he or she has a right to:*

- *request that the **health information custodian** correct the **personal health information**;*
- *receive a written notice from the custodian to grant or refuse the request;*
- *request a written notice of the requested correction, to the extent reasonably possible, be sent to those to whom the custodian disclosed the information, except if it will have no effect on the provision of health care or other benefits to the individual; and*
- *require the **health information custodian** to attach a **statement of disagreement** to the information if the requested correction was not made and to disclose the statement of disagreement whenever the **health information custodian** discloses the information in issue.*

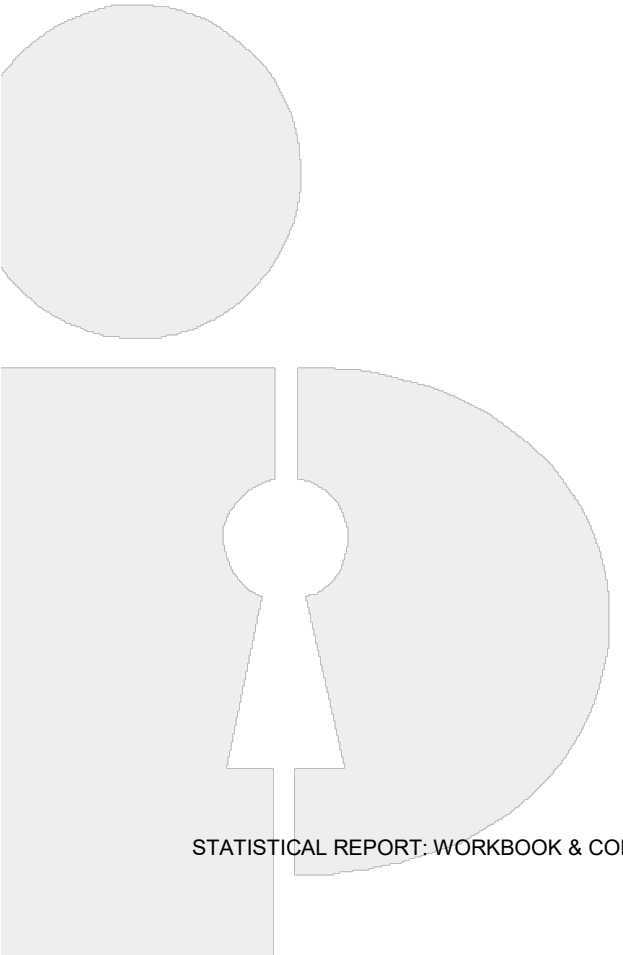
9.1	Enter the number of new correction requests received for the **reporting year**.	0

What course of action was taken when the requests for correction were received?

9.2	Enter the number of corrections that were made in their entirety.	
9.3	Enter the number of corrections partially made.	
9.4	Enter the number of correction requests that were refused.	
9.5	Enter the number of correction requests that were withdrawn by the requester before completion.	
9.6	Add boxes 9.2 to 9.5 to determine the total number of correction requests made for the **reporting year**. This total should be equal to the amount shown in box 9.1.	0

9.7	Enter the number of correction requests that were made in part (box 9.3) or denied in full (box 9.4) where **statements of disagreement** were attached to the **personal health information record**.	0
9.8	Enter the number of notices of correction or statements of disagreements that were sent to a third party	0

Enter the numbers in the table above into boxes 9.2 through 9.8 of the online questionnaire.



Completing and Submitting Your Questionnaire

This workbook and guide is for your use in completing your report and should not be faxed or mailed to the Information and Privacy Commissioner in lieu of online submission. **Faxed or mailed copies of this workbook and guide will NOT be accepted.** Please submit your report online using the IPC's Online Statistics Submission Website.

Your institution should have a login ID and password for the Online Statistics Submission Website. If you have lost or forgotten your ID or password, visit https://statistics.ipc.on.ca/ and click on the "Forgot your password or login ID?" link.

New Institutions

If your institution has recently come under the jurisdiction of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) or the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, AND you are also a **Health Information Custodian** as defined in Section 3 of *PHIPA*, you are required to submit a statistical report annually to the IPC using the using the Online Statistics Submission Website for which you will need a login ID and a password. If this is your first time submitting an annual report to the IPC, visit our Registration for Statistical Reporting page to set up an account and get a login ID and a password. You will need to include:

- the name of your institution
- the name and e-mail address of the head of the institution (for *FIPPA/MFIPPA* only)
- the name and e-mail address of the person responsible for the content of the report (the management contact)
- the name, e-mail address, telephone and fax numbers and the mailing address of the person responsible for completing the report (the primary contact**)**
- your language preference (English or Français)

As a **Health Information Custodian**, you have the option of a single login id and password to submit both your *FIPPA*/*MFIPPA* report and your *PHIPA* report (which is convenient if the same person will be submitting both reports) or you may wish to have one login id and password for *FIPPA*/*MFIPPA* and another for *PHIPA* (which makes it easier if two different people will submit the reports) – it all depends on your organizational structure.

Once you have your login id and password and have completed this workbook, log on to the Online Statistics Submission Website at https://statistics.ipc.on.ca and enter your questionnaire data section by section. You may log off the system at any time and it will remember where you left off when you log on the next time. This means you do not have to complete and submit your questionnaire all in one session as long as you do complete and submit it before the deadline date **The Online Statistics Submission Website will not be available after the deadline date**.

When you have completed entering your questionnaire, the system allows you to review your answers and make any necessary corrections before confirming and submitting your questionnaire. Once you have confirmed and submitted your questionnaire you are done, but should you discover that a correction is necessary after you have confirmed and submitted your questionnaire, you may log on to the Online Statistics Submission Website at any time before the deadline date and make the correction as needed. You will need to re- confirm your questionnaire and submit it again in order for the correction to be applied.

Changes to the type of questionnaire submitted may be made in the same manner. If, for example, you originally submitted a questionnaire stating that you had received no requests for access to **personal health information** (a “zero report”), but then discovered that you indeed had received one or more such requests, you may log on to the Online Statistics Submission Website at any time before the deadline date and simply change the questionnaire type selection at the end of Section 2. The system will take care of the rest and will take you to the appropriate sections of the questionnaire so you may complete them. Again, you will need to re-confirm your completed questionnaire and submit it again in order for the correction to be applied.

If you have specific questions that are not answered by this workbook and guide, please email **statistics.ipc@ipc.on.ca** or call the Information and Privacy Commissioner of Ontario’s main switchboard **416-326-3333**. If you are calling long distance, use our toll free line: **1-800-387-0073**.

Glossary of Terms

Fee(s), Waived - A head may waive all or part of a fee if the custodian feels it is fair and equitable to do so.

Health Information Custodian - Any person or organization described in subsection (reporting context only) 3(1) of *PHIPA* or any group of entities that has been permitted to act as a single health information custodian pursuant to a Minister's order under subsection 3(8).

Notice of Extension - A health information custodian or head may extend the time to complete a request by a maximum of an additional 30 days. This is only permissible if meeting the initial 30 day timeline would interfere with the operations of the custodian (e.g. due to numerous pieces of information or information that requires a lengthy search to locate) or if consultations would require more time to complete. The notice must include:

- the length of the extension; and
- the reason for the extension.

Personal Health Information - Personal health information means identifying information about an individual in oral or recorded form, if the information,

- relates to the physical or mental health or provision of health care to the individual;
- is a plan of service within the meaning of the *Long-term Care Act* for the individual;
- relates to payments or eligibility for health care of the individual;
- 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 of bodily substance;
- is the individual's health number;
- identifies an individual's substitute decision-maker.

Personal health information also includes a mixed record that contains identifiable personal information that is not personal health information, but is contained in a record that contains personal health information. However, it excludes employee records held by a custodian that are not primarily used for health care.

Provision to deny access (Exclusions, Exemptions) - These are specific sections in *PHIPA* that provide the grounds on which the health information custodian or head may deny access to information.

Provision to deny access (Frivolous or Vexatious or made in bad faith) **-** A custodian may refuse to grant access or make a correction to a record if believed to be on reasonable grounds that the request was for frivolous or vexatious reasons or made in bad faith.

Record(s) - A record means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record

Reporting Year - January to December.

Request, Access - Access requests occur only when access requests are made by individuals (or by the individuals' substitute decision-makers) for their own personal health information. DO NOT include disclosures for personal health information to any other party, including other health information custodians, even if the individual requested these disclosures.

Request, Completed - A request is considered to be complete once a decision letter has been sent to the individual in response to a personal health information access request.

Request, Correction - A request to have one's own personal health information corrected.

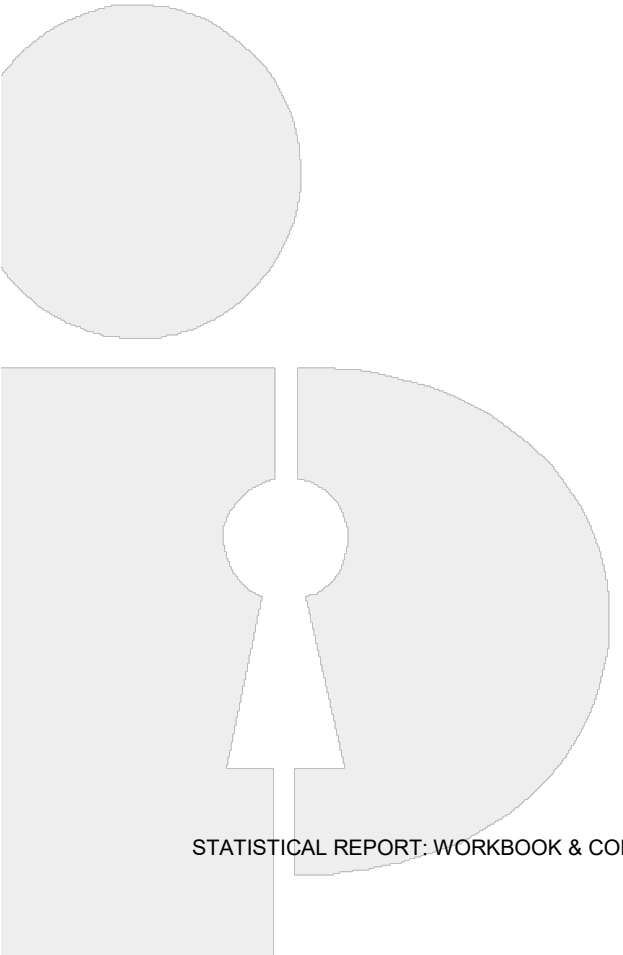
Request, Disposition - The end result of a completed access request (e.g. personal health information was disclosed, denied, or the request was withdrawn or never accessed)

Request, Expedited Access - When the individual requests that a health information custodian provide a response within a time period specified by the requester under subsection 54(5).

Statement of Disagreement - A precise statement of disagreement prepared by the individual that sets out the correction the health information custodian has refused to make

Written Public Statement - A written statement, made available to the public, that:

- provides a description of the custodian's information practices;
- describes how to contact the contact person or custodian;
- describes how an individual may access or request correction of a record of personal health information;
- describes how to make a complaint to the custodian and the IPC.



Reconciliation Chart

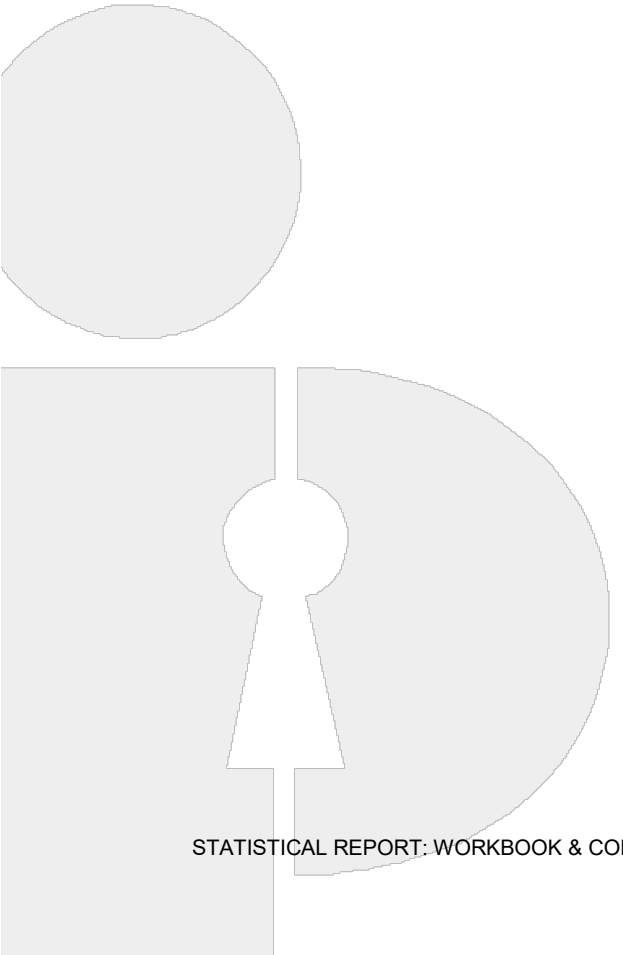
The chart below should be used to help verify your figures in completing this workbook and entering your questionnaire on the Online Statistics Submission Website.

