Notice No: 14-04

Niagara Regional Housing

APPLICABLE TO:

x	**Municipal & Private Non Profit**
x	**Co-operative**
x	**Federal Non Profit**
	OCHAP/CSHP
	Rent Supplement

DATE: March 31, 2014

x	**Mandatory**
	For Information

SUBJECT: ***Personal Information and Electronic Documents Act (PIPEDA)***

BACKGROUND

The *Personal Information Protection and Electronics Documents Act (PIPEDA)* was enacted on January 1, 2001. The Act applies to all private sector organizations and all organizations involved in commercial activity or regular activities that are commercial in nature.

NRH Notice #05-10 was issued in December 2005 requiring housing providers to establish policies and procedures related to the collection, use or disclosure of personal information in compliance with PIPEDA. Although some housing providers may fall under the *MFIPPA* legislation (i.e., Municipal Non-Profit Housing Corporations) or *FIPPA*, NRH recommended that the best approach to ensure protection of personal information is to have all housing providers comply with the requirements of *PIPEDA*.

Over the past few years, our operational reviews have found that some housing providers have not implemented appropriate policies and practices to safeguard personal information and reduce the risk of privacy breaches, or are not aware of their requirements under *PIPEDA*.

This Notice is issued to remind all housing providers of their requirements under *PIPEDA*. A copy of the full *PIPEDA* legislation can be found at: www.laws-lois.justice.gc.ca

REPORT

PIPEDA defines best business practices for the handling of personal information of RGI and market households, staff, board members, and other volunteers.

The following are examples of Personal Information:

1. Personal address, telephone number or email address of an individual
2. Any identifying number assigned to an individual which can lead to their identification (e.g., SIN)
3. Information about an individual's income and assets
4. Bank account and credit card information
5. Information about rent payment history

6. Information relating to the race, national or ethnic origin, citizenship status, colour, religion, age, sex, sexual orientation, marital or family status
7. Information relating to the education, medical, psychiatric, psychological, criminal or employment history of the individual
8. Credit and rental history reports
9. Financial information for the purposes of establishing Rent-Geared-to-Income Assistance
10. An individual's blood type or fingerprints
11. Information about an individual's political or personal opinions
12. Correspondence sent to the housing provider that is of a private or confidential nature, and any replies from the housing provider that would reveal contents of the original correspondence
13. The individual's name if it appears with other confidential information (i.e., rental arrears reports)
14. Employee information including resumes, salary and benefits, disciplinary action, bank account information, tenant complaints about the individual, and problems between staff.

Principles of *PIPEDA*

Appendix A lists the ten principles that all housing providers must adhere to related to personal information.

Housing Provider Responsibilities under *PIPEDA*

Appendix B lists the responsibilities of housing providers related to the *PIPEDA* requirements.

ONPHA and CHF have sample confidentiality agreements and sample policies for housing provider use.

Examples of Privacy Issues and Requests for Information

Over the past several years, NRH has received several inquiries from housing providers related to requests for information from tenants/members and the public.

As a general rule, each request should be reviewed on a case-by-case basis. If the provider has implemented the proper privacy policies and processes described in this Notice, they will be better positioned to respond appropriately to individual requests.

Appendix C lists several examples of privacy requests.

Video Surveillance Equipment

Video surveillance systems refers to video, physical, or other mechanical, electronic or digital surveillance systems or devices that enable continuous or periodic video recording, observing or monitoring individuals in open, public spaces.

Video surveillance equipment is appropriate to protect public safety as well as protect the property. However, the *Information and Privacy Commissioner of Ontario* has stated that "*pervasive, routine and random surveillance of ordinary lawful activities interferes with an individual's right to privacy."*

When contemplating the implementation of video surveillance equipment, providers should consider the following requirements:

- Video surveillance should be viewed as an exceptional step;
- System should be tailored to minimize the impact on privacy;
- Public should be advised that they will be under surveillance, through posted signs;
- Information collected through video surveillance should be minimized – use should be restricted, its disclosure controlled, its retention limited, and its destruction assured;
- Excessive or unnecessary intrusions on privacy should be discouraged (i.e., cameras should not be directed at individual's units);
- Security of the equipment should be assured;
- Individuals have the right to access their recorded personal information (blurring or blocking identities of others may be necessary to protect privacy of others);
- System should be subject to independent audit;
- Policy must be developed that clearly outlines the rationale, location, field of vision, who has access to operate system, etc.

