



Privacy

“Privacy Issues for Social Delivery Agents”

Ontario Access & Privacy Convention
October 26th, 2009

Social Housing Services Corporation, © 2009 All rights reserved.



- Acronyms gone wild (and they all sound the same!)
 - **PA** – *Privacy Act*
 - **PIPEDA** - *Personal Information Protection and Electronics Document Act*
 - **FIPPA** – *Freedom of Information and Protection of Privacy Act*
 - **MFIPPA** – *Municipal Freedom of Information and Protection of Privacy Act*
 - **PHIPA** - *Personal Health Information Protection Act*
- *Which apply to your organization?*



Key Privacy Challenges

- Understanding when information can be released and cannot be released
- Retention and Destruction of information (how long should it be kept, how should it be stored, how should it be destroyed)
- Dealing with 3rd party requests for information
- Consent of the client
- Correction of inaccurate client information



Key Privacy Challenges

- Inter-agency consent for mutual clients
- Surveillance cameras in social housing communities
- Dealing with police
- Emails, cell-phones, blackberries, internet



Disclosing to the Individual



Access by the Individual to his/her personal information

Disclosing to Third Parties



Consent from the Individual



Police with legal authority



What is Personal Information?

- or -

What needs to be kept in the vault?



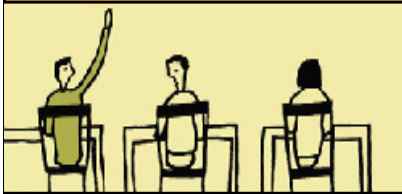
Definition of Personal Information

Information that can identify an individual

- The usual suspects: financial history, name, social insurance number...
- Lesser known suspects: political opinions, personal opinions, insurance information...

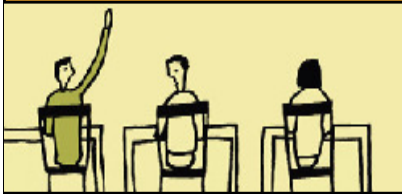


The 10 Principles of Privacy



The 10 Principles of Privacy

- Identifying the Purposes
- Limiting the Collection of Information
- Limiting Use, Disclosure and Retention of Information
- Accountability
- Accuracy
- Safeguards
- Openness
- Challenging Compliance
- Access
- Consent

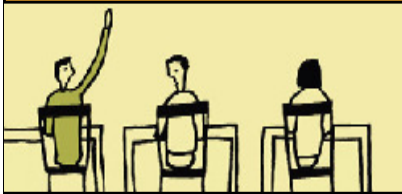


The 10 Principles - Simplified

- **Why** do you collect the information?
 - Identifying the purposes
- **What** do you collect to put in the vault?
 - Limiting the collection of information
- **How** do you set up a secure vault?
 - Accountability
 - Limiting use, disclosure and retention of information
 - Accuracy
 - Safeguards
 - Openness
 - Challenging compliance
- **When** do you allow information to leave the vault?
 - Access
 - Consent



Consent for Social Service Delivery Agents



Three Types of Consent

- When obtaining consent from an individual for the collection, use, and disclosure of their personal information, there are 3 types of consent that can be considered:
 - 1) Express Consent
 - 2) Implied Consent
 - 3) Deemed Consent



Three Types of Consent

1. Express Consent

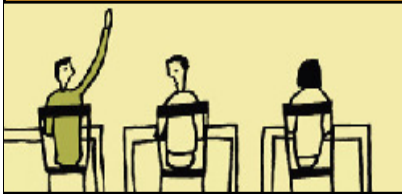
- Authorization has been obtained from the individual either in verbal or written format. Express consent is **indisputable!**
- Components of Express Consent include:
 - a) Signing a specific consent form
 - b) Providing a dated letter or other document authorizing certain activities
 - c) Providing an authorization electronically



Three Types of Consent

2. Implied Consent

- The housing provider has not received a specific authorization but the *circumstances* allow the housing provider to collect, use or disclose personal information
- Example of Implied Consent



Three Types of Consent

3. Deemed Consent

- Specifically deals with the posting of advertisements that may identify an individual specifically or the association of an individual with an organization
- This would not be necessarily applicable to social housing; however it is a form of consent that housing providers should be aware of
- Example of Deemed Consent



Dealing with 3rd Parties



When do you allow information to leave the vault?

Disclosing to Third Parties



Consent from the Individual



Police with legal authority



What is a Third Party?

- A person, group of persons, organization, or public body other than the individual whom the information is about and the organization or public body of that individual
- A **public body** includes a department, government agency, executive council office, Ministerial office, and a local public body of the municipality
- A **public body does not** include the office of a member of the Legislative Assembly who is not a Minister, or the Court of Appeal, the Court of Queen's Bench or the provincial government



Disclosing Information to Third Parties

- When transferring personal information to third parties **there should be** a privacy protection clause to guarantee that the third party entrusted with the information provides the same level of protection that your organization follows.
- Violation of privacy by a third party does not hold them accountable necessarily.
- Remember Principle 2: Limiting use, disclosure and retention of information



What a Third Party Privacy Contract Clause Should Contain

- a) Name of a person to handle all privacy aspects of the contract
- b) Limit the use of the personal information to the purposes specified to fulfill the contract
- c) Limit the disclosure of the information to what is authorized your organization or required by law
- d) Refer any people looking for access to their personal information to the appointed Privacy Officer for your organization



What a Third Party Privacy Contract Clause Should Contain

- e) Return or dispose of the transferred information upon completion of the contract
- f) Use of appropriate security measures to protect the personal information
- g) Allow your organization to audit the third party's compliance with the contract as necessary



Privacy and the Social Housing Reform Act, 2000



Differences Between SHRA and Privacy Legislation

- Privacy rules in the SHRA requires the holding of personal information for a specified period of time.
- Privacy rules in the SHRA allows housing providers to refuse access to personal information of a tenant or potential tenant.



