Subject: Corporate Access to Information and Privacy Protection Policies

Report to: Corporate Services Committee

Report date: Wednesday, August 5, 2020

Recommendations

1. That Corporate Policy C-IMT-003, Information Access and Privacy Protection Policy (Appendix 1 of Report CLK 3-2020), **BE REPEALED**;

2. That the Access to Information and Privacy Protection Policy (Appendix 2 of Report CLK 3-2020) **BE APPROVED**; and

3. That the Personal Health Information Protection Policy (Appendix 3 of Report CLK 3-2020) **BE APPROVED**.

Key Facts

- The purpose of this report is to seek Council's approval of two new corporate policies respecting access to information and protection of privacy.
- These policies put into place requirements based on the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act* (PHIPA).
- The current corporate privacy policy C-IMT-003, Information Access and Privacy Protection Policy, was last revised in 2012.
- Recommendation 5 of the Ontario Ombudsman Report "Inside Job", recommended Niagara Region ensure that all officials and employees with access to personal information understand their obligations under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).
- The new policies more clearly outline how Niagara Region remains in compliance with Ontario's legislative framework for privacy by creating separate policies for each piece of legislation.
- The new policies provide greater clarity respecting the roles and responsibilities of officials and staff throughout the organization.

Financial Considerations

There are no financial considerations associated with this report.

Analysis

On November 29, 2019, the Ontario Ombudsman released his report titled “Inside Job” respecting the investigation he conducted regarding the process Niagara Region undertook in the hiring of its Chief Administrative Officer. Recommendation 5 of the Ombudsman Report states:

The Regional Municipality of Niagara should ensure that all officials and employees with access to personal information understand their obligations under the Municipal Freedom of Information and Protection of Privacy Act.

The current Information Access and Privacy Protection Policy deals with both provincial privacy laws, MFIPPA and PHIPA. In light of the Ombudsman’s recommendation, the obligations and corporate expectations of both officials and staff could be more clearly defined.

The two new policies being recommended by this report provide additional direction to staff with respect to what they are required to do to remain in compliance with the fundamental principles of the legislation. Additionally, to ensure the understanding of these expectations, Clerk’s Office staff will lead an education campaign throughout the fall of 2020, to ensure all staff are aware of policy changes and their individual obligations as defined therein.

The Access to Information and Privacy Protection Policy (Appendix 2 of Report CLK 3-2020), additionally states the requirements for conducting privacy impact assessments, completing personal information banks, and for the management of privacy incidents and contraventions against MFIPPA.

This policy will allow Niagara Region to be better prepared to:

- Anticipate, identify and prevent privacy invasive events before they occur;
- Build in the maximum degree of privacy into the default settings of Niagara Region’s systems and business practices. Doing so will keep a user’s privacy intact, even if they choose to do nothing;

- Embed privacy settings into the design and architecture of information technology systems and business practices instead of implementing them after the fact as an add-on; and
- Protect the interests of users by offering strong privacy defaults, appropriate notice, and empowering user-friendly options.

The Personal Health Information Protection Policy (Appendix 3 of Report CLK 3-2020), specifically applies to Niagara Region's Health Information Custodians, a role defined by the *Personal Health Information Protection Act*. This policy provides additional guidance to the custodians and their staff with respect to an individual's ability to access their own health records, as well as the roles and responsibilities within the organization that are responsible for ensuring the protection of those records.

Alternatives Reviewed

Council may choose to continue with the current Information Access and Privacy Protection Policy, C-IMT-003. This is not recommended given the age of the policy and the recommendation from the Ontario Ombudsman respecting staff knowledge and understanding of their roles under the *Municipal Freedom of Information Protection of Privacy Act*.

Relationship to Council Strategic Priorities

The recommendations in this report align with Council's Strategic Priority of Sustainable and Engaging Government.

Other Pertinent Reports

CAO 17-2019 Recommendations from the Ontario Ombudsman Report "Inside Job" November 2019

Prepared and Recommended by:
Ann-Marie Norio
Regional Clerk
Administration

Submitted by:
Ron Tripp, P.Eng.
Acting Chief Administrative Officer

This report was prepared in consultation with M. Trennum, Deputy Regional Clerk, and reviewed by S. Hannell, Manager, Information Management Services, M. Antidormi, Privacy Officer, and D. Gibbs, Director, Legal and Court Services.

Appendices

Appendix 1 C-IMT-003 (C3.F03) - Information Access and Privacy Protection Policy

Appendix 2 Draft Access to Information and Privacy Protection Policy

Appendix 3 Draft Personal Health Information Protection Policy

SECTION	NAME OF POLICY
INFORMATION	INFORMATION ACCESS & PRIVACY PROTECTION

****This policy has been provided by Niagara Region for reference purposes only and does not constitute legal advice. This policy has no association with or authority over the operations of any organization beyond Niagara Region.****

DEVELOPED BY: Corporate Records and Information Services, Office of the Regional Clerk

APPROVED BY: CMAT

DATE: October 19, 2010

REVIEW DATE: October 19, 2012

POLICY STATEMENT

All Niagara Region employees and members of Regional Council shall comply with Ontario's information access and privacy requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA, 1991) and the *Personal Health Information Protection Act* (PHIPA, 2004).

POLICY PURPOSE AND BACKGROUND

This policy confirms Niagara Region's obligation to provide information access and privacy protection in accordance with MFIPPA and PHIPA.

The accompanying procedures provide staff guidelines for how to comply with both Acts. All underscore the principles of openness and responsiveness expressed in corporate policy C3.A10, "Accountability and Transparency."

