OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Municipalities Newfoundland and Labrador

Privacy Breach Training

Andrew Collins

November 14, 2019

Privacy – *ATIPPA, 2015*

Privacy under *ATIPPA, 2015* involves the protection of personal information from unauthorized collection, use and disclosure

Persons who believe there has been an unauthorized collection, use or disclosure of their personal information may file a complaint with the OIPC

What is Personal Information?

"Personal information" is defined as "recorded information about an identifiable individual." It includes, but is not limited to:

- name, address and telephone number
- race, ethnicity, religious or political beliefs
- age, sex, sexual orientation, marital status
- identifying numbers and symbols
- fingerprints, blood type and inheritable characteristics
- health care status or history
- educational, financial, criminal or employment status or history
- opinions about an individual

Collection (section 61)

Collection occurs when a public body gathers, acquires, receives, obtains or compiles personal information and then creates a record of that personal information

Collection must be limited to **minimum amount necessary** to accomplish the purpose

Forms of collection: written information (forms, applications etc.); verbal information then converted to writing (record created); video recordings; audio recordings; electronic media; and information transferred from another public body

Use (section 66)

"Use" means using personal information within the public body for the administration of a project or program

Public body may use personal information only:

- for the reason for which it was collected or a use consistent with that original purpose for collection
- where individual has consented to the use, or
- for a disclosure authorized by *ATIPPA, 2015*

Use must be limited to **minimum amount necessary** to accomplish the purpose

Disclosure (section 68)

"Disclosure" means showing, sending, or giving personal information to another division or outside department or agency

Disclosure must be limited to **minimum amount necessary** to accomplish the purpose

Public body may only disclose information with the consent of the individual; for the reason it was collected; to comply with another law or court order; to assist an investigation or law enforcement proceeding; or where in compelling circumstances that affect a person's health or safety (among others)

Protection (section 64)

Public bodies must take reasonable steps to ensure that:

- personal information is protected against theft, loss, unauthorized collection, access, use or disclosure
- records are protected against unauthorized copying or modification; and
- records are retained, transferred and disposed of securely

Public bodies may need to notify the individual of any theft, loss, improper disposal or unauthorized access or disclosure **unless the Public Body reasonably believes the loss does not create a risk of significant harm**

Safeguards

Common safeguards include:

- locked drawer or file cabinet
- locked office door
- keeping desks clean of files and records
- do not leave public body assets vulnerable (e.g. in the backseat of your car)
- encrypt emails containing sensitive information
- double check email addresses and fax numbers
- passwords – robust, no sharing, time-outs
- auditable networks, databases and shared drives

Privacy Breaches

A privacy breach occurs when personal information is inappropriately collected, used or disclosed

- Information is lost, stolen, or mistakenly disclosed
- Information is accessed without a legitimate work purpose

Personal information should be protected to ensure only persons with authorization handle it

Privacy Breaches

Common types of privacy breaches include:

- fax sent to the wrong number
- email sent to the wrong email address
- document placed in the wrong envelope

Other types of privacy breaches include:

- snooping in files
- providing information to an unauthorized recipient

Mandatory Breach Reporting

Public bodies must report **all** privacy breaches to the OIPC

Human errors are the most common cause of privacy breaches. Making a mistake is not an offense under *ATIPPA, 2015*, however hiding a privacy breach may be

There is no personal liability for a mistake under the *ATIPPA, 2015*. It is the Public Body that has the responsibility for ensuring compliance and it is the Public Body that the OIPC would investigate in the event of a complaint

It is incumbent on you to report breaches to your ATIPP Coordinator. The Coordinator must report it to the OIPC

Intentional Violation of Privacy

While mistakes happen, intentional violations of privacy should not. Every individual must take care not to violate another person's privacy

Section 115 of *ATIPPA, 2015* makes it an offence to willfully collect, use or disclose personal information in violation of *ATIPPA, 2015*. There is personal liability for these actions

Wilful privacy breach may result in a fine of up to $10,000 or imprisonment of up to 6 months, or both

A prosecution for such an offence must begin within 2 years of discovering the offence

Identifying Breaches

An employee had access to a database with client information

His son was having a birthday party and wanted to invite several friends. He had gone through the phone directory to get the address of a particular friend but it was not listed in the phone book