<u>Acceptable Locations for Video Surveillance</u>:

- Video cameras can be placed in public hallways (however, the camera cannot be positioned to record the entrance and exit of a tenant/member from their specific unit)
- Cameras can be placed in stairwells and over all entrances into the building – front, side, and back doors;
- Cameras can be placed in designated common rooms;
- Cameras can be placed at the entrance or in the elevators;
- Cameras can be placed in parking lots;
- Cameras can be placed at the entrance to the office, but not in staff lunchrooms or staff meeting rooms.

<u>Unacceptable Locations for Video Cameras</u>:

- Video cameras should not be located in laundry rooms unless there is ongoing vandalism taking place in the laundry room. If installing cameras in the laundry room, tenants/members must be made aware and consent obtained;
- Video cameras should not be located in the garbage room – cameras can be positioned at the entrance of the garbage room at an elevated level so that a person's "headshot" is only captured; camera cannot record the garbage that is being disposed;
- Cameras cannot be placed in public washrooms or change rooms;
- Cameras cannot be positioned to record the entrance and exit of a tenant/member from their unit.

Refer to Notice #14-03 for more information on video surveillance.

This Notice is provided to housing providers as a general guideline. In all cases, housing providers must ensure they comply with the *PIPEDA* requirements in the collection, use and disclosure of personal information and ensure personal information is protected when responding to requests for access to personal information.

In cases where the request is unique or exceptional and the housing provider has concerns as to what can or cannot be provided to the requestor, the Board should seek legal advice.

Housing Provider's Role

Housing providers must review their existing policies and procedures related to privacy and protection of personal information, and make the necessary revisions to ensure compliance with *PIPEDA*, which includes establishing a proper Privacy Policy, appointing a Privacy Officer and ensuring that appropriate training is provided to board members and staff.

Housing providers should contact their applicable sector organization for forms, templates and information on training opportunities.

Service Manager's Role

NRH will review policies and procedures to ensure compliance with *PIPEDA* during the operational review process.

If you have any questions or concerns regarding this notice, please contact your Housing Administrator at (905) 682-9201.

_____
Lora Beckwith, General Manager

Enclosures:

1. Appendix A – Principle of PIPEDA
2. Appendix B – Housing Provider Responsibilities
3. Appendix C – Privacy Request Examples

Appendix A

Principle of PIPEDA

1. **Accountability**: a housing provider is responsible for the personal information under its control and shall designate an individual(s) who is/are accountable for the organization's compliance with the legislative requirements.

2. **Identifying Purposes**: the purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent:** The knowledge and consent of the individual is required for the collection, use, or disclosure of personal information.

4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. If an organization plans to use the information for a new purpose, they must again obtain the consent of the individual. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy:** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information, including measures such as locked cabinets, computer passwords, and encryption.

8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information (e.g, Privacy Policy posted in the office or distributed through the newsletter).

9. **Individual Access:** Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance:** An individual shall be able to challenge compliance with the above principles to the designated individual or individuals (Privacy Officer) accountable for the organization's compliance.

Appendix B

Housing Provider Responsibilities

1. Assign a Privacy Officer: providers are required to appoint a "Privacy Officer", who is accountable for ensuring that the provider follows legislative requirements.

   It is the responsibility of the Privacy Officer to ensure that systems are in place for obtaining consent, maintaining confidentiality and responding to requests for personal information. The contact information for the Privacy Officer must be made public.

2. Develop/Review Confidentiality or Privacy Policy: the provider is required to develop a policy that includes –
   a. Job description for privacy officer
   b. Description of the types of personal information that is collected, used and stored
   c. List of persons who have access to personal information
   d. List of all individuals and agencies with whom the provider will be exchanging personal information
   e. Description of the type of security systems that should be in place for the storage and retrieval of personal information
   f. A complaints procedure
   g. System for discarding information when the provider is no longer legally obligated to keep it

3. Review how personal information is currently collected and bring practices in line with legislation.

4. Educate board members and staff on their responsibilities and liabilities under legislation.

5. Have all board members and staff sign a confidentiality agreement.

6. Ensure there is a consent clause in the lease/occupancy agreement that identifies the agencies and individuals with whom providers may be exchanging information to confirm or establish a credit or rental history.