MFIPPA came into effect January 1, 1991. It has several key principles:

1. That the majority of information held by public institutions (i.e. Niagara Region) should be publicly accessible

2. That only under specific circumstances, as described in MFIPPA, should information be withheld from the public

3. That all personal information (PI), personal health information (PHI), and otherwise confidential information held by public institutions should be protected from unwarranted disclosure

4. That individuals who provide personal information to public institutions have a right at any time to view and/or correct this information.

MFIPPA also outlines a step by step process by which members of the public can request to view or obtain copies of information from public institutions.

PHIPA came into effect January 1, 2004. It is similar to MFIPPA, but makes no provisions for information access. PHIPA applies specifically to the confidentiality of personal health information (PHI) and dictates:

1. That all personal health information held by public institutions (i.e. Niagara Region) should be protected from unwarranted disclosure

2. That individuals who provide personal health information to public institutions (i.e. Niagara Region) have a right at any time to view, obtain a copy of and/or correct this information.

SCOPE

This policy and procedures apply to all Niagara Region employees, including members of Regional Council.

ENFORCEMENT

Consequences of a failure to comply with MFIPPA and PHIPA include:

- Privacy breach or breach of confidentiality
- Investigation by the Information and Privacy Commission of Ontario (IPC)
- IPC Orders issued against Niagara Region, its policies and/or employee practices
- Negative media coverage for Niagara Region, Regional departments, services and programs
- Loss of the public's trust
- Potential for legal appeals and/or litigation, with associated financial costs

Under MFIPPA s.42(2), any individual who wilfully acts in contravention of MFIPPA, requests information under false pretenses, obstructs an investigation by the IPC or fails to follow an order by the IPC is liable to a fine of up to $5,000.

PROCEDURE

This procedure describes the steps required to complete a formal written request for information under MFIPPA or PHIPA. Sometimes, information is requested informally via verbal, telephone or email exchanges. Please consult with supervisors and/or Access and Privacy staff within Clerk's for advice on how to respond to informal requests.

ACCESS TO INFORMATION

Step 1 – Request Received

- The Niagara Region Access and Privacy Unit within the Office of the Regional Clerk receives a written request for information, or
- Niagara Region employees receive a written FOI request and send it directly to the Access and Privacy Unit. Divisional management may be notified of a request, but the identity of the requestor must be kept confidential.

Step 2 – Request Acknowledged

- Legislated timelines for responding to an information request start "ticking" as of the date when the requester pays a fee of $5.00 as required under MFIPPA. PHIPA does not require an administrative fee.
- Access and Privacy staff send a letter of receipt to the requester.

Step 3 – Staff Notified

- Access and Privacy staff notify the appropriate MFIPPA/PHIPA staff contact that a request for information from their department or division has been made
- Staff contacts typically respond by providing records to the Access and Privacy Unit within five business days.

Step 4 – Further Staff Required (Optional)

- If the information request is very complex, Niagara Region employees may indicate that additional staff and/or councillors need to be involved.
- The Access and Privacy Unit will notify additional staff and/or councillors and ask if they have any records related to the request.
- Records must be provided regardless of format: paper, email, digital files, photos, video, voicemail, instant messages, etc.

If staff and/or councillors have no records relevant to the request, they will confirm this fact in writing.

If staff and/or councillors do have records relevant to the request, these records must be provided to Access and Privacy staff within legislated timelines.

Step 5 – Fee Estimate (Optional)

- Before any records are actually provided, the Access and Privacy Unit may ask for an estimate of how many records each individual holds that pertain to the request. These numbers may be used to create a fee estimate, which is then sent to the requester.
- Fee estimates may be quite large, depending on the staff time required to search and review records. Upon receipt of a fee estimate, the requester may choose to:
    a) Not pay the fee, and not pursue the information request further
    b) Not pay the fee, and contact Access and Privacy staff to narrow the scope of their request
    c) Not pay the fee, and initiate an appeal with the Office of the Information and Privacy Commissioner for Ontario (IPC)
    d) Pay the fee (full amount if total is under $100.00; minimum 50% deposit required if total is over $100.00) and continue pursuing the information request in its original form

Step 6 – Application for Extension (Optional)

- If the request is going to require extensive search time or requires clarification, Niagara Region may apply for an extension as defined in MFIPPA. Access and Privacy staff will notify the requester of the extension. Extensions may occur once only per request.

Step 7 – Records Provided

- Records related to the information request must be provided to Access and Privacy staff as soon as possible.
- This may be done in paper or electronic form. Originals should be provided whenever possible.

Step 8 – Records Reviewed

- Access and Privacy staff review records and, if necessary, sever information that is exempt from public disclosure under MFIPPA. Exemptions may include:

Discretionary Exemptions	**Mandatory Exemptions**
Draft by-laws	Third party information
Advice or recommendations	Relations with governments
Discretionary Exemptions (ctd.)	**Mandatory Exemptions (ctd.)**
Law enforcement	Personal information
Economic/Other interests	Personal health information
Danger to health and safety	
Danger to national security	
Solicitor-client priviledge	
Information soon to be published	
Constituent business	

Step 9 – Third Party Notification (Optional)

- If third party information is present in the requested records, Access and Privacy staff will notify the parties concerned and request their representation on the disclosure of the affected records.
- Third Parties will submit their response within 20 working days to the Access and Privacy Unit, along with their views on the disclosure.

Step 10 – Disclosure Decision

- Under MFIPPA, organizations must identify a "designated head" that has the final authority to make decisions about information disclosure. At Niagara Region, by-law 6077-90 names the Chair of Regional Council as the designated head for the purposes of MFIPPA.
- Similarly, the Niagara Region Medical Officer of Health is identified as a Health Information Custodian for the purposes of PHIPA.