Box Number	Criteria *	Box = Number(s)
4.4	=	4.1 to 4.3
5.3	=	5.1 +5.2
5.6	=	5.4 + 5.5
5.7	=	5.3 + 5.6
5.7	=	4.4
5.10	=	5.8 + 5.9
6.10	=	6.1 to 6.8
6.10	= or >	4.4
6.11	=	6.2 + 6.5
6.11	= or <	7.12
7.12	=	7.1 to 7.11
8.4	=	8.2 + 8.3
9.6	=	9.2 to 9.5
9.6	=	9.1

* = equal to
> greater than
< less than

9.7	Enter the number of correction requests that were made in part (box 9.3) or denied in full (box 9.4) where **statements of disagreement** were attached to the **personal health information record**.	
9.8	Enter the number of notices of correction or statements of disagreements that were sent to a third party	

Enter the numbers in the table above into boxes 9.2 through 9.8 of the online questionnaire.



Completing and Submitting Your Questionnaire

This workbook and guide is for your use in completing your report and should not be faxed or mailed to the Information and Privacy Commissioner in lieu of online submission. **Faxed or mailed copies of this workbook and guide will NOT be accepted.** Please submit your report online using the IPC's Online Statistics Submission Website.

Your institution should have a login ID and password for the Online Statistics Submission Website. If you have lost or forgotten your ID or password, visit https://statistics.ipc.on.ca/ and click on the "Forgot your password or login ID?" link.

New Institutions

If your institution has recently come under the jurisdiction of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) or the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, AND you are also a **Health Information Custodian** as defined in Section 3 of *PHIPA*, you are required to submit a statistical report annually to the IPC using the using the Online Statistics Submission Website for which you will need a login ID and a password. If this is your first time submitting an annual report to the IPC, visit our Registration for Statistical Reporting page to set up an account and get a login ID and a password. You will need to include:

- the name of your institution
- the name and e-mail address of the head of the institution (for *FIPPA/MFIPPA* only)
- the name and e-mail address of the person responsible for the content of the report (the management contact)
- the name, e-mail address, telephone and fax numbers and the mailing address of the person responsible for completing the report (the primary contact**)**
- your language preference (English or Français)

As a **Health Information Custodian**, you have the option of a single login id and password to submit both your *FIPPA*/*MFIPPA* report and your *PHIPA* report (which is convenient if the same person will be submitting both reports) or you may wish to have one login id and password for *FIPPA*/*MFIPPA* and another for *PHIPA* (which makes it easier if two different people will submit the reports) – it all depends on your organizational structure.

Once you have your login id and password and have completed this workbook, log on to the Online Statistics Submission Website at https://statistics.ipc.on.ca and enter your questionnaire data section by section. You may log off the system at any time and it will remember where you left off when you log on the next time. This means you do not have to complete and submit your questionnaire all in one session as long as you do complete and submit it before the deadline date **The Online Statistics Submission Website will not be available after the deadline date**.

When you have completed entering your questionnaire, the system allows you to review your answers and make any necessary corrections before confirming and submitting your questionnaire. Once you have confirmed and submitted your questionnaire you are done, but should you discover that a correction is necessary after you have confirmed and submitted your questionnaire, you may log on to the Online Statistics Submission Website at any time before the deadline date and make the correction as needed. You will need to re- confirm your questionnaire and submit it again in order for the correction to be applied.

Changes to the type of questionnaire submitted may be made in the same manner. If, for example, you originally submitted a questionnaire stating that you had received no requests for access to **personal health information** (a “zero report”), but then discovered that you indeed had received one or more such requests, you may log on to the Online Statistics Submission Website at any time before the deadline date and simply change the questionnaire type selection at the end of Section 2. The system will take care of the rest and will take you to the appropriate sections of the questionnaire so you may complete them. Again, you will need to re-confirm your completed questionnaire and submit it again in order for the correction to be applied.

If you have specific questions that are not answered by this workbook and guide, please email **statistics.ipc@ipc.on.ca** or call the Information and Privacy Commissioner of Ontario’s main switchboard **416-326-3333**. If you are calling long distance, use our toll free line: **1-800-387-0073**.

Glossary of Terms

Fee(s), Waived - A head may waive all or part of a fee if the custodian feels it is fair and equitable to do so.

Health Information Custodian - Any person or organization described in subsection (reporting context only) 3(1) of *PHIPA* or any group of entities that has been permitted to act as a single health information custodian pursuant to a Minister's order under subsection 3(8).

Notice of Extension - A health information custodian or head may extend the time to complete a request by a maximum of an additional 30 days. This is only permissible if meeting the initial 30 day timeline would interfere with the operations of the custodian (e.g. due to numerous pieces of information or information that requires a lengthy search to locate) or if consultations would require more time to complete. The notice must include:

- the length of the extension; and
- the reason for the extension.

Personal Health Information - Personal health information means identifying information about an individual in oral or recorded form, if the information,

- relates to the physical or mental health or provision of health care to the individual;
- is a plan of service within the meaning of the *Long-term Care Act* for the individual;
- relates to payments or eligibility for health care of the individual;
- 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 of bodily substance;
- is the individual's health number;
- identifies an individual's substitute decision-maker.

Personal health information also includes a mixed record that contains identifiable personal information that is not personal health information, but is contained in a record that contains personal health information. However, it excludes employee records held by a custodian that are not primarily used for health care.

Provision to deny access (Exclusions, Exemptions) - These are specific sections in *PHIPA* that provide the grounds on which the health information custodian or head may deny access to information.

Provision to deny access (Frivolous or Vexatious or made in bad faith) **-** A custodian may refuse to grant access or make a correction to a record if believed to be on reasonable grounds that the request was for frivolous or vexatious reasons or made in bad faith.

Record(s) - A record means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record

Reporting Year - January to December.

Request, Access - Access requests occur only when access requests are made by individuals (or by the individuals' substitute decision-makers) for their own personal health information. DO NOT include disclosures for personal health information to any other party, including other health information custodians, even if the individual requested these disclosures.

Request, Completed - A request is considered to be complete once a decision letter has been sent to the individual in response to a personal health information access request.

Request, Correction - A request to have one's own personal health information corrected.

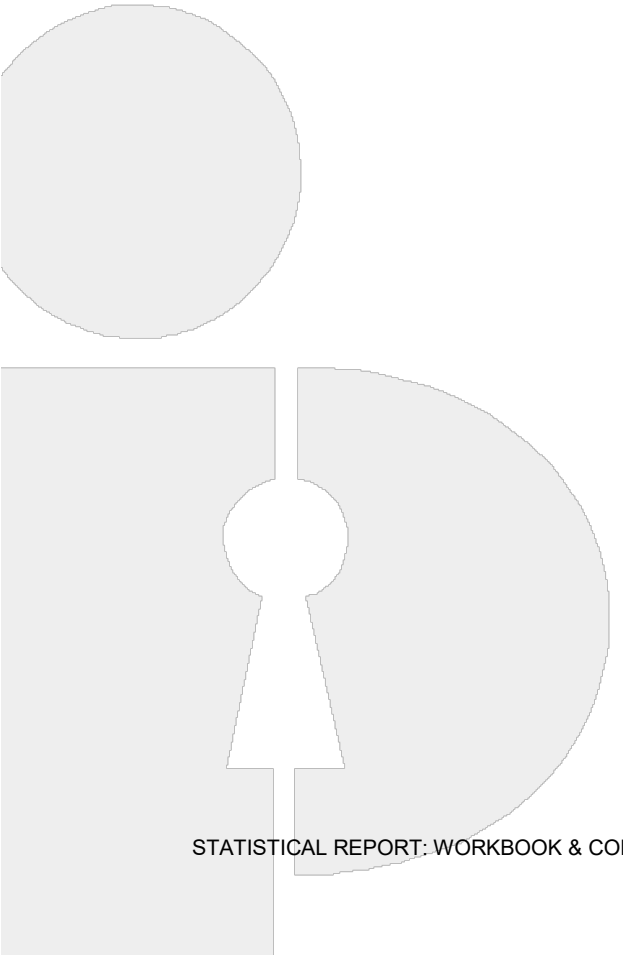
Request, Disposition - The end result of a completed access request (e.g. personal health information was disclosed, denied, or the request was withdrawn or never accessed)

Request, Expedited Access - When the individual requests that a health information custodian provide a response within a time period specified by the requester under subsection 54(5).

Statement of Disagreement - A precise statement of disagreement prepared by the individual that sets out the correction the health information custodian has refused to make

Written Public Statement - A written statement, made available to the public, that:

- provides a description of the custodian's information practices;
- describes how to contact the contact person or custodian;
- describes how an individual may access or request correction of a record of personal health information;
- describes how to make a complaint to the custodian and the IPC.

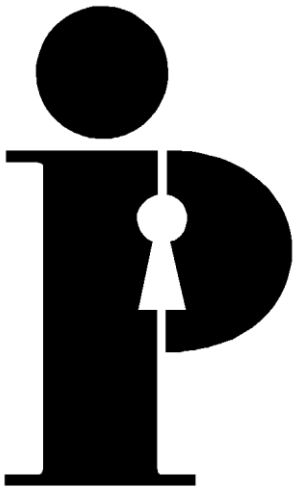


Reconciliation Chart

The chart below should be used to help verify your figures in completing this workbook and entering your questionnaire on the Online Statistics Submission Website.

Box Number	Criteria *	Box = Number(s)
4.4	=	4.1 to 4.3
5.3	=	5.1 +5.2
5.6	=	5.4 + 5.5
5.7	=	5.3 + 5.6
5.7	=	4.4
5.10	=	5.8 + 5.9
6.10	=	6.1 to 6.8
6.10	= or >	4.4
6.11	=	6.2 + 6.5
6.11	= or <	7.12
7.12	=	7.1 to 7.11
8.4	=	8.2 + 8.3
9.6	=	9.2 to 9.5
9.6	=	9.1

* = equal to
> greater than
< less than



The Year-End Statistical Report
for the
Information and Privacy Commissioner of Ontario, Canada

WORKBOOK AND COMPLETION GUIDE

General Information

This workbook and guide is designed to provide step-by-step instructions for the completion of the Information and Privacy Commissioner's (IPC) Year-End Statistical Report as required by the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA or,* the *Act*). We encourage you to use it to help you complete and submit your questionnaire online, especially if you are unfamiliar with it.

For your convenience:

- This workbook and guide is organized into sections corresponding to those in the online questionnaire. For help with a certain section in the questionnaire, turn to the same section in this workbook.
- Certain sections which appear in *italicized text* have been expanded to contain background information that may be helpful to you.
- All terms which appear in **bold** are defined in the **Glossary** at the back of this guide.
- The Reconciliation Chart is designed to help verify the figures in the questionnaire.

If you have specific questions that are not answered by this workbook and guide, please email **statistics.ipc@ipc.on.ca** or call the Information and Privacy Commissioner of Ontario's main switchboard **416-326-3333**. If you are calling long distance, use our toll free line: **1-800-387-0073**.

Please note incomplete questionnaires may result in your institution's submission being **partly or entirely excluded** from the statistics generated for the IPC's annual report.

All institutions must complete a questionnaire and submit it online to the Information and Privacy Commission. If no requests for access to information or requests for correction of personal information were received, your institution must still complete and submit Sections 1 and 2.

This workbook and guide is for your use in completing your questionnaire and should not be faxed or mailed to the Information and Privacy Commission in lieu of online submission. **Faxed or mailed copies of this workbook and guide will NOT be accepted.** Please submit your questionnaire online at: https://statistitics.ipc.on.ca

Institutions that do not submit a questionnaire before the deadline will be listed as such in the Information and Privacy Commissioner's Annual Report.

Thank you for your co-operation!

Section 1: Identification

1.1 Please clearly indicate the name of the institution, the name and e-mail address of the head of the institution, the name and e-mail address of the person responsible for the content of the report (the management contact), and the name, e-mail address, telephone and fax numbers and the mailing address of the person responsible for completing the report (the primary contact) should any questions arise regarding the content of the report.

1.2 Please identify the type of institution you are reporting for by checking one of the boxes provided. If the type of institution you are reporting for does not appear on the list, check *other* and specify.

Here are some examples of common types of institutions:

Corporations

The City of Kingston
The City of Oshawa
Township of Norwich
The City of Pickering
The County of Brant
The Regional Municipality of Niagara
The Town of Ingersoll
The Restructured County of Oxford
The Village of Sundridge

Commissions

Belleville Transit Commission
London Transit Commission
Oshawa Transit Commission
Niagara Transit

Boards

Athens Public Library Board
Durham District School Board
Wabigoon Local Services Board
Killaloe and District Public Library
Perth Police Services Board

Section 2: Inconsistent Use of Personal Information

What is an Inconsistent Use?

*An **inconsistent use** occurs when **personal information** from a **personal information bank** is used or disclosed differently from the way it is used on a regular basis (see Section 35 of the Act). The Act requires the institution to attach a record or notice of the **inconsistent use** or disclosure to the **personal information** involved. This record then becomes part of the **personal information** it is attached to.*

2.1 Please enter the number of times your institution made **inconsistent use** of **personal information** contained in its **personal information banks**. 0

What is Personal Information?