7. Ensure all documents used to collect personal information include:
   a. Consent for collection, verification and release of personal information
   b. Name and contact information for the privacy officer
   c. Statement that any complaints should be directed to privacy officer

Appendix C

Privacy Request Examples

1. **Requests for Individual's Own Information:** The provider's Privacy Policy should address the process of how tenants/members can review their own personal information. Staff will need to identify and retrieve the personal information and to make it available to the individual who has requested the information. According to legislation, the housing provider has 30 days to make the information available.

   Note: Care must be taken when giving individuals access to their own information to ensure that the privacy of others is protected. This may require a review of the file to remove third party information before the tenant/member reviews the file.

2. **Requests for public documents**: This request should be made in writing to the housing provider. Copies of the provider's audited financial statements, regular board minutes, capital plans, budgets, policies and procedures are all public documents and can be provided to the individual who made the request, within the same 30 day time period. Depending on the volume, a fee may be imposed to cover photocopying.

3. **Requests for other general records** of the housing provider, such as complete files or records which include the personal information of more than one person. This request must be made in writing and should include a fee. In these cases, it is recommended that the provider seek legal advice on what can be released, in light of the personal information contained in the documents. Based on the advice of the provider's lawyer, a decision is provided to the requestor within the 30 calendar day time frame.

4. **Requests for in-camera minutes** are not public documents, as they include individual's personal information which must be protected. In-camera minutes should be filed and stored in a secure location with restricted access.

5. **Requests for Information from Third Parties**: Generally speaking, personal information that is disclosed to third parties shall be done with the individual's knowledge and consent.

   However, *PIPEDA* permits disclosure of personal information, without the individual's knowledge and consent, to the following third parties or for the following reasons:

   a. Made to a barrister or solicitor who is representing the organization;
   b. For the purposes of collecting a debt owed by the individual to the organization;
   c. Required to comply with a subpoena or warrant issued or an order made by the court;

d. Made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information, and indicated that it suspects that the information relates to national security, the defense of Canada or the conduct of international affairs, or enforcing a law of Canada or carrying out an investigation;
e. Made to a person who needs the information because of an emergency that threatens the life, health or security of an individual;
f. For statistical or scholarly study or research, purposes that cannot be achieved without disclosing the information;
g. Made to an institution whose functions include the conservation of records of historic or archival importance;
h. Made after the earlier of i) 100 years after the record containing the information was created, and ii) 20 years after the death of the individual;
i. Required by law.

6. **Requests from Police:** Privacy legislation permits the disclosure of personal information to law enforcement agencies that requires the information for the purposes of carrying out an investigation related to a law enforcement proceeding.

In the case of law enforcement agencies, access to personal records are granted if a written request in the form of a subpoena or warrant is provided. The housing provider must respond to such a request with due diligence and in any case not later than thirty days after receipt of the request.

Subpoenas/Summons: Providers may be under the impression that because a subpoena or summons has been issued, they are obligated to release a record of personal information in advance to the police or to the party who has issued the subpoena or summons. The subpoena or summons authorizes a person to show up at a designated time to testify and to bring specific documents.

If the individual discloses the information prior to the hearing, that individual may be found to be in violation of *PIPEDA.*

Warrants: The police may obtain a search warrant which allows them to enter the named location to conduct a search for evidence with respect to the commission of an offense against the *Criminal Code* or other act of Parliament. Although law enforcement agencies are required to provide a warrant before information can be released, personal information can be released to the police without a warrant if:

- Staff have personal knowledge of a theft or damages to the premises
- Witnesses to crimes against persons are obligated to report and provide appropriate information to police
- If there are reasonable grounds to believe that a tenant has a substance abuse problem, the provider can disclose personal information relevant to remedying the specific incident.
- If the victim of the crime is a child or person with a disability that renders them incapable of making the decision to report