Step 11 – Records Provided to Requester

- After a careful review, records are provided to the requester within legislated timelines.
- The requester may view records in person, receive them electronically, or obtain a hard copy.

PRIVACY PROTECTION

The following procedures are based on the requirements of MFIPPA, PHIPA, and 10 privacy principles developed by the Canadian Standards Association.

Principle 1: Accountability

Niagara Region, its employees and councillors are publicly accountable for protecting the privacy of clients, customers and business partners who submit personal or otherwise privileged information to the Region in confidence, provided that public expectations of privacy fall within the dictates of MFIPPA and PHIPA. See corporate policy C3.A10, "Accountability and Transparency."

Principle 2: Identifying Collection Purposes
When collecting personal information (PI) or personal health information (PHI), Niagara Region will inform clients and customers as to why this information is required and how it will be used.

2.1 At Niagara Region, common reasons for collecting PI and PHI include:

- program administration
- property administration (taxes, building inspection and licensing)
- provision of services
- provision of utilities
- by-law enforcement
- personnel administration
- public safety
- general correspondence

2.2 Niagara Region will demonstrate its legal authority to collect PI and PHI, and will provide a contact for questions about the collection and use of PI and PHI. This may require:

- a notification clause or collection disclaimer on all forms that collect personal information, including those that appear on www.niagararegion.ca
- contact numbers and/or notification clauses posted visibly at service counters where personal information is received verbally

2.3 Niagara Region does not share personal information with other government agencies, except where provided for by an Act of legislation or informed consent.

2.4 If it is necessary to use PI or PHI for purposes other than those originally stated at the time of collection, Niagara Region will obtain informed consent from the individual(s) involved.

Principle 3: Consent
Niagara Region obtains consent for the collection, use and disclosure of personal information, except for instances when requiring consent may endanger the health or safety of an individual.

Principle 4: Limiting Collection
Niagara Region will only collect information that is absolutely necessary for the delivery of programs or services, general administration, public safety, collection of taxes or by-law and law enforcement.

4.1 When Niagara Region collects PI and/or PHI, it will do so in a transparent manner. In other words, no PI and/or PHI will be collected from individuals indirectly or without their knowledge.

4.2 Indirect collection of personal information will occur only when the guardian of a person under the age of consent (a minor) is supplying the information, or when collection is necessary for the purpose of by-law or law enforcement, administrative investigations or public safety.

4.3 If Niagara Region receives any unsolicited PI/PHI from citizens or clients, it must be retained in a secure and confidential manner. If sent in error, contact the sender to return the information. If related to a Niagara Region program or service, direct the sender to a more appropriate contact. If received via email, instant message or Facebook, ensure that privacy of the message will be maintained and contact the sender to establish a more secure method of exchange. Always take great care when receiving, storing and transmitting PI/PHI.

Principle 5: Limiting Use, Disclosure & Retention

In addition to limiting use and disclosure, PI and PHI will only be retained by Niagara Region long enough to meet legislative or operational requirements contained in the Regional Municipality of Niagara Records Retention By-Law and Schedule "A".

5.1 Niagara Region does not give, rent, trade or sell personal information lists to any organization other than its own departments or agencies, except where provided for by an Act of legislation.

5.2 Appropriate physical, technological, and procedural safeguards will be implemented to ensure that all PI and PHI retained by Niagara Region remains secure from unintentional disclosure.

Principle 6: Accuracy

Niagara Region will maintain all records containing PI and PHI as accurate, complete and up-to-date.

6.1 Niagara Region updates information as it is made available by the individual who provided the information.

6.2 Niagara Region does not routinely update personal information unless such a process is necessary to fulfill the purpose for which the personal information was originally collected.

6.3 It is the responsibility of the individual who supplied PI and/or PHI to advise Niagara Region when changes are required to this information.

6.4 As per section 36 of MFIPPA, any individual may request corrections to PI and/or PHI held by The Region, if they believe that an error or omission has been made. Click here for the MFIPPA form to correct personal information.

Not all requests for correction will be fulfilled, but there will at minimum be a notation added to the original information that outlines the requested change. Notice will be supplied as to whether or not the correction was made and the reasons for the decision.

Principle 7: Safeguards

Niagara Region protects PI and PHI with physical, technological and procedural safeguards that are appropriate to the format and sensitivity of the information.

7.1 Protection methods for personal information include:

- staff training
- locked file cabinets and file rooms
- restricted office access
- clean desk practices
- employee confidentiality agreements
- passwords and network security
- data encryption

7.2 If a third party is contracted to collect or use personal information on behalf of Niagara Region, legal agreements or written consent processes must be developed that require the third party to use practices that protect the personal information in accordance with MFIPPA and PHIPA.

7.3 Completion of a Privacy Impact Assessment (PIA) is highly recommended as a method of assessing risks to privacy and ensuring that all Niagara Region programs and services operate with privacy protection as a priority. Detailed information and advice on completing a PIA is available from:

- Access and Privacy Staff (FOI@niagararegion.ca; x.3273)
- Ontario Ministry of Government Services (http://www.accessandprivacy.gov.on.ca/english/pia/index.html)
- Office of the Information and Privacy Commissioner of Ontario (http://www.ipc.on.ca)

Principle 8: Openness

Niagara Region adheres to and supports the principles of access and transparency embodied by MFIPPA.

8.1 Information, once requested, will be released unless it falls under one of the exemptions listed in MFIPPA, or:

- it contains PI and/or PHI that does not belong to the requester
- disclosure is limited by some other legislation
- there is a legal agreement in place prohibiting release
- disclosure would limit by-law and law enforcement

Principle 9: Individual Access

Upon completion of the FOI Request Form, Access and Privacy Unit staff will provide to the individual making the request, access to PI and/or PHI that is held about them by Niagara Region.