***Personal information** is recorded information about an identifiable individual including:*

- *the individual's address, telephone number, fingerprints or blood type;*
- *information about the individual's race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital or family status;*
- *information about the individual's educational, medical, psychological, criminal, or employment history or information concerning his or her financial transactions;*
- *any identifying number, symbol or other particular assigned to the individual;*
- *the individual's personal opinions or views except when they relate to someone else;*
- *private or confidential correspondence sent to an institution by the individual, and replies to that correspondence that would reveal the contents of the original correspondence;*
- *the views or opinions of someone else about the individual; and*
- *the individual's name when it appears with other **personal information** about that individual or when disclosure of the name would reveal other **personal information** about that individual.*

Check one:

☐	If your institution received **no requests for access** to information **or correction** of personal information please stop here and click the SAVE AND CONTINUE button at the bottom of the page to proceed to the REVIEW QUESTIONNAIRE page where you may review your questionnaire answers before you submit your report. You may make any necessary changes and/or corrections on this page then click the SAVE & CONTINUE button to update your questionnaire and proceed to the confirmation and submission page. Changes and corrections may be made any time before or after submission up to the deadline date, but must be re-confirmed and re-submitted.
☒	If your institution received (or carried forward from last year) **at least one request for access** to information, please complete the rest of the report. Click the SAVE AND CONTINUE button at the bottom of the page to proceed to the next section.
☐	If your institution only received **at least one request for correction** of personal information without any requests for access to information, please complete sections 1 ,2, and 11. Click the SAVE AND CONTINUE button at the bottom of the page to proceed to the Section 11.

Section 3: Number of Requests Completed

Please Note: *There are two types of information requests, and these need to be entered separately:*

- ***personal information*** *requests, where the requester, or authorized representative, is asking for information about himself or herself.*
- ***general records*** *requests, where the requester is asking for general information or information that includes* ***personal information*** *about someone else.*

How Are Requests Counted?

The information in this section is important to help you decide how many requests for information your institution received, since the form or letter the requester sends may actually contain a number of separate requests:

- *for* ***general records*** *requests, if the request deals entirely with one subject, it should be counted as one request. This is still the case even if the information is retrieved from different locations in your institution; or*
- *if a* ***general records*** *request deals with information about two (or more) subjects, the request should be divided into two (or more) requests; or*
- *any* ***personal information*** *request is counted as one request because it is about only one subject****,*** *the person asking for the information; or*
- *if you receive a request that must be returned to the sender for clarification, do not count this as a request received until the requester returns it to you with all the information you need to* ***complete*** *the request.*

3.1 *Enter the number of new* ***personal information*** *and* ***general records*** *requests received during the* ***reporting year*** *(January – December). This includes those requests that have been received directly by your institution and those that have been transferred in from other institutions to your institution to complete, regardless of whether or not one or more of those requests is later transferred out to another institution. On the next page is a template that you may want to use to determine the number of new requests.*

	Personal Information	General Records
New requests received directly from the requester during the **reporting year**.	4	7
Indicate the number of **personal information** and **general records** requests that were transferred to you from other institutions to be **completed** by your institution.	0	0
TOTAL NEW REQUESTS (Add the above two boxes) (reflect these totals in Box 3.1 of the statistical report)	4	7

3.2 *Enter the total number of **personal information** and **general records** requests that have been completed between January 1 to December 31 of the reporting year.*

To determine the total number of requests completed:

Add the following number of requests for personal information and general records separately:

- *new requests received during reporting year (see section 3.1 of the statistical report) and requests that were carried forward from the previous year to the current year to complete*

*Subtract the following **personal information** and **general records** requests from the above:*

- *requests transferred out to other institutions to complete; and*
- *requests carried over to the next year to complete*

*The total sum of the above calculation will result in the total numbers of **personal information** and **general records** requests that were completed for the reporting year.*

*On the next page is a worksheet to be used as a tool to determine the total number of requests for the **reporting year**.*

	Personal Information	General Records
Total new requests (copy from box 3.1).	4	7
Requests carried forward from previous year. (Enter the number of **personal information** and **general records** requests that your institution could not **complete** in the previous **reporting year**, January-December, and **carried forward** to be **completed** in the current reporting year.)	0	0
TOTAL (add the above two boxes)	**A** 4	**A** 7
Requests transferred out to other institutions to complete. (Enter the number of **personal information** and **general records** requests that were **transferred** to another institution because that institution had control or custody of the information, or a greater interest in the information.)	0	0
Requests carried over to the next year to complete. (Enter the number of **personal information** and **general records** requests your institution received that were **carried over** to the next reporting year.)	0	1
TOTAL (add the above two boxes)	**B** 0	**B** 1
TOTAL REQUESTS COMPLETED (subtract B from A) (reflect these totals in Box 3.2 of the statistical report)	4	6

Section 4: Source of Requests

4.1-4.8 Enter the number of **personal information** and **general records** requests you completed from the sources listed.

PLEASE NOTE:

Use the Individual/Public *category to capture requests made by an individual themselves and use the* Individual by Agent *category to capture requests made on behalf of individuals by a third party, such as a substitute decision-maker, lawyer, insurance adjuster, etc. If the request comes from an employee of your institution, enter the request in the* Individual/Public *category if they are requesting the information themselves or the* Individual by Agent *category if the request is being made on their behalf by a third party, such as a substitute decision-maker, lawyer, insurance adjuster, etc.*

		Personal Information	General Records
4.1	Individual/Public	2	1
4.2	Individual by Agent	1	3
4.3	Business		
4.4	Academic/Researcher		
4.5	Association/Group		
4.6	Media		1
4.7	Government (All Levels)	1	
4.8	Other		1
4.9	Add all the requests you have entered for both **personal information** and **general records** and write the totals in Box 4.9. These totals should be the same as those in Box 3.2 (**Total Requests Completed**).	4	6

Enter the numbers in the table above into boxes 4.1 through 4.9 of the online questionnaire.

Section 5: Time to Completion

5.1-5.4 Enter the number of **completed personal information** and **general records** requests in the appropriate categories. If your institution received a **transferred** request from another institution, the time to **completion** starts when the first institution received the request.

PLEASE NOTE:

1. *When locating and reviewing records, an institution may extend the time to provide a response to the requester under s.20(1). Time extension notices issued under s.20(1) allow you more than the standard 30 days in which to complete a request. If the request is completed (i.e. the access decision is issued) before the time extension period expires, the request is still considered to be compliant even though it took more than 30 days to complete it. This is known as* **extended compliance***. Please refer to the glossary and Section 6 for more information.*

2. *Section 5 deals with the absolute time to completion for requests, regardless of compliance. For example, if you issued a time extension request under s.20(1) for an additional 90 days (for a total of 120 days) and completed the request in 102 days, then you should count this request in the "91 days or longer" category. It should then be entered as compliant in part B or C in Section 6 below. Refer to Section 6 for more information.*

3. *The time from when a fee estimate/interim decision letter has been issued (s.45, O.Reg 823 s.6, s.6.1 and s.7) up to the time the deposit has been paid is not included when calculating the number of days to complete a request.*

How many requests were completed in:		**Personal Information**	**General Records**
5.1	30 days or less	4	6
5.2	31 – 60 days		
5.3	61 – 90 days		
5.4	91 days or longer		
5.5	Enter the totals of the previous entries (5.1–5.4) into this box. These totals should be equal to the **Total Requests Completed** in Box 3.2.	4	6

Enter the numbers in the table above into boxes 5.1 through 5.5 of the online questionnaire.

Section 6: Compliance with the *Act*

The Act *states that requests for access to information should be completed within 30 days. In cases where there is a need to search numerous records or to make consultations with a person outside the institution, the head of the institution can* ***extend*** *the 30-day time limit and still be in compliance with the* Act*. This can be achieved by issuing a Notice of Extension (s.20(1) and/or Notice to Affected Person (s.21(1)).*

This section has been broken down into four different situations that are mutually exclusive and will be used to determine the number of requests that are in compliance or not in compliance with the statutory time lines under the Act*.*

A. ***No*** *notices issued;*

B. ***Both*** *a Notice of Extension (s.20(1)) and a Notice to Affected Person (s.21(1)) issued;*

C. ***Only*** *a Notice of Extension (s.20(1)) issued; or*

D. ***Only*** *a Notice to Affected Person (s.21(1)) issued.*

PLEASE NOTE:

1. *The four different situations are mutually exclusive and the number of requests completed in each situation should add up to the total number of requests completed in Section 3.2. (Add boxes 6.3 + 6.6 + 6.9 + 6.12 = box 6.13) and (box 6.13* ***must equal*** *box 3.2)*

2. *Requests that require more than the statutory 30 days to complete are considered compliant if you issue a Notice of Extension under s.20(1) and/or a Notice to Affected Person under s.21(1) AND you complete the requests within the time limit specified in the Notice(s). This is known as* **extended compliance***.*

3. *Enter the number of requests in each category as follows:*

    a. *Requests where you issued NEITHER a Notice of Extension under s.20(1) NOR a Notice to Affected Person under s.21(1) should be entered in Part A.*

    b. *Requests where you issued BOTH notices should be entered in Part B (do NOT include the requests entered in Part C and Part D).*

    c. *Requests where you issued a Notice of Extension under s.20(1) ONLY (i.e. not including those requests where a Notice to Affection Person under s.21(1) was also issued) should be entered in Part C.*

    d. *Requests where you issued a Notice to Affected Person under s.21(1) ONLY (i.e. not including those requests where a Notice of Extension under s.20(1) was also issued) should be entered in Part D.*

    The sum of the requests entered in all four parts should equal Box 3.2

4. *The time taken to complete each request with notice(s) issued under s.20(1) and/or s.21(1) should be entered in Section 5 in the appropriate category according to the actual time it took to complete the request, regardless of compliance. See the example for more information.*

***Example** (for simplicity, let's assume we have only general records requests):*

Your institution completed 9 requests for access to information in the current reporting year.

Three (3) of those requests (requests a, b, and c) had neither a Notice of Extension under s.20(1) nor a Notice to Affected Person under s.21(1) issued. Two (requests a and c) were completed within the statutory 30 days and one (request b) was completed in 42 days.

On two (2) requests (requests d and e), you issued both a Notice of Extension under s.20(1) and a Notice to Affected Person under s.21(1):

- *On request d, the Notice of Extension specifies an additional 30 days to complete the request (for a total of 60 days from the date of receipt of the request). In addition, a Notice to Affected Person under s.21(1) was issued 34 days after the request was received (s.28(3)), specifying that the head will decide whether or not to disclose the record within 30 days of the Notice to Affected Person (s.28(4)(c)). The total time allowed for the completion of this request is 64 days. This request was completed in 66 days.*

- *On request e, the Notice of Extension specifies an additional 90 days to complete the request (for a total of 120 days from the date of receipt of the request). In addition, a Notice to Affected Person under s.21(1) was issued 42 days after the request was received (s.28(3)), specifying that the head will decide whether or not to disclose the record within 30 days of the Notice to Affected Person (s.28(4)(c)). The total time allowed for the completion of this request is 120 days. This request was completed in 112 days.*

On two more (2) requests (requests f and g), you issued only a Notice of Extension under s.20(1). You did not issue a Notice to Affected Person under s.21(1):

- *On request f, the Notice of Extension specifies an additional 45 days to complete the request (for a total of 75 days from the date of receipt of the request) and the request was completed in 42 days.*

- *On request g, the Notice of Extension specifies an additional 30 days to complete the request (for a total of 60 days from the date of receipt of the request) and the request was completed in 63 days.*

On two more (2) requests (requests h and i), you issued only a Notice to Affected Person under s.21(1). You did not issue a Notice of Extension under s.20(1)

- *On request h, the Notice to Affected Person was issued 12 days after the receipt of the request (for a total of 42 days from the date of receipt of the request) and the request was completed in 42 days.*

- *On request i, the Notice to Affected Person was issued 8 days after the receipt of the request (for a total of 38 days from the date of receipt of the request) and the request was completed in 40 days.*

***How to complete Section 6 for these requests**:*

- *Requests a, b and c had neither Notice Issued, so they are entered in Part A of Section 6.*
    - *Requests a and c were completed within the statutory 30 days, so they are entered in Box 6.1. They should also be included in the count of requests entered in Box 5.1 (30 days or less) in Section 5*
    - *Request b took 42 days, so it should be entered in Box 6.2. It should also be included in the count of requests entered in Box 5.2 (31 -60 days) in Section 5.*
- *Requests c and d had both Notices issued, so they are entered in Part B of Section 6.*
    - *Request d was allowed 64 days for completion, but took 66 days to complete, therefore it should be entered in Box 6.5. It should also be included in the count of requests entered in Box 5.3 (61-90 days) in Section 5.*
    - *Request e was allowed 120 days for completion, but took 112 days to complete, therefore it should be entered in Box 6.4. It should also be included in the count of requests entered in Box 5.4 (91 days or longer) in Section 5.*
- *Requests f and g had ONLY a Notice of Extension issued under s.20(1). The Notice to Affected Person under s.21(1) was NOT issued. Therefore, requests f and g are entered in Part C of Section 6.*
    - *Request f was allowed 75 days for completion, but took 42 days to complete, therefore it should be entered in Box 6.7. It should also be included in the count of requests entered in Box 5.2 (31-60 days) in Section 5.*
    - *Request g was allowed 60 days for completion, but took 63 days to complete, therefore it should be entered in Box 6.8. It should also be included in the count of requests entered in Box 5.3 (61-90 days) in Section 5.*
- *Requests h and i had ONLY a Notice to Affected Person issued under s.21(1). The Notice of Extension under s.20(1) was NOT issued. Therefore, requests h and i are entered in Part D of Section 6.*
    - *Request h was allowed 42 days for completion and took 42 days to complete, therefore it should be entered in Box 6.10. It should also be included in the count of requests entered in Box 5.2 (31-60 days) in Section 5.*
    - *Request i was allowed 38 days for completion, but took 40 days to complete,*

therefore it should be entered in Box 6.11. It should also be included in the count of requests entered in Box 5.2 (31-60 days) in Section 5.

