Perspective patronale en droit de l'emploi et relations de travail
Labour and Employment Law for Employers

Emond Harnden LLP

PRIVACY LAW UPDATE

PART I - PHIPA
PART II – PIPEDA UPDATE

STEVEN WILLIAMS

September 28, 2004

www.emond-harnden.com

PART I - PHIPA

ONTARIO'S NEW HEALTH PRIVACY LAW

SCHEDULE A
THE PERSONAL HEALTH INFORMATION PROTECTION ACT, 2004 (PHIPA)

- PHIPA is the part of Bill 31 (HIPA) which will govern the manner in which personal health information may be collected, used and disclosed within the health care system.

- PHIPA will also regulate individuals and organizations that receive personal information from health care professionals.

WHAT DOES PHIPA DO?

- PHIPA creates a “level playing field” for all health care professions by building upon and codifying existing high standards and protections enshrined in the common law, various professional codes, policies, and guidelines.

WHAT DOES PHIPA DO? (con'd)

- PHIPA gives individuals greater control over the collection, use, and disclosure of their personal health information:
  - It requires patient consent for the collection, use and disclosure of personal health information, with limited exceptions.
  - It gives individuals the right to understand the purposes for the collection, use and disclosure of personal health information
  - Individuals may withdraw consent by providing notice to the health information custodian

WHAT DOES PHIPA DO? (con'd)

- PHIPA confirms a patient's existing right to access one's own personal health information, and to correct errors therein.
- It provides health care professionals with a flexible framework to access and use health information as necessary in order to deliver adequate and timely health care.
- It sets guidelines for the use and disclosure of personal health information for research purposes.

TO WHOM DOES PHIPA APPLY?

- PHIPA applies to a wide variety of individuals and organizations within the health care sector, defined as ***health information custodians***.

- A ***health information custodian*** is a listed individual or organization under PHIPA that, as a result of their power or duties, has custody or control of personal health information (eg. Health care practitioners, pharmacies, nursing homes).

TO WHOM DOES PHIPA APPLY? (con'd)

- PHIPA also applies to ***agents***.
- PHIPA defines an ***agent*** as any person who is authorized by a health information custodian to perform services or activities on the custodian's behalf and for the purposes of that custodian.
- An ***agent*** may include a company or person that contracts with (or is employed by) a health information custodian and as such, would have access to personal health information.

WHAT IS "PERSONAL HEALTH INFORMATION?"

- PHIPA defines ***personal health information*** as "identifying information" collected about an individual.
- The information can be in oral or written format
- It is information about an individual's health or health care history relating to:
  - Physical or mental condition, including family medical history
  - ***Provision of health care*** to the individual
  - Long-Term health care services
  - Health Card number

WHAT IS "PERSONAL HEALTH INFORMATION?" (con'd)

- Payment or eligibility for health care
- The identity of a health care provider or a substitute decision maker
- Blood or body part donations

- If the information is maintained primarily for a purpose *other* than the provision of health care (ie. Sick leave, insurance benefits, accommodation) it is not considered personal health information

WHAT DOES THE "PROVISION OF HEALTH CARE" MEAN?

- Any observation, examination, assessment, care, service, or procedure provided for health care purposes that is carried out:
  - To treat, diagnose, or maintain an individual's physical or mental condition
  - To prevent disease or injury, or promote health care
  - For, or part of, palliative care

WHAT DOES THE "PROVISION OF HEALTH CARE" MEAN? (con'd)

- Provision of health care also includes:
  - The compounding, dispensing, or selling of a drug, device, or equipment pursuant to a prescription
  - A community service described in the *Long-Term Care Act, 1994*

WHAT MUST HEALTH INFORMATION CUSTODIANS DO?