9.1 If required, assistance is available in completing a request.

9.2 Niagara Region may request identification to verify the identity of individuals seeking access to their own personal information.

9.3 Niagara Region will make every effort to comply with legislated deadlines and fee structures as per MFIPPA.

9.4 In the event of a highly complex or voluminous request, an estimate of applicable charges and/or fees will be provided to the requestor, and approved by the requestor, prior to the gathering of information to fill the request.

Principle 10: Challenging Compliance

An individual may challenge Niagara Region's compliance with these privacy principles or with MFIPPA and/or PHIPA by contacting Access and Privacy staff via FOI@niagararegion.ca or 905-685-4225 x.3741

10.1 The FOI Coordinator will make every reasonable effort to satisfy the concerns of a challenge, including reviewing the policies and practices of The Region and submitting a response to the individual making the challenge.

10.2 If an applicant is not satisfied with the response received from The Region's FOI Coordinator regarding compliance, or any part of an information request, an appeal can be sent to the Office of the Information and Privacy Commissioner of Ontario (IPC). A staff member of the Commissioner's office will arrange to mediate with the two parties and come to an agreement. If this process fails to satisfy the applicant then a formal inquiry will be held with the Commissioner. The Commissioner's ruling is binding on both parties.

10.3 If required, The Region's FOI Coordinator will assist an applicant in sending an appeal to the Office of the Information and Privacy Commissioner.

Policy Owner	Corporate Administration, Office of the Regional Clerk, Access and Privacy Office, Deputy Regional Clerk
Approval Body	Council
Approval Date	
Effective Date	
Review by Date	August 2022

1. Policy

Niagara Region shall comply with the Province of Ontario's access to information and privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Access and Privacy Principles
Niagara Region is committed to fostering trust and confidence with the public through its adherence to the following fundamental principles of MFIPPA:

1) Information should be available to the public

Niagara Region shall provide access to information under its custody or under its control, whether through routine disclosure, proactive dissemination, Open Data, and/or through the formal freedom of information request process, in accordance with the principles that:

a. Information should be available to the public; and
b. Necessary exemptions from the right of access should be limited and applied in specific circumstances, such as the protection of personal information, third party information, and confidential government information protected by legal privilege.

2) Individuals shall have access to their own personal information
Niagara Region's divisions, programs, or services which collect, use, retain, disclose, and/or dispose of personal information shall, in consultation with the Access and Privacy Office, develop, implement and annually review procedures for granting individuals' access to their own personal information, including a standard for what information may be provided through routine disclosure and what information may require the individual to submit a freedom of information request.

   Every individual who is given access to his/her personal information is entitled to request correction of the personal information Niagara Region has in its custody or in its control, if the individual believes there is an error or omission.
   - In the event Niagara Region is unable to make a correction due to the inability to verify accuracy, Niagara Region shall instead ensure the request is documented and appended to the information in question reflecting any correction that was requested but not made and the reasons therefore.
   - Additionally, Niagara Region shall ensure that anyone to whom the personal information was disclosed, within the year before the correction was requested, be notified of the correction or the statement of disagreement.

3) Institutions must protect the privacy of individuals with respect to personal information; Niagara Region will:
   a. Establish and maintain a corporate privacy program and procedural framework in accordance with the Canadian Standard Association's (CSA) guiding principles of privacy;
      i. Accountability
      ii. Identifying Collection Purposes
      iii. Consent
      iv. Limiting Collection
      v. Limiting Use, Disclosure & Retention
      vi. Accuracy
      vii. Safeguards
      viii. Openness
      ix. Individual Access
      x. Challenging Compliance

b. Ensure all officials and employees share responsibility for the protection of personal information as further described in the roles and responsibilities identified in this policy;

c. Plan for and ensure that the protection of personal information is embedded in the design of all Niagara Region programs, processes, projects and technology;
   i. Niagara Region's programs and services shall conduct a privacy impact assessment (PIA), in a manner that is proportionate with the privacy risk identified by the PIA screening tool, for any new or modified collection, use, retention, disclosure and/or disposal of personal information, or personal health information.

d. Establish and communicate a set of privacy standards and guidelines to improve the protection of personal information by identifying, investigating, assessing, monitoring, and mitigating privacy risks in Regional programs and services which collect, use, disclose and dispose of personal information;

e. Apply this policy and related policies and practices to the collection, use, retention, disclosure, and disposal of personal information;

f. Clearly communicate to the public how personal information is collected, used, disclosed and disposed;
   i. Niagara Region shall make available for inspection by the public an index of all personal information banks (PIB) in the custody or under the control of the institution. The information should include:
      1. Its name and location;
      2. The legal authority for its establishment;
      3. The types of personal information maintained in it;
      4. How personal information is used on a regular basis;
      5. To whom the personal information is disclosed on a regular basis;
      6. The categories of individuals about whom personal information is maintained; and
      7. The policies and practices applicable to the retention and disposal of the personal information.

ii. Niagara Region will ensure Personal Information Banks receive routine maintenance and updating as required to ensure the accuracy and transparency of the information;

g. Make privacy training mandatory, proportional with their job responsibilities, for all Regional officials and employees with access to personal information to understand their obligations under MFIPPA;

4) Niagara Region shall ensure that reasonable measures, respecting the safeguarding and retention of records in the custody or under the control of Niagara Region, are defined, documented, and administered, taking into account the nature of the records to be protected.

