

Privacy: Best Practices

Presented to:

*Nova Scotia Board of Examiners in Psychology /
Association of Psychologists of Nova Scotia*



Jennifer Gray

October 29, 2004



NOVA SCOTIA • NEW BRUNSWICK • NEWFOUNDLAND AND LABRADOR • PRINCE EDWARD ISLAND

Presentation Outline

- Introduction
- Module 1: Setting the Stage
 - Existing obligations pre-January 1, 2004
 - The new privacy landscape post January 1, 2004
 - *Personal Information Protection and Electronic Documents Act* (“PIPEDA”)
- ~ BREAK ~
- Module 2: Privacy Compliance
 - Privacy and Your Office
 - Privacy and Research
 - Privacy and Business



Introduction: Goals

- Through this seminar you should:
 - Gain a basic understanding of the regulation of privacy in Nova Scotia and Canada, in particular, for psychologists;
 - Learn how to recognize a “privacy issue” in your practice; and
 - Know how to respond (or at least where to go to get more information!).



Introduction: privacy v. confidentiality

■ **Privacy**

- The quality or condition of being secluded from the presence or view of others
- The state of being free from unsanctioned intrusion
- The right to be “left alone”

■ **Confidentiality**

- the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them
- One observes rules of confidentiality out of respect for privacy



Introduction: a right to privacy?

■ What is the “Right to Privacy”?

- Not traditionally a “right” at common law
- Recognition that in today’s society, it is impossible to be “left alone”, but we should be able to limit intrusions on our privacy
- Confidentiality of the doctor/patient relationship
- More recently, there has developed the concept of the right to control access to one’s information about oneself (federal Privacy Commissioner)
- Developing “right” through legislation



Module 1: Setting the Stage

Regulation of Privacy



Outline for Module 1

- Brief history of privacy regulation
- Existing obligations of psychologists pre-2004
- PIPEDA
 - Purpose and overview
 - The principles
 - Key issues
 - How PIPEDA is enforced?



Brief history of privacy regulation in Canada

- 1983
 - Federal public sector privacy legislation (really just government)
- 1993
 - Nova Scotia enacts public sector privacy legislation
 - Quebec recognizes the right to privacy in the *Civil Code of Quebec* and enacts the first private sector privacy legislation
- late 1990s
 - Increasing pressure from the EU for data protection legislation
 - The federal government seeks to increase consumer confidence in e-commerce and online transactions
 - 1996: Canadian Standards Association
- 2001
 - PIPEDA is enacted (in stages, 2001, 2002 and 2004)
 - January 1, 2004 – private sector dealings



The shift: 2004

- prior to January 1, 2004
 - the private sector was largely self-regulated in the areas of privacy and personal information
- January 1, 2004
 - PIPEDA came into force with respect to all organizations that use personal information in the course of commercial activities, self-regulated or not



Pre-2004 obligations of psychologists

- *Canadian Code of Ethics for Psychologists* (3rd ed., 2000)
 - Principle I: Respect for the Dignity of Persons
- *NSBEP Standard of Professional Conduct*
 - Principle 7
- *NSBEP Standards for Providers of Psychological Services*
 - Principle 2.3.5
- *Psychologists Act* (Nova Scotia)
 - Section 32: confidentiality in the discipline process



Pre-2004 obligations of psychologists

- *Hospitals Act* (Nova Scotia)
 - hospitals (including health authorities generally)
 - Section 71: confidentiality of records “concerning a person or patient in the hospital or a person or patient formerly in the hospital”
- *Freedom of Information and Protection of Privacy Act* (Nova Scotia) (“FOIPOP”)
 - “public bodies”
 - government
 - universities
 - hospitals



...and then came PIPEDA

- Federal legislation
 - Part 1: *Protection of Personal Information in the Private Sector*
- Came into force in April of 2000 (in three stages)
- Third stage (January 1, 2004)
 - PIPEDA now extends to **all organizations that carry out commercial activities within a Province**, unless the Province has passed a “substantially similar legislation” to that of PIPEDA
 - Currently only Quebec has passed legislation which meets this test
 - The Atlantic Provinces do not have such legislation
- Unusual in that it incorporates a CSA standard into law



PIPEDA: purpose

■ Section 3

■ "...to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."



Who is subject to PIPEDA?

■ Ironically the title is...

■ "An Act to support and promote *electronic commerce* by protecting personal information that is collected, used or disclosed in certain circumstances..."

■ PIPEDA applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activity.

■ Not just electronic commerce – large impact on health care



Important definitions

■ "organization"

■ Includes an association, partnership, a person and a trade union

■ "personal information"

■ Information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization

■ "commercial activity"

■ Any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists



Overview: the ten principles

- Organizations that are subject to PIPEDA must comply with the following ten principles from the *CSA Model Code for the Protection of Personal Information* when engaging in the collection, use and disclosure of personal information:

- ✓ **Accountability**
- ✓ **Identifying purposes**
- ✓ **Consent**
- ✓ **Limiting collection**
- ✓ **Limited use, disclosure, retention**
- ✓ **Accuracy**
- ✓ **Safeguards**
- ✓ **Openness**
- ✓ **Individual access**
- ✓ **Challenging compliance**



The principles

■ **Accountability**

- An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

■ **Identifying purposes**

- The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.