- PHIPA requires health information custodians (HICs) to establish and implement information practices that comply with the provisions of the act
- However, their existing policies and practices do not need to be completely set aside
- PHIPA builds upon existing guidelines and policies for health care professionals and provides enforceable rules regarding the collection, use or disclosure of personal health information

WHAT MUST HEALTH INFORMATION CUSTODIANS DO? (con'd)

- PHIPA requires HICs to:
  - Obtain an individual's consent when collecting, using, and disclosing personal health information, except in limited circumstances
  - Collect personal health information appropriately by lawful means and for lawful purposes
  - Collect no more personal health information than is reasonably necessary

WHAT MUST HEALTH INFORMATION CUSTODIANS DO? (con'd)

- PHIPA requires HICs to:
  - Take reasonable precautions to safeguard personal health information (even when it is used and disclosed outside of Ontario) including:
    - Protection against theft or loss
    - Protection against unauthorized use, disclosure, copying, modification or destruction
    - Notification to an individual at the first reasonable opportunity if the information is stolen, lost or accessed by an unauthorized person

WHAT MUST HEALTH INFORMATION CUSTODIANS DO? (con'd)

- PHIPA requires HICs to:
  - Ensure health records are as accurate, up-to-date and complete as necessary for the purposes which they use or disclose personal health information
  - Ensure health records are stored, transferred, and disposed of in a secure manner
  - Inform an individual of any uses and disclosures of personal health information without the individual's consent that occurred outside the custodian's information practices

WHAT MUST HEALTH INFORMATION CUSTODIANS DO? (con'd)

- PHIPA requires HICs to:
  - Designate a contact person who is responsible for:
    - Responding to access/correction requests
    - Responding to inquiries about the custodian's information practices
    - Receiving complaints regarding any alleged breaches of PHIPA
    - Ensuring overall compliance with PHIPA

WHAT MUST HEALTH INFORMATION CUSTODIANS DO? (con'd)

- PHIPA requires HICs to:
  - Provide a written statement that is readily available to the public and describes:
    - A custodian's information practices
    - How to reach the contact person
    - How an individual may obtain access, request a correction or make a complaint regarding his/her personal health information

WHAT MUST HEALTH INFORMATION CUSTODIANS DO? (con'd)

- PHIPA requires HICs to:
  - Ensure that all agents of the custodian are appropriately informed of their duties under PHIPA

SO WHAT ABOUT EMPLOYERS? (con'd)

- Employers handle medical information in a variety of contexts:
  - Certifying illness to support absence from work
  - To confirm entitlement to medically related benefits
  - Accommodating disabled employees
  - Managing workplace accidents

BUT WHAT ABOUT PIPEDA?

- Do organizations need to comply with both PIPEDA and PHIPA?

- As of January 1, 2004, PIPEDA has applied to all private sector organizations (pharmacies, laboratories, health care providers) with operating practices that qualify as “commercial activities”.

BUT WHAT ABOUT PIPEDA? (con'd)

- It is expected that the federal government will deem PHIPA to be "substantially similar" to PIPEDA. Health care providers covered under PHIPA will therefore be exempted from also complying with PIPEDA.

- BUT…PIPEDA will continue to apply to all commercial activities relating to the exchange of personal health information ***between*** provinces and territories and to information transfers ***outside*** of Canada.

PHIPA LINKS

Information and Privacy Commissioner/Ontario

http://www.ipc.on.ca

- click on "NEW – Ontario Health Privacy Legislation"

Ministry of Health and Long-Term Care

http://www.health.gov.on.ca/english/public/updates/archives/hu_03/priv_legislation.html

PART II

PIPEDA UPDATE

TOPICS OF DISCUSSION

1. VIDEO SURVEILLANCE AND PIPEDA

2. PRIVACY LAW IN THE UNIONIZED WORKPLACE: THE JURISDICTION OF GRIEVANCE ARBITRATORS

3. RECENT DECISIONS OF THE PRIVACY COMMISSIONER OF CANADA

VIDEO SURVEILLANCE AND PIPEDA

- Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada

- Privacy Commissioner of Canada - Decision #273

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FACTS

- The Canadian Pacific Railway ("CP") installed 6 digital recording surveillance cameras in their mechanical facility area at Scarborough, Ontario to:
  - reduce vandalism/theft,
  - reduce CP's potential liability for property damage
  - provide security for staff
- Eastmond, an employee of CP and a member of CAW-Local 1001, made a complaint to the Privacy Commissioner of Canada

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) COMMISSIONER'S REPORT

- In examining Eastmond's complaint, the Privacy Commissioner set up a four part test to determine whether CP's use of the video cameras was reasonable:
  1. Is the measure demonstrably necessary to meet a specific need?
  2. Is it likely to be effective in meeting that need?
  3. Is the loss of privacy proportional to the benefit gained?
  4. Is there a less privacy-invasive way of achieving the same end?