Managing Privacy Incidents and Privacy Breaches

Niagara Region shall work to contain, investigate, and reduce the risk of future incidents when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws.

All privacy incidents shall be immediately reported, or reported as soon as reasonably possible, to Niagara Region's Access and Privacy Office.

2. Purpose

To foster public trust by establishing mandatory requirements and clear responsibilities and accountability for the protection of personal information that is collected, used, disclosed, or disposed of by Niagara Region.

3. Scope

This policy applies to all Niagara Region employees, elected officials, students and volunteers. Niagara Region employees responsible for managing, developing, and entering into contracts with any third party service providers or contractors that involve information that would be subject to this policy are responsible for ensuring that those contractual arrangements are in alignment with this policy.

This policy applies to all personal information including personal health information in the custody or the control of Niagara Region and is not limited by the scope of any individual legislation or regulation with the exception of personal health information in the custody or control of Niagara Region's Health Information Custodians pursuant to PHIPA.

3.1. Roles and Responsibilities

3.1.1. Regional Clerk

a. Provide oversight of and compliance with this Policy and Framework by all Regional Staff.

3.1.2. Corporate Leadership Team

a. Integrate protection of personal information requirements into the development, implementation, evaluation, and reporting activities of divisional programs and services in accordance with this policy and any of its procedures;
b. Promote a culture of business practices that ensure Regional information is shared and accessible to the greatest extent possible, while respecting privacy requirements of personal information and other confidentiality obligations.

3.1.3. Deputy Regional Clerk

a. Develop and implement policies, programs and services for management and protection of personal information based on Privacy by Design principles;
b. Establish privacy standards, guidelines and procedures to support this Policy and Framework;
c. Coordinate the corporate privacy breach protocol and the response to complaints regarding the misuse of personal information;
d. Authorize and sign-off on the Privacy Impact Assessment report prior to implementation of any technology, system, program or service involving the collection or use of personal information or personal health information;

e. Engage the Chief Information Officer to assess the security of any technological system that collects or uses personal information or personal health information.

3.1.4. Freedom of Information Coordinator

a. Accept formal freedom of information (FOI) requests on behalf of Niagara Region and facilitate the search, gathering and redaction of the records, as required;
b. Maintain all records and information pertaining to an FOI request;
c. Review divisional procedures for granting individuals' access to their own personal information, including access through routine disclosure and freedom of information requests;
d. Complete annual reporting to the Information and Privacy Commissioner/Ontario which includes compiling and verifying required data.

3.1.5. Access and Privacy Office

a. Implement this policy, in partnership with Regional Divisions, including the development of required procedures;
b. Review divisional practices for the collection, use, disclosure and disposition of personal information;
c. Consult with business programs to meet privacy requirements as identified in this Policy, applicable legislation, privacy standards and procedures;
d. Investigate reports of privacy breaches and communicate findings to complainant and engage with Legal Services as required;
e. Review and investigate all privacy incidents to determine whether or not a breach has occurred. The Access and Privacy Office will coordinate and manage all privacy breaches according to Niagara Region's Privacy Breach Protocol procedure
f. Conduct Privacy Impact Assessments in consultation with Regional Divisions and programs;
g. Develop, coordinate and deliver privacy training as required by this policy and its associated procedures.

3.1.6. Manager, Information Management Services

a. Oversee, develop and implement corporate strategies, policies, standards, procedures, best practices and programs to promote the Regions records and information management program;

b. Lead records and information training and awareness campaigns;

c. Provide advice and guidance on records and information management policies and related matters.

3.1.7. Chief Information Officer

a. Implement Privacy by Design principles in Enterprise Architecture, information technology policies, standards, procedures and technologies;

b. Conduct Risk Assessments (Threat Risk Assessments, and Vulnerability Assessments) on all technological systems involving the collection or use of personal information prior to implementation or deployment;

c. Execute recommendations identified in Privacy Impact Assessment reports;

d. Provide to the Deputy Regional Clerk the results of all Threat Risk Assessments and Vulnerability Assessments on any technological system that collects or uses personal information or personal health information.

3.1.8. Directors and Divisional Leadership

a. Be accountable for ensuring personal information is collected, used, disclosed and disposed in accordance with legislation and associated regulations, standards and other Regional policies, and in compliance with this policy;

b. Develop, in consultation with the Freedom of Information Coordinator and the Privacy Officer, procedures for granting individuals' access to their own personal information, including a standard for what information may be provided through routine disclosure and what information may require the individual to submit a freedom of information request;

c. Implement this Policy and Framework and communicate to staff under their direction;

d. Restrict access to personal information to those individuals who require access to personal information in order to perform their duties and where access is necessary for the administration of their business;

e. Maintain personal information and develop, and implement processes whereby individuals can view information held about them and what the Region uses it for. These processes will also facilitate individuals needing to correct or update their information;

f. In collaboration with the Privacy Officer, the Chief Information Officer, applicable Commissioner, Procurement staff, and the Chief Administrative Officer, ensure that any contractual arrangements with third party service providers or contractors are in alignment with this policy;

g. Consult with the Deputy Regional Clerk and the Chief Information Officer during the planning stages, before any procurement, and prior to implementation of any technology, system, program or service involving the collection, use, disclosure or disposition of personal information or personal health information.