The principles

■ **Consent**

- The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

■ **Limiting collection**

- The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.



The principles

■ 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.

■ 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.



The principles

■ Safeguards

- Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

■ Openness

- An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.



The principles

■ 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.

■ Challenging Compliance

- An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.



Key issues: consent

- Of the 10 principles, obtaining “knowledge and consent” of the individual is the key principle
 - knowledge = informed choice
 - communicate:
 - why you are collecting personal information
 - what you are going to do with the personal information
 - to whom you may disclose personal information
 - new purposes/uses, should these arise following collection



Other key issues

- Access
 - Individuals have a right of access to their personal information held by organizations and to correct and update personal information as necessary
- Grandfathering
 - No grandfathering! All information collected before January 1, 2004 is also subject to PIPEDA



PIPEDA: consent requirement

- Informed
- Meaningful
- Person giving consent should understand of the purposes for which the information will be collected, used and disclosed
- Be aware of the sensitivity of the information
- Understand the expectations of the individual
- Manner of obtaining consent may vary with the type of personal information in question
 - Express consent
 - Opt out consent
 - Implied consent



When is consent not required?

■ *Collection*

- Collection that is in the interest of the individual and consent cannot be obtained in a timely way
- Where knowledge and consent would compromise availability/accuracy and the information is part of an investigation of a breach of an agreement or contravention of law
- Collection for journalistic, artistic, literary purposes
- Information that is “publicly available” as defined in the regulations



When is consent not required?

■ *Use*

- Use in the investigation of a contravention of law
- Emergencies that threaten life, health or security of the individual
- Study/research
 - impractical to obtain consent
 - inform the Privacy Commissioner
- Information that is “publicly available”
- When collected without consent in accordance with the previous slide



When is consent not required?

■ *Disclosure*

- To a solicitor
- For collection of a debt
- In accordance with a subpoena, warrant, court order
- Lawful request of government
- To or by an “investigative body” as defined in the regulations



When is consent not required?

■ Disclosure

- Emergency
- Public information
- Study/research
- To government (crime, national defence)
- After time has passed
 - 100 years after record was made
 - 20 years after death of individual
- Preservation of historic/archival records
- *As required by law...*



Exceptions to access: the hot topic

- Can refuse access only if...
 - solicitor-client privilege
 - confidential commercial information
 - if it would reveal personal information about **another individual** unless there is consent from that individual
 - could reasonably be expected to threaten the life or security of another individual
 - if the organization has disclosed information to a government institution for law enforcement or national security reasons
 - the information was generated in the course of a formal dispute resolution process



Enforcement

- Enforced through the **Office of the Privacy Commissioner** (acts as an Ombudsman)
- Complaint-driven process; however, Commissioner can unilaterally investigate or audit
- Broad powers of investigation, including:
 - subpoena of witnesses
 - entry onto premises
 - inspection of documents
 - compliance audits of organizations
 - public disclosure of organizational practices
 - reference to the Federal Court for remedies and enforcement



Enforcement

- Office of the Privacy Commissioner
 - Investigates
 - Completes a report
 - Makes recommendations
 - Federal Court (hearing and penalty)



Enforcement

- If the Federal Court determines that there has been a violation of PIPEDA it has the power to:
 - order an organization to correct its practices;
 - order publication by the organization of its corrective action;
 - award damages to the complainant (including for humiliation); and/or
 - levy a monetary fine (on summary conviction \$10,000 or on an indictable offense \$100,000).



Are you subject to PIPEDA?

- ✓ *Do you carry on commercial activities in Canada?*
- ✓ *In the course of carrying on those commercial activities, do you collect, use or disclose personal information?*



End of Module 1



Module 2: Privacy Compliance



Outline for Module 2

- Privacy compliance
 - Privacy and your office
 - Implementing an internal privacy compliance program
 - Best practices
 - consent
 - grandfathering
 - Privacy and research
 - Privacy and business



Are you subject to PIPEDA?

✓ Do you carry on commercial activities in Canada?

Yes

✓ In the course of carrying on those commercial activities, do you collect, use or disclose personal information?

Yes



Should I panic?

■ **Yes and no.**

- While compliance with PIPEDA was required as of January 1, 2004, psychologists are likely generally compliant with respect to clients, so long as they are adhering to their pre-2004 obligations
- However, you now have additional obligations with respect to personal information of third parties, not just your clients



Should I panic?