Calculating Basic and Extended Compliance

Requests a, c, e, f and h are all considered compliant with the Act as each of them were completed within their specified time lines. Since requests a and c were completed within the statutory 30 day time limit, they have **basic compliance.** *Requests e, f and h have time lines extended beyond the 30 day time limit through the issuance of the Notice of Extension under s.20(1) and/or the Notice to Affected Person under s.21(1). Since each of requests e, f and h were completed within their respective stated time limits, they have* **extended compliance.**

The Basic Compliance rate as reported in the IPC's Annual Report is calculated for your institution by the following formula:

$$\frac{\text{Total Requests Completed in 30 Days or Less (Box 5.1)}}{\text{Total Requests Completed (Box 3.2)}} \times 100$$

The Extended Compliance rate as reported in the IPC's Annual Report is calculated for your institution by the following formula:

$$\frac{\text{Box 6.1 + Box 6.4 + Box 6.7 + Box 6.10}}{\text{Total Requests Completed (Box 3.2)}} \times 100$$

Using the above example and these formulas, the basic compliance rate is calculated as:

Box 5.1 / Box 3.2 x 100 = 2 / 9 x 100 = 22.2%

And the extended compliance rate is calculated as:

Box 6.1 + Box 6.4 + Box 6.7 + Box 6.10 / Box 3.2 x 100 = (2 + 1 + 1 + 1) / 9 x 100 = 55.6%

A. No Notices Issued

		Personal Information	General Records
6.1	Number of requests completed within the statutory time limit (30 days) where **neither** a Notice of Extension (s.20(1)) nor a Notice to Affected Person (s.21(1)) were issued.	4	6
6.2	Number of requests completed in excess of the statutory time limit (30 days) where **neither** a Notice of Extension (s.20(1)) nor a Notice to Affected Person (s.21(1)) were issued.	0	0
6.3	**Total** (Add boxes 6.1 + 6.2 = box 6.3)	4	6

►

Personal Information	General Records
4	6

B. Both a Notice of Extension (s.20(1)) and a Notice to Affected Person (s.21(1)) Issued

		Personal Information	General Records
6.4	Number of requests completed within the time limits permitted under **both** the Notice of Extension (s.20(1)) and Notice to Affected Person (s.21(1)).		
6.5	Number of requests completed in excess of the time limit permitted by the Notice of Extension (s.20(1)) and the time limit permitted by the Notice to Affected Person (s.21(1)).		
6.6	**Total** (Add boxes 6.4 + 6.5 = box 6.6)	0	0

►

Personal Information	General Records
0	0

C. Only a Notice of Extension (s.20(1)) Issued

		Personal Information	General Records
6.7	Number of requests completed within the time limit permitted under the Notice of Extension (s.20(1)).		
6.8	Number of requests completed in excess of the time limit permitted under the Notice of Extension (s.20(1)).		
6.9	**Total** (Add boxes 6.7 + 6.8 = box 6.9)	0	0

►

Personal Information	General Records
0	0

D. Only a Notice to Affected Person (s.21(1)) Issued

		Personal Information	General Records
6.10	Number of requests completed within the time limit permitted under the Notice to Affected Person (s.21(1)).		
6.11	Number of requests completed in excess of the time limit permitted under the Notice to Affected Person (s.21(1)).		
6.12	**Total** (Add boxes 6.10 + 6.11 = box 6.12)	0	0

►

Personal Information	General Records
0	0

E. Total Completed Requests (sections A to D)

		Personal Information	General Records
6.13	**Overall Total** (Add boxes (6.3 + 6.6 + 6.9 + 6.12 = box 6.13) and (box 6.13 **must equal to** box 3.2)	4	6

►

Personal Information	General Records
4	6

Enter the numbers in the tables above into the corresponding boxes in Section 6 of the online questionnaire

***Calculate your own basic compliance and extended compliance rates**:*

These calculations are for your own information only. They are not entered as part of the online questionnaire, but the total compliance rates will be calculated based on your submitted questionnaire and included in the IPC's Annual Report.

Basic Compliance Rate:

	Personal Information	***General Records***	***Total***
A: Total Requests Completed in 30 Days or Less (Box 5.1)	4	6	10
B: Total Requests Completed (Box 3.2)	4	6	10
DIVIDE: A / B x 100, round to one decimal place			100

Extended Compliance Rate:

	Personal Information	***General Records***	***Total***
A: Box 6.1 + Box 6.4 + Box 6.7 + Box 6.10			
B: Total Requests Completed (Box 3.2)			
DIVIDE: A / B x 100, round to one decimal place			

Section 6a: Contributing Factors

Write any reasons that made it difficult to meet the 30-day time limit. Also, include circumstances that will improve your ability to be in compliance with the Act.

Enter the reasons above into Section 6a of the online questionnaire

Section 7: Disposition of Requests

This section asks you to indicate how your institution dealt with each of the requests for access to information it received. The options are as follows:

7.1 ***All Information Disclosed -*** *Enter the number of* ***personal information*** *and* ***general records*** *requests that resulted in full disclosure of all information requested.*

7.2 *Disclosed in Part - Enter the number of* ***personal information*** *and* ***general records*** *requests for which the* ***head*** *of your institution disclosed only part of the information requested. Include those requests where some of the information was exempted, excluded, did not exist, was outside of the Act, i.e. Y.O.A., or frivolous or vexatious.*

7.3 *Nothing Disclosed - Enter the number of* ***personal information*** *and* ***general records*** *requests for which the* ***head*** *of your institution disclosed no information. Include those requests where all of the information was* ***exempted****, was outside of the Act, or frivolous or vexatious.*

7.4 *No Responsive Records Exist - Enter the number of personal information and general records requests for which no responsive records exist.*

7.5 *Request* ***Withdrawn -*** *or* ***Abandoned -*** *In this category enter the number of requests that were* ***withdrawn*** *or* ***abandoned*** *by the requester.*

- *A* ***withdrawn*** *request is one in which the requester notifies your institution that he or she does not wish to proceed with the request.*

- *A request is considered **abandoned** when the requester does not respond to your attempts to proceed with the request.*
    - *For **general records** the request can be considered **abandoned** if the requester does not respond to correspondence that is necessary to **complete** the request (for example, a notice of fee estimate), within 30 days of the date you sent the communication. The **head** of your institution may **extend** this time limit, and this practice is encouraged.*
    - *For **personal information** requests, the policy is to allow up to 365 days (one year) before considering the request **abandoned**.*
    - *If appropriate, consider including a "respond by" date in your correspondence when requesting a response from the requester indicating that you will consider the request abandoned if you do not hear from them on or before that date.*

*7.6 **Total Requests Processed***

*The sum of all the entries in **personal information** and **general records** for all questions 7.1 to 7.5 should be equal to or greater than the amounts in 3.2 (**Total Requests Completed**).*

		Personal Information	General Records
7.1	All information disclosed	4	3
7.2	Information disclosed in part		3
7.3	No information disclosed		
7.4	No responsive records exist		
7.5	Request withdrawn, abandoned or non-jurisdictional		
7.6	Total Requests Processed: Add Boxes 7.1 to 7.5 = Box 7.6. Box 7.6 must be greater than or equal to Box 3.2	4	6

Enter the numbers in the table above into boxes 7.1 through 7.6 of the online questionnaire.

Section 8: Exemptions and Exclusions Applied

*To complete this section you will need to be familiar with the **exemptions** described in the* Act*. Please refer to the section on **exemptions** in:*

- *your copy of the* Act*, or*
- *the **Municipal Freedom of Information and Protection of Individual Privacy Manual** produced by the Ministry of Government Services:*

  http://www.accessandprivacy.gov.on.ca/English/manual/index.html

8.1-8.19 In this section you are asked to indicate **which exemptions** were applied to those requests where the head of your institution withheld some or all of the requested information. Every request that was exempted, (in part or in full) must have at least one **exemption** listed, but may have more than one. For example, two different **exemptions** may be used to account for why information was withheld.

8.20 *If a request made under the Act also contains personal health information as defined in Section 4 of the Personal Health Information Protection Act, 2004 (PHIPA), then Section 8(1) of PHIPA may be applied to that personal health information as an **exclusion*** unless *PHIPA* specifies otherwise.

8.21 Enter the sum of all the requests you entered in the **personal information** and **general records** columns.

Please Note:

- *Section 14 **exemption**, Personal Privacy (of third party) applies only to **general records** requests.*
- *Section 38 **exemption**, Personal Information (of requester) applies only to **personal information** requests.*
- *There is no correlation between the sum entered in Box 8.21 and the total number of requests completed as entered in Box 3.2. More than one **exemption** and/or **exclusion** may be applied to a given request and a given **exemption** and/or **exclusion** may be applied to more than one request.*

For the Total Requests with Exemptions/Exclusions/Frivolous or Vexatious Requests, how many times did your institution apply each of the following? (More than one exemption may be applied to each request.)

		Personal Information	General Records
8.1	Section 6 — Draft Bylaws, etc.		
8.2	Section 7 — Advice or Recommendations		
8.3	Section 8 — Law Enforcement[1]		
8.4	Section 8(3) — Refusal to Confirm or Deny		
8.5	Section 8.1 — *Civil Remedies Act, 2001*		
8.6	Section 8.2 — *Prohibiting Profiting from Recounting Crimes Act, 2002*		
8.7	Section 9 — Relations with Governments		
8.8	Section 10 — Third Party Information		
8.9	Section 11 — Economic/Other Interests		
8.10	Section 12 — Solicitor-Client Privilege		
8.11	Section 13 — Danger to Safety or Health		
8.12	Section 14 — Personal Privacy (Third Party)[2]	N/A	3
8.13	Section 14(5) — Refusal to Confirm or Deny		
8.14	Section 15 — Information Soon to be Published		
8.15	Section 20.1 — Frivolous or Vexatious		
8.16	Section 38 — Personal Information (Requester)		N/A
8.17	Section 52(2) — Act Does Not Apply[3]		
8.18	Section 52(3) — Labour Relations & Employment Related Records		
8.19	Section 53 — Other Acts		

8.20	*PHIPA* Section 8(1) applies		
8.21	**TOTAL EXEMPTIONS** (Add boxes 8.1 to 8.20 = box 8.21)	0	3

Enter the numbers in the table above into boxes 8.1 through 8.24 of the online questionnaire.

[1] not including Section 8(3)
[2] not including Section 14(5)
[3] not including Section 52(3)

Section 9: Fees

*This section concerns **additional fees** and **application fees**.*

		Personal Information	General Records	TOTAL
9.1	Number of requests where fees other than application fees were collected		1	1
9.2.1	Application fees collected	$	$ 20	$ 20
9.2.2	Additional fees collected	$	$ 570	$ 570
9.2.3	Total Fees (Add boxes 9.2.1 + 9.2.2 = box 9.2.3)	$	$ 590	$ 590
	*Under certain conditions, the **head** of your institution may **waive** all or part of the additional fees being charged. These conditions include: the requesters' ability to pay, whether release of the information will benefit public health or safety, how much difference there is between the fee being charged and the actual cost of processing the request, and whether the requester is ultimately given access to the information requested.*			
9.3	Total dollar amount of fees waived	$ 0	$ 0	$ 0

Enter the numbers in the table above into boxes 9.1 through 9.3 of the online questionnaire.

Section 10: Reasons for Additional Fee Collection

This section concerns the reasons and the number of requests involved for the additional fee collection.

*If your institution collected **additional** fees for any requests, please enter the appropriate number of requests in the given categories to indicate why the fee was charged. A request can be entered into more than one category. For example, an institution may have charged $10 to process a request, $5 to reproduction costs and $5 to shipping costs.*

Please Note:

- ***additional fees** for **personal information** requests can only be charged for reproduction and computer costs.*

		Personal Information	General Records	TOTAL
10.1	Search time	N/A	360	360
10.2	Reproduction			
10.3	Preparation	N/A	210	210
10.4	Shipping	N/A		
10.5	Computer costs			
10.6	Invoice costs (and others as permitted by regulation)	N/A		
10.7	Total (Add boxes 10.1 to 10.6 = box 10.7 and Box 10.7 greater than or equal to Box 9.1)		570	570

Enter the numbers in the table above into boxes 10.1 through 10.7 of the online questionnaire.