3.1.9. Niagara Region Personnel

Each individual that collects, uses, discloses, or disposes of information received as part of their duties as a Regional employee including personal information, is accountable for the actions they take with the information including ensuring the information is used only for the purpose it was obtained and is not disclosed to either other employees or non-employees except as permitted in accordance with this policy and applicable legislation whatever form the information is stored or transmitted in. All employees will:

a. Manage personal information that they collect, use, retain, disclose and dispose of for Regional business in accordance with this policy and its procedures to safeguard such information;

b. Take privacy training as required by their role, position, or in consultation with the Access and Privacy Office to ensure the appropriate handling of personal information and to understand their responsibilities to protect privacy in executing their operational duties;

c. Ensure that personal information is only accessible and discussed by authorized users;
d. Report any privacy incidents to the Access and Privacy Office immediately, or as soon as reasonably possible;
e. Be aware of their individual privacy responsibilities as defined by departmental, divisional, or program specific procedures for the collection, use, retention, disclosure, or disposal of personal information;

Each individual should be aware that non-compliance with MFIPPA requirements, risks and consequences may include any or all of the following:

- Loss of trust or confidence in the Niagara Region
- Privacy Breach or breach in confidentiality
- Legal liabilities and proceedings
- Investigation by privacy oversight bodies (IPC)
- IPC Orders issued against Niagara Region, its policies and/or employee practices
- Negative media coverage for Niagara Region, Regional departments services and programs

Under MFIPPA s.42(2), any individual who willfully acts in contravention of MFIPPA, requests information under false pretenses, obstructs an investigation by the IPC or fails to follow an order by the IPC is liable to a fine of up to $5,000.

Definitions

MFIPPA means the *Municipal Freedom of Information and Protection of Privacy Act* (Ontario) and its regulations, as amended from time to time.

Personal Information means all recorded information that is about an identifiable individual or is defined or deemed to be “personal information” pursuant to any laws or regulations related to privacy or data protection that are applicable to the Regional Municipality of Niagara (including, without limitation, any information that constitutes “personal information” as such term is defined by MFIPPA or “personal health information” as such term is defined by PHIPA).

Privacy Breach means any inappropriate or unauthorized collection, use, retention, disclosure, or disposal of personal information.

Privacy by Design means the consideration of privacy during the design process that integrates the protection of "personal information" directly into the technology/system through creation, operation, and management of the system or technology itself.

Privacy Impact Assessment (PIA) means the tool used by the corporation to review any change to the collection, use, retention, disclosure, or disposal of "personal information" to assess the risks to privacy associated with the change, and to provide recommendations on how to mitigate these risks.

Privacy Incident means and inappropriate or unauthorized action that involves data, information or records which include "personal information" that may lead to the discovery of a "privacy breach".

Threat Risk Assessment (TRA) means the tool use by the corporation to identify, analyzing and reporting the risks associated with an information technology system's potential vulnerabilities and threats.

Vulnerability Assessment (VA) means the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the corporation with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately

4. References and Related Documents.

4.1. Legislation, By-Laws and/or Directives

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);

Niagara Region Retention By-law

Delegation of Head by-law

4.2. Procedures

Privacy breach protocol

5. Related Policies

Personal Health and Information Protection Act (PHIPA) Policy

6. Document Control

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

Approval History

Approver(s)	Approved Date	Effective Date

Revision History

Revision No.	Date	Summary of Change(s)	Changed by

Policy Category	*Name of Policy*
Information Management & Technology	Personal Health Information Protection Policy

Policy Owner	Corporate Administration, Office of the Regional Clerk, Access and Privacy Office, Deputy Regional Clerk
Approval Body	Council
Approval Date	
Effective Date	
Review by Date	August 2022

1. Policy

Niagara Region shall comply with the Province of Ontario's access to information and privacy protection requirements as mandated by the *Personal Health Information Protection Act* (PHIPA, 2004).

Individual Access to his/her Own Personal Health Information

Niagara Region programs and services, which collect personal health information (PHI) shall develop, implement and annually review procedures for granting individuals' access to their own PHI, including a standard for what information may be provided through routine disclosure and what information may require the individual to submit a formal written request for records, or request for a correction of PHI.

Every individual who is given access to his/her PHI is entitled to request correction of the PHI, if the individual believes there is an error or omission.

- In the event Niagara Region is unable to make a correction due to the inability to verify accuracy, Niagara Region shall instead ensure the request is documented and appended to the information in question reflecting any correction that was requested but not made and the reasons therefore.
- Additionally, Niagara Region shall ensure that anyone to whom the PHI was disclosed, within the year before the correction was requested, be notified of the correction or the statement of disagreement.

Privacy Protection of Personal Health Information

Health Information Custodians will:

a. Comply with Niagara Region's corporate privacy program and procedural framework by developing health information practices, in accordance with PHIPA and with the Canadian Standard Association's (CSA) guiding principles of privacy;

   i. Accountability
   ii. Identifying Collection Purposes
   iii. Consent
   iv. Limiting Collection
   v. Limiting Use, Disclosure & Retention
   vi. Accuracy
   vii. Safeguards
   viii. Openness
   ix. Individual Access
   x. Challenging Compliance

b. Maintain, or require the maintenance of, an electronic audit log in compliance with PHIPA and Ontario Regulations for any electronic means of collection, use, disclosure, modification, retention or disposal of PHI;

c. Ensure all officials and employees share responsibility for the protection of personal information as further described in the roles and responsibilities identified in this policy;

d. Apply this policy and related policies and practices to the collection, use and disclosure, and disposal of personal information.

2. Purpose

The purpose of this privacy policy is to establish mandatory requirements and responsibilities for the protection of personal health information (PHI) that is received or sent by Niagara Region's Health Information Custodians.

Niagara Region is committed to being a leader in privacy by fostering trust and confidence with its clients and the public through its transparency of process and by maintaining confidentiality and a high level of protection of PHI.