Privacy and the Police



Overview

- Privacy legislation permits the disclosure of personal information where disclosure is to an institution or a law enforcement agency in Canada which assists in an investigation that may lead to a formal law enforcement proceeding.
- FIPPA, MFIPPA, and PIPEDA requires that a person seeking access to a record make a *written request* to the person in control of the record.



Types of Written Requests

Subpoena

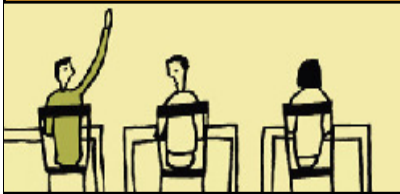
- Document issued by the court that compels an individual to appear in court at a specified time to provide testimony in a legal proceeding.
- A subpoena or summons may require an individual to bring specified documentation to the court proceeding.



Types of Written Requests

Warrant

- Authorized by a justice of the peace allowing a police officer or policing agency to enter a named location to conduct a search for specific evidence with respect to an offence under the Criminal Code or any other Act of Parliament.
- Before complying with an issued warrant, it is critical that the housing provider be sure that their rights and responsibilities are protected in respect of the warrant.



When Personal Information can be Released without a Subpoena or Warrant

- Housing provider staff have personal knowledge of a theft or damages to the premises or property of a tenant.
- Witnesses to crimes against persons are obligated to report and provide appropriate information to police.
- Reasonable grounds that a tenant has a substance abuse problem.
- If the victim of the crime is a child or person with a disability that renders them incapable of making the decision to report in the first case.

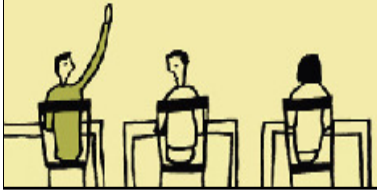


Surveillance Cameras



Overview

- Surveillance cameras are appropriate to protect public safety as well as protect the property of the housing provider.
- Surveillance cameras can act as a deterrent to criminal or negligent activity by tenants or visitors to the premises.
- The Privacy Commissioner of Ontario has publicly stated that *“pervasive, routine and random surveillance of ordinary, lawful activities interferes with an individual’s right to privacy”*.



Appropriate Video Surveillance Signage

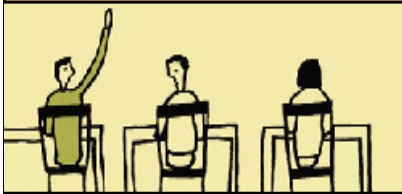
These premises are subject to

VIDEO SURVEILLANCE

WARNING

Video Surveillance is not intended
to be an emergency response system

**IN THE EVENT OF A
LIFE THREATENING EMERGENCY
CALL 911**



Video Surveillance Defined

- Video surveillance system refers to a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring individuals in open, public spaces.



Factors to Consider

- Should only be considered if other measures are rejected as unworkable
- The benefits of surveillance should substantially outweigh the reduction of an individual's privacy
- The use of video surveillance should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns



Where can video surveillance cameras be installed?

Cameras CAN be placed in:

- Designated common rooms
- Elevators
- Public hallways
- Stairwells
- Over all public entrances to the building
- The parking lot or underground parking
- Can be placed in common areas of offices.



Where should video surveillance cameras
NOT be installed?

Cameras should NOT be placed in:

- Laundry rooms
- Garbage rooms
- Public washrooms
- Areas that capture activities on tenant balconies
- Any staff lunchroom or meeting room



Privacy and the Internet



Overview

- Every housing provider who has a specific website or uses any form of “*search engine*” to identify and promote their organization must ensure that it:
 - a) discloses the fact that it uses “*cookies*” for tracking
 - b) explains the scope and purpose of each use
 - c) obtains consent to such use from the affected individuals
- Any on-line privacy policy must include an “*opt-out*” form of consent especially when dealing with sensitive information.



Email Addresses

- A personal e-mail address falls under the definition of personal information under privacy legislation.
- Housing providers seeking to collect and use e-mail addresses should ensure that the individuals disclosing such information are informed of the intended uses for their e-mail addresses.
- It is not permissible under privacy legislation to use e-mail addresses for *secondary* marketing purposes unless there is written consent in place.



Personal Health Information Protection Act, 2004



Overview

- This legislation governs *Health Information Custodians (HIC's)* that collect, use and disclose health or *Personal Health Information (PHI)*. This legislation also applies to Non-Health information custodians where they receive personal health information from a HIC.
- In the event of a conflict, PHIPA and its regulations **prevail over** any other Privacy Act unless PHIPA, its regulations and supporting directives specifically provide otherwise.



PHIPA and Consent

- Similar to all privacy legislation, consent is required for the collection, use or disclosure of personal health information subject to very specific exemptions.
- Consent must i) be a consent of the individual, ii) be knowledgeable, iii) relate to information, iv) not be obtained through deception or coercion.
- Consent may be implied between health information custodians for health care purposes; **HOWEVER**, express consent is required for disclosure to non-health information custodians (employer, health insurance company) or to health information custodians for non-health care purposes.



Persons Who May Consent

- Anyone over the age of 16 and capable to act on their own behalf
- If less than 16, a parent of the child, with some exceptions
- If incapable, a person authorized to consent on behalf of the individual under the Act
- If deceased, the estate trustee or the person who has assumed responsibility for the administration of the estate
- A person whom an Act of Ontario or Canada authorizes or requires to act on behalf of the individual



Questions



SHSC – Client Services

1-877-733-7472

1-877-733-SHSC

customercare@shscorp.ca