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) COMMISSIONER'S REPORT (con'd)

- The Privacy Commissioner held that Eastmond's complaint was well founded. A reasonable person ***would not*** consider the circumstances sufficient to warrant this intrusive measure;
  1. A demonstrable need for the cameras had not been proven;
  2. Adverse psychological effects due to the privacy invasion could be occurring;
  3. Other alternatives existed (eg. Increased lighting) to meet CP's purposes for the video cameras;

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FEDERAL COURT DECISION

- The Federal Court of Canada adopted the same four-part test but determined that a reasonable person ***would*** consider CP's purposes appropriate in the circumstances:
  1. The court held that "*CP has established a legitimate need to have the cameras installed where they were ….*"
  2. The court held that the camera surveillance and recording *would* be likely to be effective in meeting its need.

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FEDERAL COURT DECISION (con'd)

3. On the third part of the test, the court held that *"the loss of privacy is proportional to the benefit gained,"* and highlighted the following points:
   - the collection of personal information is not surreptitious. Warning signs are displayed.
   - The collection of personal information is not continuous and is not limited to CP employees. The collection is not to intended measure work performance
   - the recorded images are locked up and only accessed by responsible managers and CP police, and *only* if there is an incident report. If there are no incidents recorded, the recordings are destroyed within an appropriate time frame.

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FEDERAL COURT DECISION (con'd)

4. On whether or not there was a less privacy-invasive way of achieving the same end, the court held that it was satisfied that CP had looked at all alternatives and concluded that these measures were not cost effective and would be disruptive to CP's operations

- *Eastmond* makes it clear that an organization must balance its right to reduce property and security risks with the privacy rights of its employees

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 273

FACTS

- A broadcasting company employer installed video surveillance cameras at the workplace based on recommendations from a workplace security review

COMPLAINT

- Employees lodged several complaints that the cameras were being used to collect their personal information about behaviour and work performance

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 273

SUMMARY OF INVESTIGATION

- The employer said that a memo had been posted to notify the employees about how the information being collected would be used.
- The employees were not aware of the memo.

COMMISSIONER'S FINDINGS

- The Assistant Commissioner concluded that reasonable efforts had not been made to inform the employees.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 273

COMMISSIONER'S FINDINGS (con'd)

- The use of the cameras was an appropriate means of protecting the employees.
- The employer was not required to obtain employee consent as the cameras were not used to collect personal information and were not used in places were there was a reasonable possibility of invasion of privacy.
- If the cameras did inadvertently collect employee personal information, the personal information could only be used without consent in the circumstances set out in 7(2)(a) and (b) of PIPEDA.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 273

COMMISSIONER'S FINDINGS (con'd)

The Assistant Commissioner concluded that the complaint was ***resolved*** insofar as the firm**:**

1. Ensures its employees are informed of the purposes for which the cameras are being used;
2. Develops a policy on the use of surveillance cameras that is readily available to its employees

PRIVACY LAW IN THE UNIONIZED WORKPLACE:

THE JURISDICTION OF GRIEVANCE ARBITRATORS

- L'Ecuyer v. Aeroports de Montreal

- Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada

L'Ecuyer v. Aeroports de Montreal (2003) FACTS (review)

- Complainant, Ms. L'Ecuyer, lodged a harassment complaint against her supervisor
- Soon after, she made five requests for access to her personal information (re: complaints against her and disciplinary letters)
- The employer's HR Director refused her request in a letter

L'Ecuyer v. Aeroports de Montreal (2003) FEDERAL COURT DECISION

- Neither the Federal Court nor the Privacy Commissioner had the jurisdiction to review the employer's actions.
- Instead, jurisdiction fell under the grievance arbitrator
- "If the dispute between the parties in its 'essential character' arises from the interpretation, application, administration or violation of the collective agreement, it is to be determined by an arbitrator appointed in accordance with the collective agreement and not by the Courts." [*Weber*]