The father reasoned that, since his son could have obtained the address anyway, it was not really confidential in this case. Since it was also for a good cause and no real harm would be done, he looked up the information and provided it to his son

Identifying Breaches

THIS IS A PRIVACY BREACH

Employees of a Public Body must **NOT** access information without a legitimate work purpose

Identifying Breaches

A customer receives invoices by mail, and the envelope contains additional invoices relating to other individuals or businesses

Identifying Breaches

THIS IS A PRIVACY BREACH

Misdirected mail pose a risk of unauthorized disclosure and represent an unsafe transfer of information

Employees must take steps to double and check and confirm contents of mail-outs, including when automated processes are being used

Public body responded by providing additional training for employee

Identifying Breaches

A government employee has access to the support enforcement database

She is aware that her neighbour's ex-husband has been ordered to pay child support

The employee is curious as to whether the ex-husband has been making support payments on time and so accesses the database out of curiosity to see the payment history of the ex-husband

Identifying Breaches

THIS IS A PRIVACY BREACH

Employees of a Public Body must **NOT** access information without a legitimate work purpose

Even if the neighbour had requested that the employee access the file, it would be inappropriate for an employee to circumvent the typical processes at their workplace

Identifying Breaches

Employee emailing document related to a customer's account to another employee accidentally sent it to a distribution group and message was received by 239 employees

Identifying Breaches

THIS IS A PRIVACY BREACH

Misdirected emails pose a risk of unauthorized disclosure and represent an unsafe transfer of information

Public Body took steps to attempt to recall the message

Affected individual was notified

Responding to a Breach

When responding to a breach:

1) contain the breach
2) evaluate the risks
3) notification
4) prevention

Notification Required

Notification of a breach **must** be given to the OIPC

Notification should also be given to:

- ATIPP Office (if core government)
- in certain cases, the affected individual(s)

Notifying the Individual

The *Act* requires you to notify an individual when their personal information has been:

- stolen, lost, disposed of improperly or disclosed to, or accessed by an unauthorized person

OIPC may also recommend notification (see, for example, P-2018-006)

Notification is not required where the public body "reasonably" believes there has been no risk of significant harm

Notifying the Individual

Significant harm is defined as “bodily harm, humiliation, damage to reputation or relationships, loss of employment or professional business opportunities, financial loss, identity theft, negative effects to credit record or damage to or loss of property”.

When considering whether harm is significant put yourself in the affected party’s shoes.

You must consider the sensitivity of the information and probability of misuse (section 64(9))

Reporting to the OIPC

OIPC privacy breach notifications are generally used for statistical purposes only

We do this in order to identify trends in order to provide training. We recognize human error as a factor

Notification may also form the basis of an own motion investigation if it is indicative of an egregious situation

If a privacy complaint is received in relation to a notification, the OIPC will open an investigation

OIPC Privacy Investigation

Questions for OIPC investigation

- what happened?
- how did it happen?
- why did it happen?
- how will you prevent it from happening again?
- recommendations of how you can improve your compliance with *ATIPPA, 2015*

OIPC Privacy Investigation

The goal of the OIPC is to assist public bodies to comply with the *Act* more effectively

We evaluate your process as it existed at the time of the breach, including:

- safeguards and security measures
- policies and procedures in place; and
- communication and training about privacy

When we do our investigation we hope to leave your process in a better position than it was at the time of the breach

OIPC Recommendations

At the conclusion of an investigation the OIPC is empowered to make recommendations:

- to stop collecting, using or disclosing personal information in contravention of *ATIPPA, 2015*
- to destroy personal information collected in contravention *ATIPPA, 2015*; or
- in relation to any other way to improve compliance

OIPC Recommendations

Recommendation types 1 and 2 must be accepted by the Public Body within 10 business days or application must be made to the Court to disregard the recommendations

Accepting the recommendations (by default or by choice) requires that they be implemented within one year

Resources

Office of the Information and Privacy Commissioner

https://www.oipc.nl.ca/

(709) 729-6309
commissioner@oipc.nl.ca

ATIPP Office

https://www.atipp.gov.nl.ca/

(709) 729-7072
atippoffice@gov.nl.ca

Questions