Section 11: Corrections and Statements of Disagreement

*If a person believes that an institution has **personal information** about himself/herself that is incorrect, under the* Act*, that person has the right to:*

- *request that the institution **correct** the information,*
- *require that the institution attach a statement of disagreement to the information if the requested **corrections** were not made,*
- *require that any person or organization to whom the **personal information** has been disclosed within the last 365 days be notified of the **corrections** or statement of disagreement.*

		Personal Information
11.1	Number of new correction requests received	
11.2	ADD: Correction requests carried forward from the previous year	
11.3	SUBTRACT: Correction requests carried over to the next year	
11.4	Total Correction Requests Completed [(Box 11.1 + Box 11.2) – Box 11.3 = Box 11.4] Box 11.4 must equal Box 11.9 If this number is zero, skip the rest of this section.	0

*If your institution received any requests for **correction** of **personal information**, what course of action was taken with each?*

		Personal Information
11.5	Correction(s) made in whole	
11.6	Correction(s) made in part	
11.7	Correction requests refused	
11.8	Correction requests withdrawn by requester	
11.9	Total (Add Boxes 11.5 to 11.8 = Box 11.9 and Box 11.9 must equal Box 11.4)	0

In cases where correction requests were denied, in part or in full, were any statements of disagreement attached to the affected personal information?

11.10 Number of statements of disagreement attached: 0

If your institution received any requests to correct personal information, the *Act* requires that you send any person(s) or body who had access to that information in the previous year notification of either the correction or the statement of disagreement. Enter the number of notifications sent, if applicable.

11.11 Number of notifications sent: 0

Enter the numbers in the tables above into boxes 11.1 through 11.11 of the online questionnaire.

Completing and Submitting Your Questionnaire

This workbook and guide is for your use in completing your report and should not be faxed or mailed to the Information and Privacy Commissioner in lieu of online submission. **Faxed or mailed copies of this workbook and guide will NOT be accepted.** Please submit your report online at: https://statistics.ipc.on.ca

Your institution should have a login id and password for the Online Statistical Reporting System. If you have lost or forgotten them, you may request them via an email to statistics.ipc@ipc.on.ca indicating your institution name.

New Institutions

If your institution has recently come under the jurisdiction of the *Municipal Freedom of Information and Protection of Privacy Act*, you are required to submit a statistical report annually to the IPC using the Online Statistical Reporting System at https://statistics.ipc.on.ca for which you will need a login id and a password. Please request them via an email to statistics.ipc@ipc.on.ca and include the following:

- the name of your institution
- the name and e-mail address of the head of the institution
- the name and e-mail address of the person responsible for the content of the report (the management contact)
- the name, e-mail address, telephone and fax numbers and the mailing address of the person responsible for completing the report (the primary contact**)**

- your language preference (English or Français)

- Please indicate if your institution is also a Health Information Custodian (HIC) as defined in Section 3 of the *Personal Health Information Protection Act* (*PHIPA*). Institutions under *MFIPPA* who are also HICs under *PHIPA* must submit one annual statistical report under *MFIPPA* and another report under *PHIPA*. As such, you have the option of a single login id and password to submit both reports (which is convenient if the same person will be submitting both reports) or you may wish to have one login id and password for *MFIPPA* and another for *PHIPA* (which makes it easier if two different people will submit the reports) – it all depends on your organizational structure. Please indicate whether you want a single login id and password set or two separate ones.

Once you have your login id and password and have completed this workbook, log on to the Online Statistical Reporting System at https://statistics.ipc.on.ca and enter your questionnaire data section by section. You may log off the system at any time and it will remember where you left off when you log on the next time. This means you do not have to complete and submit your questionnaire all in one session as long as you do complete and submit it before the deadline date **The Online Statistical Reporting System will not be available after the deadline date**.

When you have completed entering your questionnaire, the system allows you to review your answers and make any necessary corrections before confirming and submitting your questionnaire. Once you have confirmed and submitted your questionnaire you are done, but should you discover that a correction is necessary after you have confirmed and submitted your questionnaire, you may log on to the Online Statistical Reporting System at any time before the deadline date and make the correction as needed. You will need to re-confirm your questionnaire and submit it again in order for the correction to be applied.

Changes to the type of questionnaire submitted may be made in the same manner. If, for example, you originally submitted a questionnaire stating that you had received no requests for access or correction (a “zero report”), but then discovered that you indeed had received one or more such requests, you may log on to the Online Statistical Reporting System at any time before the deadline date and simply change the questionnaire type selection at the end of Section 2. The system will take care of the rest and will take you to the appropriate sections of the questionnaire so you may complete them. Again, you will need to re-confirm your completed questionnaire and submit it again in order for the correction to be applied.

If you have specific questions that are not answered by this workbook and guide, please email **statistics.ipc@ipc.on.ca** or call the Information and Privacy Commissioner of Ontario’s main switchboard **416-326-3333**. If you are calling long distance, use our toll free line: **1-800-387-0073**.

Glossary of Terms

Compliance Rate, Basic – This is the percentage of all requests completed within the reporting year that were completed within the statutory 30 day completion time limit

Compliance Rate, Extended – Sections 20(1) and 21(1) of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) allow for the statutory 30 day completion time limit to be extended to accommodate large and/or complex requests and/or allow affected persons to provide representations regarding the disclosure of the requested information by the issuance of a Notice of Extension (s.20(1)) and/or a Notice to Affected Person (s.21(1)). The Extended Compliance Rate is the percentage of all requests completed within the reporting year that were completed either within the statutory 30 day completion time limit (where no notice(s) were issued) or within the time limit specified in the notice. See also Notice of Extension and Notice to Affected Person, below.

Exclusion (Exclude, Excluded) - Something is excluded from being regulated by the *Act* because it is being regulated elsewhere by a different law.

Exemption (Exempt, Exempted) - An exemption is a specific provision in the Act that may be invoked by a head as justification for denying access to information, in whole or in part. Certain requests for access may be denied due to provisions of other Acts, and in these special cases, for purposes of the year-end statistical report, Section 53(2) (Other Acts) is the relevant exemption.

Exemption, Frivolous or Vexatious - A exemption is frivolous or vexatious when the head considers the request:

- as abusing the right of access or interferring with the operation of the institution, or
- to be made in bad faith or for ulterior motives.

Fee, Additional - See *Municipal Freedom of Information and Protection of Privacy Act*, s.45 (1).

Fee, Application - See *Municipal Freedom of Information and Protection of Privacy Act*, s.17 (1)(c).

Fee, Waived - A head may waive all or part of a fee that was estimated for releasing general records information, taking into account factors including: the requester's ability to pay; whether release of the information will benefit public health or safety; how much difference there is between the fee being charged and the actual cost of processing the request; and whether the requester is ultimately given access to the information requested.

Head (of institution) - The head is the individual or body selected to be the head of the institution

for the purposes of the Act by:

- the council of a municipal corporation, or by
- the members of a board, commission or other institution that is not a municipal corporation.

The head is responsible for decisions made under the legislation on behalf of the institution and for overseeing the administration of the legislation within the institution. The head may delegate some or all of its powers and duties to an officer or officers of the institution, or another institution. In this case the head is still accountable for all decisions made and actions taken under the Act.

Inconsistent Use - (of personal information) - An inconsistent use occurs whenever an institution under the Municipal Freedom of Information and Protection of Privacy Act (the Act) uses or discloses personal information from its personal information banks differently from the way this information is used or disclosed on a regular basis.

Notice of Extension - A notice sent to a requester by the head that a time extension is needed in order to complete the request. The notice must inform the requester of:

- the length of the extension,
- the reason for the extension, and
- the fact that the requester can ask the Information and Privacy Commissioner/Ontario to review the decision to extend the time period.

The extension may be made only if numerous records must be searched or consultation with a person outside the institution is required.

Notice to Affected Person - A notice sent by the head to a third party to whom the information relates before releasing the information. The notice must inform the third party of:

- the head's intention to disclose information that has something to do with the third party,
- a description of what's in the record or the part of the record that relates to the third party, and
- the fact that the third party has twenty days after the notice is given to advise the head why part or the whole record should not be disclosed.

Personal Information - See Section 2.1 of the Guide.

Personal Information Banks - A personal information bank is any collection of personal information your institution retains that is:

- organized, and
- allows personal information about an identifiable individual to be retrieved by that individual's name or some other personal identifier.

Personal information banks can be:

- about members of the public or employees of the reporting institution,
- recorded on computer disks, paper, fiche or other media.

Examples of Personal Information Banks

Death Register; Dog Owners Records; Employee Training Records; Family Counselling Client Records; General Welfare Assistance Client Files; Grievance Files; Hunting/Fishing Licence Application; Line Fence Viewing Files; Litigation Files (Legal Departments); Marriage Licence Applications; Municipal Seasonal Boaters Index; Tax Bill Records; Job Competition Files; Applications Workplace Safety Insurance Board Files

Reporting Year - January to December.

Request, Abandoned - A request that an institution has been unable to proceed with because the requester has not responded to communications necessary to process the request (for example, a notice of fee estimate). This does not include requests returned to the requester due to insufficient detail.

Request, Carried Forward From Previous Year (requests for access to information and correction) - A request received in, or carried over from the previous reporting year that had to be carried forward to the current year for completion.

Request, Carried Over to Next Year (requests for access to information and correction) - A request received in the current reporting year that had to be carried forward to the next year for completion.

Request, Completed (requests for access to information and correction) (Complete) - A request for which the head's decision (to grant/deny access, or to make/refuse corrections) has been communicated to the requester, or a request that has been formally withdrawn or abandoned by the requester.

Request, Correction - A request to have one's own personal information corrected following access to the information.

Request, Disposition of - The outcome of a completed request: information disclosed/denied, request abandoned/withdrawn.

Request, General Records - A request for access to general records information or to another person's personal information (where permission has been given).

Request, Personal Information - A request for access to personal information, made by the person to whom the information relates or their authorized representative.

Request, Transferred - A request for access to general records or personal information that

has been sent from one institution to another; the second institution having custody, control or a greater interest in the information. If Institution A receives a request that is transferred (in whole) to Institution B, Institution A would count this as a "Request Transferred Out to Another Institution", while Institution B would count it as a "Request Transferred In From Another Institution".

Request, Withdrawn - A request for which the head has been informed by the requester that he/she no longer wishes to continue with the request (prior to its completion).

Reconciliation Chart

The chart below should be used to help verify your figures in completing this workbook and entering your questionnaire on the Online Statistical Reporting System.

Box Number	Criteria *	Box Number(s)
4.9	=	4.1 to 4.8
4.9	=	3.2
5.5	=	5.1 to 5.4
5.5	=	3.2
6.3	=	6.1+6.2
6.6	=	6.4+6.5
6.9	=	6.7+6.8
6.12	=	6.10+6.11
6.13	=	6.3+6.6+6.9+6.12
6.13	=	3.2
7.6	=	7.1 to 7.5
7.6	=	3.2
8.21	=	8.1 to 8.20
9.1	= or <	10.7
9.2.3	=	9.2.1+9.2.2
10.7	=	10.1 to 10.6
10.7	= or >	9.1
11.4	=	(11.1+11.2)-11.3
11.4	=	11.9
11.9	=	11.5 to 11.8
11.9	=	11.4

* = equal to
> greater than
< less than

MIDDLESEX-LONDON HEALTH UNIT

REPORT NO. 04-22GC

TO: Chair and Members of the Governance Committee

FROM: Emily William, CEO

DATE: 2022 February 17

MLHU RISK MANAGEMENT PLAN

Recommendation

It is recommended that the Governance Committee recommend that the Board of Health:

1) ***Receive Report No. 04-22GC re: "MLHU Risk Management Plan" for information;***
2) ***Approve the new Middlesex-London Health Unit Risk Management Plan (Appendix A) and Risk Register (Appendix B).***

Key Points

- Boards of Health are required to report to the Ministry of Health in a standardized manner the high risks that are currently being managed at each board of health. The proposed Risk Management Plan remains in alignment with board of health requirements under the Ontario Public Health Standards (OPHS) and the approved Middlesex-London Health Unit (MLHU) Risk Management Policy (G-120).
- Gaps have been identified in the current risk reporting process and an updated Risk Management Plan (Appendix A) and Risk Register (Appendix B) have been developed.
- The Risk Register (Appendix B) is a repository for all risks identified (high, medium and low) and includes additional information about each risk (priority rating, mitigation strategies, and residual risk).
- Actions taken to reduce risk are monitored and efforts to improve performance will now be reported to the Board on a quarterly basis.

Background

In January 2018, the Ministry of Health and Long-Term Care implemented modernized Ontario Public Health Standards (OPHS) and introduced new accountability and reporting tools required under the Public Health Accountability Framework.

The OPHS require boards of health to have a formal risk management framework in place that identifies, assesses, and addresses risks. All boards of health are required to submit a Risk Management Report as part of their Q3 Standards Activity Report (SAR) on an annual basis. At its meeting on December 9, 2021, the Board of Health approved the 2021 Risk Management Report which summarized high risks and key mitigation strategies to be submitted to the Ministry.

Risk Management Reporting

Risk assessment and mitigation occurs at the organization, program, and project levels according to the process outlined in the approved MLHU Risk Management Policy (G-120). The Board of Health is kept informed of identified high risks and key mitigation strategies on an annual basis as detailed on the annual Risk Management Report.