3. Scope

This policy applies to all Niagara Region employees, elected officials, students and volunteers. Niagara Region employees responsible for managing, developing, and entering into contracts with any third party service providers or contractors that involve information that would be subject to this policy are responsible for ensuring that those contractual arrangements are in alignment with this policy. The policy applies to all services and corporate activities that may impact the privacy of PHI in Niagara Region's custody or control.

3.1. Roles and Responsibilities

3.1.1. Health Information Custodians

Niagara Region has two Health Information Custodians as defined by the *Personal Health Information Protection Act*, *2004*: The Medical Officer of Health, and the Commissioner of Community Services.

Appendix A provides a list of Niagara Region's Health Information Custodians. Appendix B provides a diagram of the Health Information Custodian administrative reporting structure.

Any designated Health Information Custodian at Niagara Region shall:

i. Obtain the individual's implied or express consent when collecting, using and/or disclosing PHI, except in limited circumstances as specified under PHIPA;
ii. Collect PHI appropriately (by lawful means and for the lawful purposes of providing health care as defined by PHIPA) and no more than is reasonably necessary;
iii. Take reasonable precautions to safeguard PHI:
    a) against theft or loss,
    b) unauthorized use, disclosure, copying, modification and/or destruction;
iv. Implement and annually review procedures regarding consent documentation;

v. Provide notification to an individual at the first reasonable opportunity if the information is stolen, lost or accessed by an unauthorized person;
vi. Implement and annually review procedures for auditing for compliance with this policy and PHIPA requirements for protection of privacy;
vii. Ensure health records are as accurate, up-to-date and complete as necessary for the purposes for which they were collected, used and/or disclosed;
viii. Ensure health records are stored, transferred and disposed of in a secure manner;
ix. Designate a contact person who is responsible for:
    a) responding to access/correction requests;
    b) responding to enquires about the health information custodian's information practices;
    c) receiving complaints regarding any alleged breaches of PHIPA and notifying Niagara Region's Access and Privacy Office as soon as possible;
x. Provide a written statement for each Health Information Custodian as defined in this policy that is readily available to the public, published on the Region's external website, and/or available in print from each program service area which describes:
    a) the Health Information Custodian's information practices;
    b) how to reach the contact person; and
    c) how an individual may obtain access to, request a correction and/or make a complaint regarding his/her PHI;
xi. Administer the review, response and administration of all formal requests for PHI and records in the custody or control of the Health Information Custodian, in coordination with Niagara Region's Access and Privacy Office; and
xii. Ensure that all agents of the Health Information Custodian are appropriately informed of their duties under this policy and PHIPA.

3.1.2. Access and Privacy Office, Office of the Regional Clerk

a) Develop and implement policies, programs and services for management and protection of PHI based on Privacy by Design principles;
b) Establish privacy standards, guidelines and procedures to support this Policy and Framework;

c) Develop, coordinate and deliver privacy training as required by this policy and its associated procedures;
d) Advise Niagara Region's Health Information Custodians, programs and services on the implementation of this policy, their roles and responsibilities, and interpretation of PHIPA;
e) The Access and Privacy Office is responsible for reviewing all privacy incidents and investigating to determine whether or not a breach has occurred. The Access and Privacy Office will coordinate and manage all privacy breaches of PHI according to Niagara Region's Privacy Breach Protocol procedure.

3.1.3. Niagara Region Personnel

Each individual that collects, uses, discloses, or disposes of information received as part of their duties as a Regional employee including personal information, is accountable for the actions they take with the information including ensuring the information is used only for the purpose it was obtained and is not disclosed to either other employees or non-employees except as permitted in accordance with this policy and applicable legislation whatever form the information is stored or transmitted in. All employees will:

a) Manage PHI that they collect, use, retain, disclose and dispose of for Regional business in accordance their college requirements (if applicable) and with this policy and its procedures to safeguard such information;
b) Take privacy training as required by their role, position, or in consultation with the Access and Privacy Office, to ensure the appropriate handling of personal information and to understand their responsibilities to protect privacy in executing their operational duties;
c) Ensure that PHI is only accessible and discussed by authorized users;
d) Be aware of their individual privacy responsibilities as defined by departmental, divisional, or program specific procedures for the collection, use, retention, disclosure, or disposal of personal information.

Each individual should be aware that non-compliance with PHIPA requirements, risks and consequences may include any or all of the following:

- Loss of trust or confidence in Niagara Region
- Cost and time in dealing with Privacy Breaches
- Legal liabilities and proceedings

- Investigation by privacy oversight bodies (IPC)
- Negative media coverage for Niagara Region, Regional departments services and programs

Definitions

Health Information Practices means in relation to one of Niagara Region's health information custodians, the policy of the custodian for actions in relation to "personal health information", including,

(a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and

(b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information.

Personal Health Information means all recorded information that is about an identifiable individual or is defined or deemed to be "personal health information" pursuant to any laws or regulations related to privacy or data protection that are applicable to the Regional Municipality of Niagara (including, without limitation, any information that constitutes "personal health information" as such term is defined by PHIPA).

PHIPA means the *Personal Health Information Protection Act* (Ontario) and its regulations, as amended from time to time.

Privacy Breach means any inappropriate or unauthorized collection, use, retention, disclosure, or disposal of personal information, as a result of a contravention of this policy, MFIPPA or PHIPA.

Privacy by Design means the consideration of privacy during the design process that integrates the protection of "personal information" directly into the technology/system through creation, operation, and management of the system or technology itself.

Privacy Incident means and inappropriate or unauthorized action that involves data, information or records which include "personal information" that may lead to the discovery of a "privacy breach".