L'Ecuyer v. Aeroports de Montreal (2003) FEDERAL COURT DECISION (con'd)

- This is the case here. Everything involved in her applications flowed from the unionized workplace context (ie: her original harassment complaint, her request for her disciplinary files, her union members being copied on the correspondence, and so on)

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FACTS (review)

- The Canadian Pacific Railway ("CP") installed 6 digital recording surveillance cameras in their mechanical facility area at Scarborough, Ontario

- Eastmond, an employee of CP and a member of CAW-Local 1001, made a complaint to the Privacy Commissioner of Canada

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FEDERAL COURT DECISION

- Before addressing whether CP was in breach of its PIPEDA obligations, the court first addressed CP's jurisdictional argument.

- CP, relying on *Weber* and *L'Ecuyer v. Aeroports de Montreal,* stated that neither the federal court nor the Privacy Commissioner in its initial ruling had jurisdiction to hear this complaint.

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FEDERAL COURT DECISION (con'd)

- CP argued that the dispute arose from the interpretation, application, administration, or violation of the collective agreement between CP and the Union. The dispute should, therefore, be resolved through arbitration proceedings.

- The court rejected this argument.

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FEDERAL COURT DECISION (con'd)

- The court made this jurisdictional ruling on the following points:
- First, the statutory jurisdiction of PIPEDA as set out in the conditions of s.14 have been met.
- Second, the exclusive arbitration model set out in *Weber* does not apply. It was not the intention of parliament to automatically exclude unionized workers from the scope of PIPEDA. Two statutory regimes can exist concurrently.

Eastmond v. Canadian Pacific Railway & Privacy Commissioner of Canada (2004) FEDERAL COURT DECISION (con'd)

- The court also stated that section 13 (2)(a) gives the Privacy Commissioner the discretion to investigate a complaint or defer it if alternate grievance or review procedures were appropriate.
- On these grounds, the court stated that an arbitrator would not have had jurisdiction in this case.

RECENT DECISIONS OF THE PRIVACY COMMISSIONER OF CANADA

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 274

FACTS

- A man received a call from a research firm company. The company received the man's information from his cell phone service provider.
- The man called his cell phone company but was unsuccessful in obtaining information about the call and why his personal information was being disclosed to this third party.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 274

COMPLAINT

- The complainant was not upset about the call, but the fact that no one from the cell phone company could confirm that the call was legitimate.

SUMMARY OF INVESTIGATION

- The cell phone company provided the research firm with the information. The privacy brochure did state it might disclose personal information for this purpose and stated customer's could opt-out of this activity.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 274

SUMMARY OF INVESTIGATION (con'd)

- The cell phone company called the complainant to apologize for the lack of information and explain the purpose of the call from the research firm.
- Representatives were provided with an information package so they could better respond to such inquiries.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 274

COMMISSIONER'S FINDINGS

The Assistant Commissioner concluded that the complaint was ***resolved.***

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 272

FACTS

- An individual's credit card application was refused. The individual wrote to the bank and requested access to the personal information gathered about him.

COMPLAINT

- That the bank did not respond to his request for personal information.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 272

SUMMARY OF INVESTIGATION

- The bank stated it attempted to contact the individual a number of times and left messages.
- The bank then sent a written reply more than 38 days after receipt of the request
- The bank was unable to provide a copy of the credit bureau request because it is only retained for three months if credit is refused. The information had already been destroyed at the time of the information request.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 272

SUMMARY OF INVESTIGATION (con'd)

- The bank further maintained it complied with the one-month time period due to the telephone call attempts.

COMMISSIONER'S FINDINGS

- The bank did not retain the record long enough to allow the individual access to it, in violation of subsection 8(8) & principle 4.5.2
- The bank should have replied in writing within 30 days of the request.

PRIVACY COMMISSIONER OF CANADA CASE SUMMARY # 272

COMMISSIONER'S FINDINGS (con'd)

The Assistant Commissioner therefore concluded that the complaint was ***well-founded***

QUESTIONS