The following gaps have been identified in the current risk reporting process:

1. Medium to low risks faced by the organization are not captured on the Risk Management report.
2. Monitoring the effectiveness of the mitigation strategies on an annual basis limits the ability of the Health Unit and the Board of Health to determine the level of residual risk faced by the organization.

MLHU Risk Management Plan

An updated MLHU Risk Management Plan (Appendix A) has been developed to address the current gaps in the risk reporting process. This plan includes a new Risk Register (Appendix B) that is a repository for all risks identified (high, medium and low) and includes additional information about each risk (priority rating, mitigation strategies, and residual risk).

The risk register captures MLHU's response to actions taken to address risks and includes the assignment of responsibility. Actions taken to reduce risk are monitored and efforts to improve performance will now be reported to the Board on a quarterly basis.

Next Steps

The Governance Committee has the opportunity to review the MLHU Risk Management Plan (Appendix A) and the Risk Register (Appendix B) included with this report. Once the Governance Committee is satisfied with its review, the Risk Management Plan will be forwarded to the Board of Health for approval.

This report was prepared by the Manager, Strategy, Risk and Privacy, Healthy Organization division.

Emily Williams, BScN, RN, MBA, CHE
Chief Executive Officer

BUREAU DE SANTÉ DE MIDDLESEX-LONDON HEALTH UNIT
www.healthunit.com

Risk Management Plan

Middlesex-London Health Unit
February 17, 2022

Presented By:

Kendra Ramer
Manager, Strategy, Risk and Privacy

Overview

The **Risk Management Plan** identifies emerging issues and potential threats that may impact the achievement of established organizational objectives that are documented on the **Risk Register**. The risk management process includes assessing the impact and likelihood of those risks and evaluating the mitigation strategies in place to manage those risks. Risk mitigation involves the implementation of controls that are monitored on a quarterly basis to determine the level of **residual risk** faced by the organization.

The organization's response to actions taken to address risks includes the assignment of responsibility. Reporting results of actions taken to reduce risk and efforts to improve performance are provided as at the reporting date.

MLHU has adopted the Ontario Public Service Risk Management Framework outlined in MLHU Policy G-120 Risk Management.

DEFINITIONS

"Control/Mitigation Strategy" reduce the negative risks or increase opportunities.

"Risk Register" is a risk management tool that is a repository for all risks identified and includes additional information about each risk (priority rating, mitigation strategies, assigned owner).

"Risk Management" is the process of identifying, assessing and controlling threats to an organization.

"Risk Management Plan" is a document that details the MLHU risk management process and includes the organization's risk register and associated risk matrix.

"Risk Matrix" is used to define the level of risk by considering the impact and likelihood of the risk and assigning a priority rating.

"Risk Tolerance" is the amount of risk that the organization being assessed can manage.

"Residual Risk" is the amount of risk associated with an issue or threat remaining after the risk has been reduced by mitigation/controls.

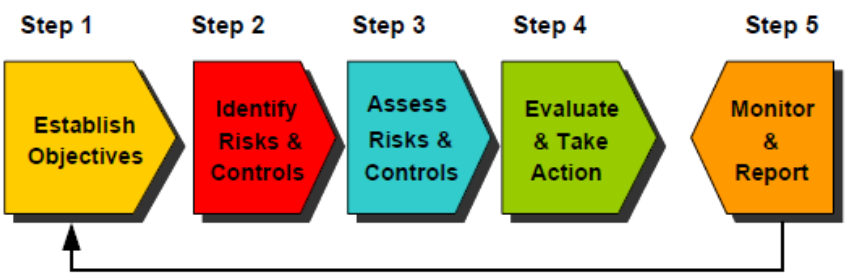
Risk Categories

The MLHU Risk Register addresses the following risk categories:

Financial	Operational or Service Delivery	Strategic/Policy
Uncertainty around obtaining, committing, using, losing economic resources or not meeting overall financial budgets/commitments.	Uncertainty regarding activities performed in carrying out the entity's strategies or how the entity delivers services.	Uncertainty around strategies and policies achieving required results; or that old and/or new policies, directives, guidelines, legislation, processes, systems, and procedures fail to recognize and adapt to changes.
Stakeholder/Public Perception	**People/Human Resources**	**Legal Compliance**
Uncertainty around managing the expectations of the public, other governments, Ministries, or other stakeholders and the media to prevent disruption or criticism of the service and a negative public image.	Uncertainty as to the capacity of the entity to attract, develop and retain the talent needed to meet the objectives.	Uncertainty regarding compliance with laws, regulations, standards, policies, directives, contracts, MOU's and the risk of litigation.
Security	**Information/Knowledge**	**Governance/Organizational**
Uncertainty relating to breaches in physical or logical access to data and locations (offices, warehouses, labs, etc.)	Uncertainty regarding access to, or use of, inaccurate, incomplete, obsolete, irrelevant or untimely information, unreliable information systems; inaccurate or misleading reporting.	Uncertainty about maintenance or development of appropriate accountability and control mechanisms such as organizational structures and systems processes; systemic issues, culture and values, organizational capacity, commitment and learning and management systems, etc.
Political	**Technology**	**Privacy**
Uncertainty that events may arise from or impact the Minister's Office/Ministry, e.g. a change in government, political priorities, or policy direction.	Uncertainty regarding alignment of IT infrastructure with technology and business requirements; availability of technological resources.	Uncertainty with regards to exposure of personal information or data; fraud o identity theft; unauthorized data.
Environmental	**Equity**	
Uncertainty usually due to the external risks facing an organization including air, water, earth, forests. An example of an environment, ecological risk would be the possible occurrence of a natural disaster and its impact on an organization's operations.	Uncertainty that policies, programs or services will have a disproportionate impact on the population.	

Ontario Public Service Risk Management Framework

The risk management process



Step 1: Establish objectives

- Risks must be assessed and prioritized in relation to an objective
- Objectives can be at any level; operational, program, initiative, unit, branch, health system
- Each objective can be general or can include specific goals, key milestones, deliverables and commitments

Step 2: Identify risks & controls

Identify risks - What could go wrong?

- Consider each category of risk
- Obtain available evidence
- Brainstorm with colleagues and/or stakeholders
- Examine trends and consider past risk events
- Obtain information from similar organizations or projects
- Increase awareness of new initiatives/ agendas and regulations

Identify existing controls – What do you already have in place?

- Preventive controls
- Detective controls
- Recovery / Corrective controls

Step 3: Assess Risks & Controls

Assess inherent risks

- *Inherent likelihood* – Without any mitigation, how likely is this risk?
- *Inherent impact* – Without any mitigation, how big will be the impact of the risk on your objective?

Assess controls

- Evaluate possible preventive, detective, or corrective mitigation strategies.

Reassess residual risks

- Re-assess the impact, likelihood and proximity of the risk with mitigation strategies in place.
- *Residual likelihood* – With mitigation strategies in place, how likely is this risk?
- *Residual impact* – With mitigation strategies in place, how big an impact will this risk have on your objective?

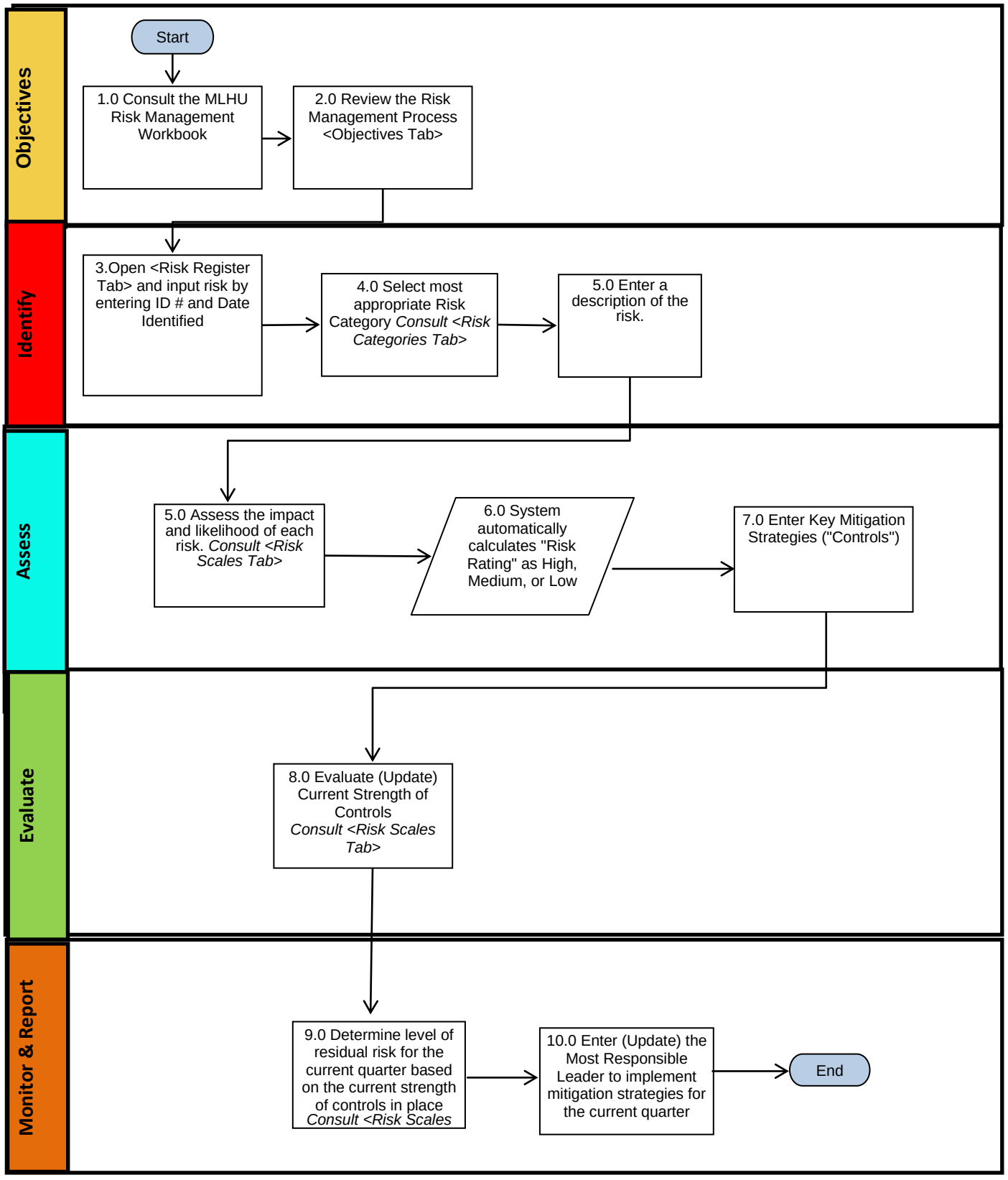
Step 4: Evaluate & Take Action

- Identify risk owners.
- Identify control owners.
- Have mitigation strategies reduced the risk rating (Impact x Likelihood) enough that the risk is below approved risk tolerance levels?
- Do you need to implement further mitigation strategies?
- Develop SMART (Specific, Measurable, Achievable, Realistic, Time-specific) actions that will either reduce the likelihood of the risks or minimise the impact.
- Develop detailed action plans with timelines, responsibilities and outline deliveries.

Step 5: Monitor & Report

- Have processes in place to review risk levels and risk mitigation strategies as appropriate.
- Monitor and update by asking:
  - Have risks changed? How?
  - Are there new risks? Assess them
  - Do you need to report or escalate risks? To whom? When? How?
- Develop and monitor risk indicators

MLHU Risk Management Process



MLHU Risk Register

IDENTIFY				ASSESS				EVALUATE		MONITOR & REPORT					Comments
ID	Date Identified	Risk Category	Risk Description	Impact (1-5)	Likelihood (1-5)	Risk Rating (H,M,L)	Key Mitigation Strategies ("Controls")	Actions Taken	Current Strength of Controls	Q1 Residual Risk	Q2 Residual Risk	Q3 Residual Risk	Q4 Residual Risk	Most Responsible Leader	Comments

Risk Matrix

Risk Priority Risk Map

Risk Matrix Interpretation

Risk maps provide an effective, means of identifying and prioritizing risks. Risks with a high Probability, and a medium to high Impact are the highest priority, however risk strategies should be developed to deal with all identified risks.