4. References and Related Document

4.1. Legislation, By-Laws and/or Directives

Personal Health Information Protection Act, 2004 (PHIPA)

4.2. Procedures

C-XXX-000-001 **Formal Request for Records of Personal Health Information Procedure**

C-XXX-000-002 **Delegation of Authority to Agents of the Health Information Custodian**

5. Related Policies

C-XXX-000 Access to Information and Privacy Protection Policy

6. Appendices

Appendix A – List of Niagara Region's Health Information Custodians
Appendix B – Health Information Custodian Reporting Structure

7. Document Control

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

Approval History

Approver(s)	Approved Date	Effective Date

Revision History

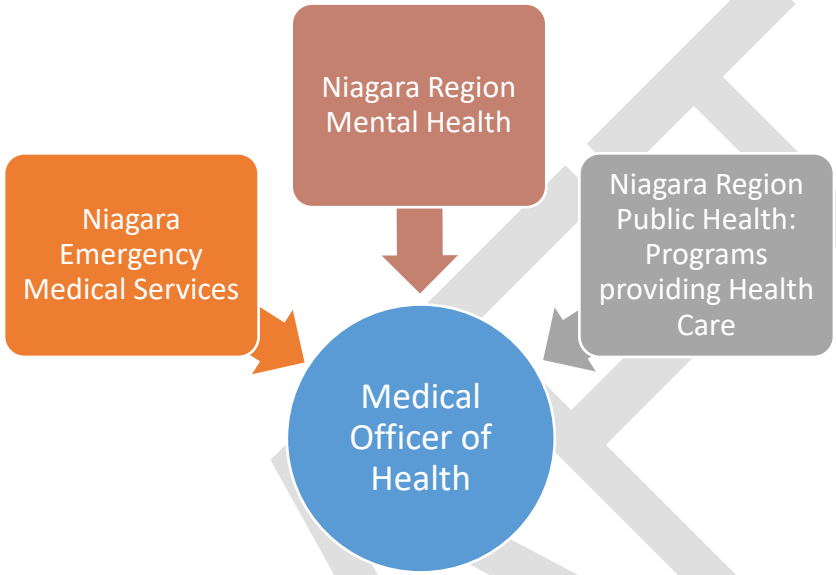
Revision No.	Date	Summary of Change(s)	Changed by

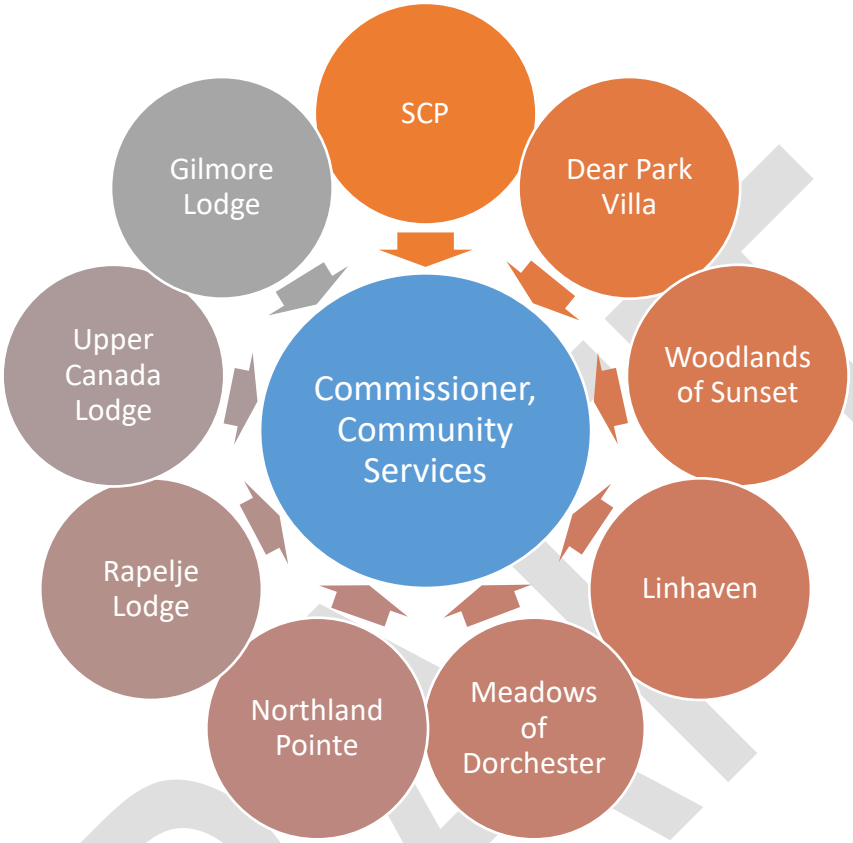
Appendix A – List of Niagara Region's Health Information Custodians

Niagara Region Operates with two distinct Health Information Custodians.

Health Information Custodians	**Agents (Associated Programs and Services)**
1. **Medical Officer of Health/ Commissioner Public Health**	Niagara Region Public Health programs providing health care
	Niagara Region Mental Health
	Niagara Emergency Medical Services
2. **Commissioner, Community Services**	Seniors Community Programs
	Deer Park Villa Long-Term Care Home
	Woodlands of Sunset Long-Term Care Home
	Linhaven Long-Term Care Home
	Meadows of Dorchester Long-Term Care Home
	Northland Pointe Long-Term Care Home
	Rapelje Lodge Long-Term Care Home
	Upper Canada Lodge Long-Term Care Home
	Gilmore Lodge Long-Term Care Home

Appendix B - Health Information Custodian Administrative Reporting Structure




SCP
Gilmore Lodge
Dear Park Villa
Upper Canada Lodge
Commissioner, Community Services
Woodlands of Sunset
Rapelje Lodge
Linhaven
Northland Pointe
Meadows of Dorchester