Impact	5 Threatens the success of the project					
	4 Substantial Impact on time, cost or quality					
	3 Notable impact on time, cost or quality					
	2 Minor impact on time, cost or quality					
	1 Negligible impact					
	Ranking	1 Unlikely to occur	2 May occur occasionally	3 Is as likely as not to occur	4 Is likely to occur	5 Is almost certain to occur
		Likelihood				

Legend	
	High Risk Priority
	Medium Risk Priority
	Low Risk Priority

Risk Scales

Risk Rating Scale:

VALUE	LIKELIHOOD	IMPACT	SCALE
1	Unlikely to occur	Negligible Impact	Very Low
2	May occur occasionally	Minor impact on time, cost or quality	Low
3	Is as likely as not to occur	Notable impact on time, cost or quality	Medium
4	Is likely to occur	Substantial impact on time, cost or quality	High
5	Is almost certain to occur	Threatens the success of the project	Very High

Current Strength of Controls Scale:

SCORE	RANK	PRESENSE OF CONTROL	EFFECTIVENESS	RESIDUAL RISK
0	Not able to rate	There are no controls in place to assign a rating		Significant
1	Very ineffective (Virtually no controls)	Very few, if any, controls are in place	Controls are ineffective at mitigating the risk	Significant
2	Ineffective (Low control effectiveness)	Limited controls are in place	Only a limited number of the controls are effective	Moderate
3	Partly effective (Moderate control effectiveness)	A moderate number of controls are in place	The controls are adequate at mitigating part of the risk	Moderate
4	Effective (High control effectiveness)	The majority of controls are in place	The controls mitigate the majority of the risk	Minor
5	Very effective (Very high control effectiveness)	Nearly all of the required controls are in place	The controls are effective at mitigating the risk	Minor

Residual Risk:

RESIDUAL RISK	DESCRIPTION
Significant	Represents the highest residual risk exposure as the assessed level of risk control effectiveness is insufficient for the level of risk. Management should consider improving risk control plans for these risks.
Moderate	Represents additional residual risk exposure that could be investigated further as the assessed risk control effectiveness is not propitiate with the level of risk. Control plans should be documented and reviewed or appropriateness.
Minor	Areas where the risk control effectiveness is proportionate with the level of risk.

RISK MANAGEMENT POLICY

PURPOSE

To ensure that an appropriate and effective risk management process is in place to monitor and respond to emerging issues and potential threats from both internal and external sources, to the Middlesex-London Health Unit (MLHU).

POLICY

MLHU engages in a wide range of activities in its facilities and in the community, all of which are subject to some level of risk. It is the policy of MLHU to:

- Embed risk management into the culture and operations of MLHU;
- Integrate risk management into strategic planning, program planning, performance management and resource allocation decisions;
- Manage threats and leverage opportunities as appropriate and in accordance with best practices;
- Re-assess regularly and report on MLHU's risks and the effectiveness of existing risk mitigation strategies to the Board;
- Anticipate and respond to changing social, environmental and legislative requirements;
- Support the development of risk management competencies across the organization and,
- Encourage all staff to report risks and to ensure that no person, who in good faith reports a risk, is subjected to any form of retribution, retaliation or reprisal.

In accordance with the requirements set out in the Ontario Public Health Standards, the Board of Health shall be responsible for providing risk oversight and ensuring a formal risk management framework that identifies, assesses and addresses risks, is in place. The Board shall obtain an understanding of the risks inherent in the organization's strategies and shall monitor and provide advice to management regarding critical risk issues. The Board shall also identify categories of risk, provide direction on the extent/range to which these are acceptable and define the scope and frequency of risk management reporting.

MLHU has adopted the Ontario Public Service Risk Management Framework (Appendix A), which includes the following steps:

1. Establish objectives
2. Identify risks and controls
3. Assess risks and controls
4. Evaluate and take action
5. Monitor and report

Management shall ensure that policies are carried out and processes are executed in accordance with objectives and identified risk tolerances, as well as actively embrace an integrated approach to risk management, sharing risk information transparently throughout the agency and promoting a culture in which risk management permeates all levels of the organization.

The Medical Officer of Health and Chief Executive Officer shall have overall responsibility for risk management, ensuring both the effective execution of the organization's risk management framework and processes, and that all significant risks are addressed. The Director, Healthy Organization shall be responsible for the development, implementation, and review of a systematic risk management process.

APPENDICES

G-120 App A – MLHU Risk Management Framework

APPLICABLE LEGISLATION AND STANDARDS

Ontario Public Health Standards: Requirements for Programs, Services, and Accountability, 2018

RISK MANAGEMENT PLAN

Area:	
Date:	
Version:	

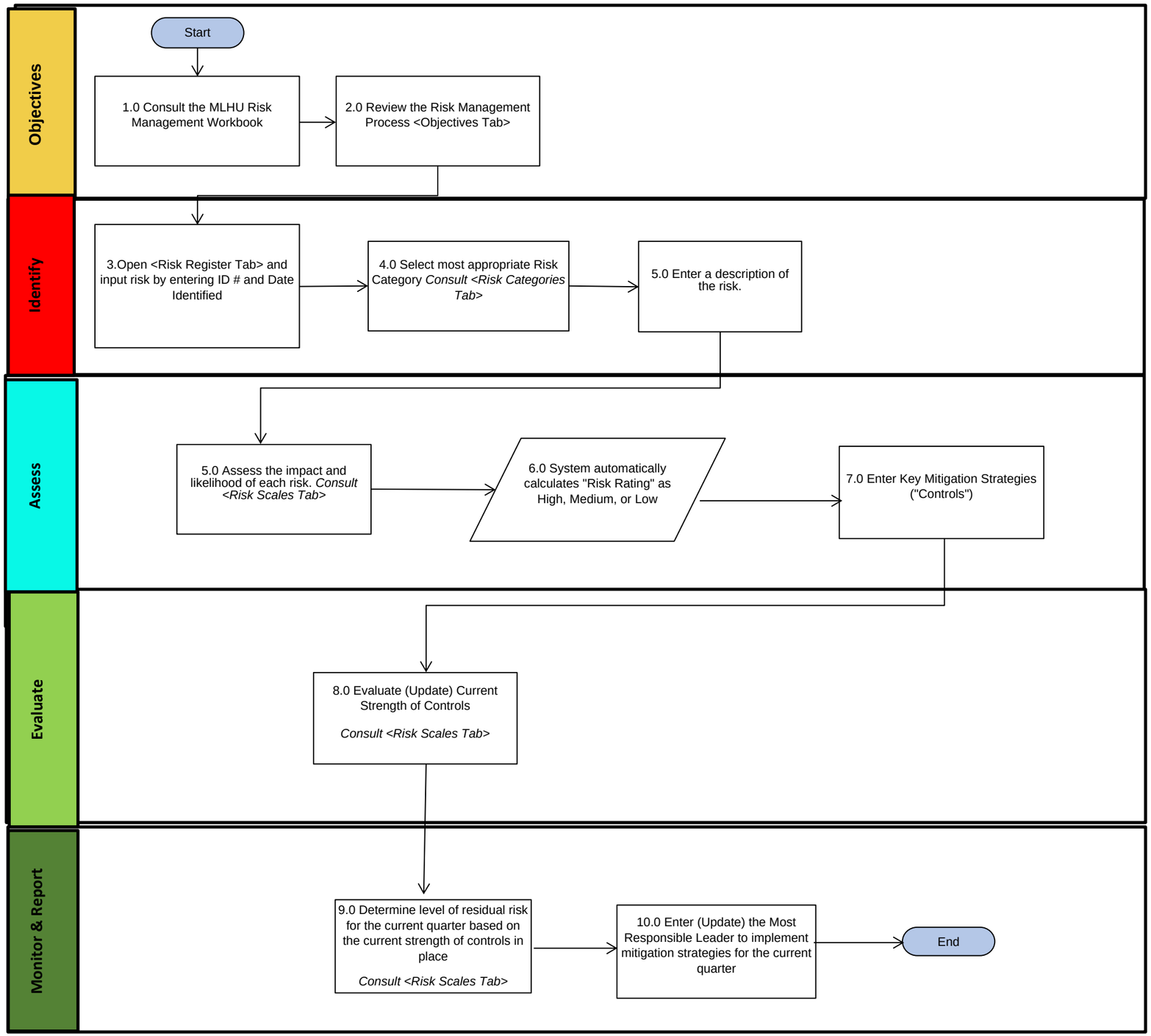
Purpose:	*This tool is designed to identify, assess and evaluate the risks facing MLHU and provide a comprehensive report on a quarterly basis.*

Background:	*This tool is designed to create a risk register that is consistent with the annual Standard Activity Report that is submitted annually to the Ministry.*

Workbook Index

Worksheet Name	Description
Overview	This worksheet provides the overview of the project and a table of contents to navigate the workbook.
Instructions	This worksheet provides users with the instructions for using this workbook. This tab should be reviewed prior to executing the risk assessment workbook. A process flowchart and detailed user guide are included.
Risk Categories	This worksheet provides the definitions of the risk categories used to identify risks.
Objectives	This worksheet highlights the risk management process.
Risk Register	This worksheet is used to identify potential risk categories, assess risks and mitigation strategies, evaluate strenth of controls, monitor and report residual risks on a quarterly basis.
Risk Matrix	This worksheet displays the results of the risk assessment into graphics for reporting and decision making purposes.
Risk Charts	This worksheet displays the results of the risk assessment into summary tables and charts.
Risk Scales	This worksheet provides the ranking models used to conduct the risk assessment.
Reference	This worksheet displays the drop down lists utilized in the risk register.

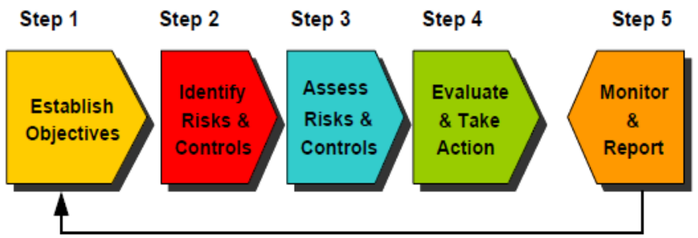
The MLHU Risk Management Process



RISK CATEGORIES

Financial	Operational or Service Delivery	Strategic/Policy
Uncertainty around obtaining, committing, using, losing economic resources or not meeting overall financial budgets/commitments.	Uncertainty regarding activities performed in carrying out the entity's strategies or how the entity delivers services.	Uncertainty around strategies and policies achieving required results; or that old and/or new policies, directives, guidelines, legislation, processes, systems, and procedures fail to recognize and adapt to changes.
Stakeholder/Public Perception	**People/Human Resources**	**Legal Compliance**
Uncertainty around managing the expectations of the public, other governments, Ministries, or other stakeholders and the media to prevent disruption or criticism of the service and a negative public image.	Uncertainty as to the capacity of the entity to attract, develop and retain the talent needed to meet the objectives.	Uncertainty regarding compliance with laws, regulations, standards, policies, directives, contracts, MOU's and the risk of litigation.
Security	**Information/Knowledge**	**Governance/Organizational**
Uncertainty relating to breaches in physical or logical access to data and locations (offices, warehouses, labs, etc.)	Uncertainty regarding access to, or use of, inaccurate, incomplete, obsolete, irrelevant or untimely information, unreliable information systems; inaccurate or misleading reporting.	Uncertainty about maintenance or development of appropriate accountability and control mechanisms such as organizational structures and systems processes; systemic issues, culture and values, organizational capacity, commitment and learning and management systems, etc.
Political	**Technology**	**Privacy**
Uncertainty that events may arise from or impact the Minister's Office/Ministry, e.g. a change in government, political priorities, or policy direction.	Uncertainty regarding alignment of IT infrastructure with technology and business requirements; availability of technological resources.	Uncertainty with regards to exposure of personal information or data; fraud o identity theft; unauthorized data.
Environmental	**Equity**	
Uncertainty usually due to the external risks facing an organization including air, water, earth, forests. An example of an environment, ecological risk would be the possible occurrence of a natural disaster and its impact on an organization's operations.	Uncertainty that policies, programs or services will have a disproportionate impact on the population.	

The risk management process



Step 1: Establish objectives

- Risks must be assessed and prioritized in relation to an objective
- Objectives can be at any level; operational, program, initiative, unit, branch, health system
- Each objective can be general or can include specific goals, key milestones, deliverables and commitments

Step 2: Identify risks & controls

Identify risks - What could go wrong?

- Consider each category of risk
- Obtain available evidence
- Brainstorm with colleagues and/or stakeholders
- Examine trends and consider past risk events
- Obtain information from similar organizations or projects
- Increase awareness of new initiatives/ agendas and regulations

Identify existing controls – What do you already have in place?

- Preventive controls
- Detective controls
- Recovery / Corrective controls

Step 3: Assess Risks & Controls

Assess inherent risks

- *Inherent likelihood* – Without any mitigation, how likely is this risk?
- *Inherent impact* – Without any mitigation, how big will be the impact of the risk on your objective?

Assess controls

- Evaluate possible preventive, detective, or corrective mitigation strategies.

Reassess residual risks

- Re-assess the impact, likelihood and proximity of the risk with mitigation strategies in place.
- *Residual likelihood* – With mitigation strategies in place, how likely is this risk?
- *Residual impact* – With mitigation strategies in place, how big an impact will this risk have on your objective?

Step 4: Evaluate & Take Action

- Identify risk owners.
- Identify control owners.
- Have mitigation strategies reduced the risk rating (Impact x Likelihood) enough that the risk is below approved risk tolerance levels?
- Do you need to implement further mitigation strategies?
- Develop SMART (Specific, Measurable, Achievable, Realistic, Time-specific) actions that will either reduce the likelihood of the risks or minimise the impact.
- Develop detailed action plans with timelines, responsibilities and outline deliveries.

Step 5: Monitor & Report

- Have processes in place to review risk levels and risk mitigation strategies as appropriate.
- Monitor and update by asking:
  - Have risks changed? How?
  - Are there new risks? Assess them
  - Do you need to report or escalate risks? To whom? When? How?
- Develop and monitor risk indicators

Risk Tolerance

- The amount of risk that the area being assessed can manage

Risk Appetite

- The amount of risk that the area being assessed is willing to manage

The tolerance and risk appetite values may differ e.g. Staff can afford to lose email capabilities for five hours (risk tolerance) but only be willing to lose email capabilities for one hour (risk appetite).

VALUE	LIKELIHOOD	IMPACT	PROXIMITY	*SCALE*
1	Unlikely to occur	Negligible Impact	More than 36 months	*Very Low*
2	May occur occasionally	Minor impact on time, cost or quality	12 to 24 months	*Low*
3	Is as likely as not to occur	Notable impact on time, cost or quality	6 to 12 months	*Medium*
4	Is likely to occur	Substantial impact on time, cost or quality	Less than 6 months	*High*
5	Is almost certain to occur	Threatens the success of the project	Now	*Very High*

MLHU RISK REGISTER

IDENTIFY				ASSESS				EVALUATE		MONITOR & REPORT					Comments
ID	Date Identified	Risk Category	Risk Description	Impact (1-5)	Likelihood (1-5)	Risk Rating (H,M,L)	Key Mitigation Strategies ("Controls")	Actions Taken	Current Strength of Controls	Q1 Residual Risk	Q2 Residual Risk	Q3 Residual Risk	Q4 Residual Risk	Most Responsible Leader	Comments
1	Dec-21	Operational/Service Delivery	Core public health services below essential levels due to pandemic response	**4**	**4**	**H**	Strategic planning in the midst of the pandemic will help to focus on what priorities the organization should start, stop or continue doing in order to meet the evolving needs of the community. Adapting the strategic priorities and roadmap to be more agile, flexible, and directional will be crucial for service delivery planning. The likelihood of core public health services falling below essential levels is expected to decrease after Q1 2022 with continued implementation of the risk mitigation strategies mentioned.							CEO MOH	A number of programs and services remain on hold as redeployment continues during the pandemic response.
2	Dec-21	Equity	Lack of resources to respond to emerging and exacerbated public health issues as a result of the pandemic, including food insecurity, domestic violence, racism, substance misuse and mental health	**4**	**5**	**H**	Efforts to address emerging and exacerbated public health issues have been underway in MLHU programs since the outset of the pandemic (e.g., COVID Care packages provided to clients in quarantine/self-isolation, enhanced mental health screening in home visiting programs, Harvest Bucks and food cards provided to HBHC clients, mobile vaccine clinics offered in collaboration with								

							Black-led organizations, etc.). Our website has up-to-date information about community resources related to these issues, and staff will continue to make referrals. As the COVID response evolves MLHU will strive to ensure these efforts are comprehensive and universal at a system level. MLHLU has prioritized anti-Black racism work; an organizational plan has been created and implementation will begin in January 2022.								
3	Dec-21	People/Human Resources	Staff burnout due to high workload and demands related to pandemic response, (e.g. operation of the mass vaccination clinics and continued redeployment to COVID work) including role and scheduling changes (type of work, length of shifts, seven day/week extended hours).	**4**	**5**	**H**	MLHU has implemented partnerships with different organizations such as City of London, Thames Valley Family Health Team, London Health Sciences Centre, etc. to help address large short term staffing needs for vaccination clinics. Ongoing recruitment efforts to hire temporary staff for COVID to replace redeployed staff. HR and Operations are reviewing hours of work, schedule rotations and staffing levels to determine where adjustments can be made to align with staff preference.								

4	Dec-21	People/Human Resources	High demand for limited pool of public health professionals	**4**	**4**	**H**	Implementation of advanced hiring by posting full-time roles for some of the temporary funding based on projected attrition in order to attract external candidates. Hiring of student PHNs and PHIs following their practicums under a temporary licence. Posting for general public health professional roles to build a pool of qualified candidates for when positions are available.								
5	Dec-21	People/Human Resources	Collective agreement negotiations in 2022 could have potential impacts on business continuity in the event of a labour disruption	**5**	**3**	**H**	Business continuity/labour disruption planning is underway in preparation for CUPE negotiations. SLT has already prioritized the key public health work that needs to be covered. Regular prioritization of labour relations issues through weekly collaboration with the union partners. Disruption would now apply mainly to administrative services.								
6	Dec-21	Financial	Uncertainty as to whether the Ministry will provide recovery funding for 2022 will impact staffing requirements during the budget creation and program delivery.	**4**	**4**	**H**	Programs that were previously budgeted will remain in the 2022 budget with the same staffing and funding as previous years. These programs will undergo robust review processes during 2022 to ensure each is aligned with mandated services as described in the Health Protection and Promotion Act and with Board of Health priorities.								

7	Dec-21	Financial	Ministry is funding at 2019 levels and caps on City/County contributions will increase financial strain and the Health Unit's ability to generate a balanced budget while absorbing record inflationary adjustments.	**4**	**5**	**H**	The Health Unit will unite with the City and County to lobby the Ministry to recognize, and fund, inflation. Budgeted contingency will be pooled and shown at the corporate level to offset unknown events. Programs will undergo robust review processes and zero-based budgeting to ensure alignment and potentially identify efficiencies.								
8	Dec-21	Financial	Financial reporting is not frequent enough to provide managers and directors with the necessary information to make informed decisions in a timely manner.	**3**	**5**	**H**	The Finance department is reviewing structure and staffing requirements to meet the demands associated with monthly reporting. The budget will be developed and shared to increase transparency and awareness. Forecasting will be introduced to improve financial management and overs.								
9	Dec-21	People/Human Resources	Targeting of program staff and leadership responsible for implementing public health measures (e.g. section 22 orders, masking, operating mass vaccination clinics, etc.) including threats made in-person, over the phone and social media.	**4**	**4**	**H**	Safety plans have been put in place for staff, leaders and specific clinic sites. Police have been involved in some cases when staff have been threatened. Security is present at Citi Plaza and at the vaccination clinics. Regular communication at Town Hall meetings to provide support to staff and direction on how to call for help.								

10	Dec-21	People/Human Resources	Retention and recruitment of leadership roles in public health.	**4**	**5**	**H**	Focus groups held with leadership staff internally as well as led by an external facilitator to understand what keeps managers at MLHU and reasons they may be leaving. Targeted exit interviews conducted by HR for leaders leaving the organization. Working with an external compensation consultant to conduct a market compensation review with comparator health units and similar sectors.								
11	Dec-21	Technology	MLHU physical servers/SAN are past end of life (8+ Years) and in need of replacement.	**4**	**5**	**H**	Completion of migration expected by end of Q1 2022.								
12	Dec-21	Stakeholder/Public Perception	Ensuring the right leadership and organizational structure is in place to support the evolving needs of the Health Unit.	**4**	**5**	**H**	The 2021 Provisional Plan goal specifically addresses this risk and the Board has examined the need to leverage skill sets to advance the strategy of the organization. There is commitment to achieving the goals as articulated on the Provisional Plan that includes assessing and refining decision-making practices across the organization.								

13	Dec-20	Financial	Uncertainty around timing and allocation of additional funding to cover COVID-related expenditures (staffing and technology costs) creates a risk of cash shortfall that may exceed our line of credit limit	**3**	**3**	**M**	Temporary use of the line of credit will help offset the timing of transfers from the province. Non-COVID program spending is reduced due to limited services provided in the community.	Control implemented in 2021 to reduce the risk.	**Effective**	Minor Risk					
14	Dec-20	Privacy	Rapid implementation of new technology and applications to facilitate pandemic response introduces new privacy and information security risks	**3**	**2**	**L**	Implementation of biennial privacy education program for staff. Agency privacy and information security policies reviewed and updated, including implementation of new virtual care policy. Encrypted tools to support remote work and data transfer. Cyber risk insurance in place. Assessment and mitigation of identified risks ongoing.	Control implemented in 2021 to reduce the risk.	**Effective**	Minor Risk					
15	Jan-22	Political	The potential for rapid turnover on the Board of Health, including Chair/Vice-Chair roles as a result of the 2022 municipal elections	**4**	**4**	**H**									

RISK MATRIX

Risk Priority Risk Map

Risk Matrix Interpretation						
Risk maps provide an effective, means of identifying and prioritizing risks. Risks with a high Probability, and a medium to high Impact are the highest priority, however risk strategies should be developed to deal with all identified risks.						
Impact	5 Threatens the success of the project					
	4 Substantial Impact on time, cost or quality					
	3 Notable impact on time, cost or quality					
	2 Minor impact on time, cost or quality					
	1 Negligible impact					
	Ranking	1 Unlikely to occur	2 May occur occassionally	3 Is as likely as not to occur	4 Is likely to occur	5 Is almost certain to occur
		Likelihood				

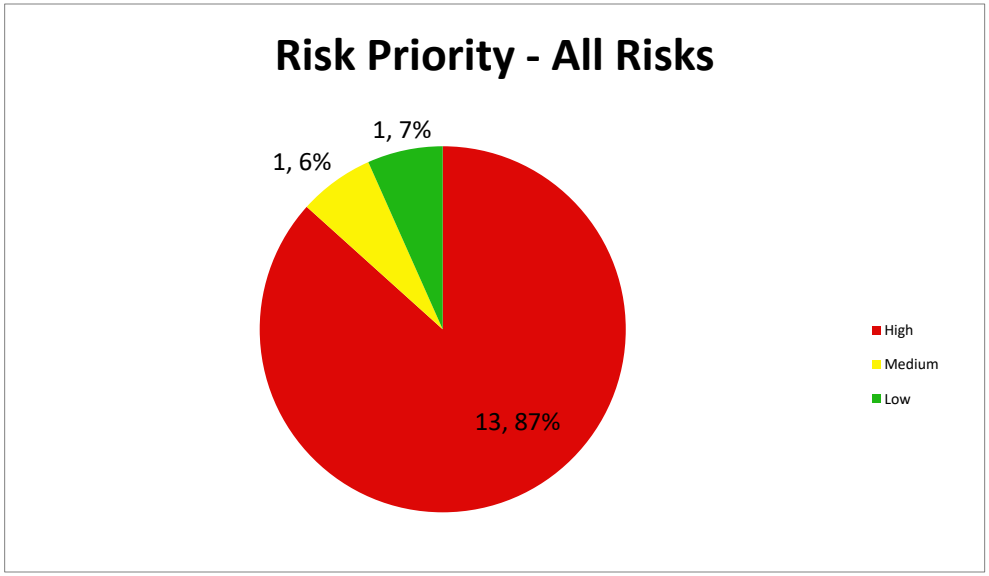
Legend	
	High Risk Priority
	Medium Risk Priority
	Low Risk Priority

RISK CHARTS

Summary Tables and Charts:

Risk Response Tactic	Total	
Risk Priority	Count	Percent
High	13	87%
Medium	1	7%
Low	1	7%
Total	15	100%

Note that the charts are based on the subtotals and exclude risks that were "Not Assessed (NA)", except Risk Priority



RISK SCALES

Risk Rating Scale:

VALUE	LIKELIHOOD	IMPACT	SCALE
1	Unlikely to occur	Negligible Impact	Very Low
2	May occur occasionally	Minor impact on time, cost or quality	Low
3	Is as likely as not to occur	Notable impact on time, cost or quality	Medium
4	Is likely to occur	Substantial impact on time, cost or quality	High
5	Is almost certain to occur	Threatens the success of the project	Very High

Current Strength of Controls Scale:

SCORE	RANK	PRESENSE OF CONTROL	EFFECTIVENESS	RESIDUAL RISK
0	Not able to rate	There are no controls in place to assign a rating		Significant
1	Very ineffective (Virtually no controls)	Very few, if any, controls are in place	Controls are ineffective at mitigating the risk	Significant
2	Ineffective (Low control effectiveness)	Limited controls are in place	Only a limited number of the controls are effective	Moderate
3	Partly effective (Moderate control effectiveness)	A moderate number of controls are in place	The controls are adequate at mitigating part of the risk	Moderate
4	Effective (High control effectiveness)	The majority of controls are in place	The controls mitigate the majority of the risk	Minor
5	Very effective (Very high control effectiveness)	Nearly all of the required controls are in place	The controls are effective at mitigating the risk	Minor

Residual Risk:

RESIDUAL RISK	DESCRIPTION
Significant	Represents the highest residual risk exposure as the assessed level of risk control effectiveness is insufficient for the level of risk. Management should consider improving risk control plans for these risks.
Moderate	Represents additional residual risk exposure that could be investigated further as the assessed risk control effectiveness is not propitiate with the level of risk. Control plans should be documented and reviewed or appropriateness.
Minor	Areas where the risk control effectiveness is proportionate with the level of risk.

References

Strength of Controls
Not able to rate
Very Ineffective
Ineffective
Partly Effective
Effective
Very Effective

Residual Risk
Significant Risk
Moderate Risk
Minor Risk

Risk Categories
Environment
Equity
Financial
Governance/Organizational
Information/Knowledge
Legal/Compliance
Operational/Service Delivery
People/Human Resources
Political
Privacy
Security
Stakeholder/Public Perception
Strategic/Policy
Technology