■ **Risks of being non-compliant**

- public attention
- order of the Privacy Commissioner
- Federal Court
- risks outside of PIPEDA – professional misconduct

■ **Risk mitigation.** Every day your practice is non-compliant with PIPEDA is a risk to you and/or your organization



Privacy and your office

- Appoint a privacy officer
- Conduct a personal information audit
- Develop a privacy policy and procedures
- Review your practices
- Communicate with clients and staff



Compliance: privacy officer

- Assist the individual in getting up to speed on all of your personal information handling practices
- If an existing employee, lighten existing duties to give time to develop policies and procedures
- Involve the person in the personal information audit and the development of the privacy policy
- Empower the individual to enforce compliance with internal policies
- Involve the person in staff training
- Encourage continuous education in the area of privacy



Compliance: audit practices

- *What personal information do we collect?*
- *Why do we collect it?*
- *How do we collect it?*
- *What is it used for?*
- *Where do we keep it?*
- *How is it secured?*
- *Who has access to or uses it?*
- *To whom is it disclosed?*
- *When and how is it disposed of?*



Compliance: privacy policy

- Why have one?
 - A place to outline the purposes and description of uses of personal information
 - Mechanism to give public notice of existence of your privacy officer
- Available...
 - upon request
 - web site
 - print form



Compliance: privacy policy

- Think of this document as a both a risk management tool and a marketing tool
- Risk management tool:
 - Follow the ten principles
 - Communicate the policy internally
 - Get your practices in place to ensure compliance with the policy
- Marketing tool:
 - Communicate to your clients that your privacy policy exists (e.g., provide a link to it on your web site)
 - Demonstrates that you are sensitive to privacy issues



Privacy policy & procedures

- Principle 1 - Accountability
 - define the purposes for collecting the personal information
 - inform and train staff on privacy policies and procedures
 - make information available explaining your practice's privacy policies and procedures to clients
 - include a privacy protection clause in contracts with third parties to guarantee that third parties provide the same level of protection as you do



Privacy policy & procedures

■ Principle 2 - Identifying purposes

- review the current personal information holdings to ensure that they are all required for a specific purpose
- notify the individual, either orally or in writing, of the purpose the personal information is being collected
- record all identified purposes and obtain consents



Privacy policy & procedures

■ Principle 3 - Consent

- consent must be "fully informed"
- record that consent was received
- do not obtain consent by deception
- do not use consent as a condition for supplying the service, unless it is required to fulfill a specific purpose
- explain consequences of withdrawing consent
- obtain consent (where possible) for personal information already collected prior to January 1, 2004



Privacy policy & procedures

■ Principle 4 - Limiting collection

- limit the amount and type of information gathered to what is necessary for the identified purposes



Privacy policy & procedures

■ Principle 5 - Limiting use, disclosure and retention

- institute maximum and minimum retention periods for personal information
- dispose of personal information that does not have a specific purpose or that no longer fulfills its intended purpose
- dispose of personal information in a manner that prevents improper access



Privacy policy & procedures

■ Principle 6 - Accuracy

- keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interests of the individual
- establish policies setting out the types of personal information that need to be updated
- update personal information when necessary to fulfill the specified purpose
- ensure that the date on which all pieces of personal information is collected is noted



Privacy policy & procedures

■ Principle 7 - Safeguards

- develop and implement a security policy to protect personal information
- use appropriate security measures to protect personal information
- remove or hide irrelevant personal information from documentation supplied to others
- keep sensitive information in a secure area and limit access to an on a "need-to-know" basis
- impress upon your employees the importance of maintaining the security and confidentiality of personal information



Privacy policy & procedures

■ Principle 8 - Openness

- name the privacy officer
- name the person to which access requests should be sent
- develop a procedure to see personal information
- develop a procedure to make a complaint
- provide information explaining your privacy policy
- describe what personal information will be made available to other organizations



Privacy policy & procedures

■ Principle 9 - Individual Access

- remember that individuals can request to see their personal information
- respond within 30 days
- provide access at minimal or no cost and inform individual of cost prior to processing request
- make sure personal information is understandable to individual
- if you refuse access, provide individual with written explanation



Privacy policy & procedures

■ Principle 10 - Challenging Compliance

- record date of complaint
- acknowledge receipt of complaint promptly
- assign investigation to qualified individual (must be fair and impartial)
- provide investigator with access to all relevant records
- notify individual of the outcome of the investigation clearly and promptly



Review practices and procedures

- Security of, and access to, paper files
- Security of, and access to, information systems
 - computer database systems
 - electronic files
 - firewalls, password protection, etc.
- Dealings with third parties who handle personal information on your behalf



Review practices and procedures

- Education of staff
 - terms of employment contract?
- Storage, retention and disposal of information
- Disaster recovery

...Revisit procedures regularly!



Privacy best practices: consent

- Consent
 - express/positive/opt-in
 - strongest form of consent – generally required
 - use wherever appropriate
 - especially important in relation to the sensitivity of the personal information in question
 - negative/opt-out
 - non-sensitive in nature
 - purpose for use limited and well defined
 - must establish a convenient method for opting out and such opt-out must take effect immediately
 - consent mechanism (i.e., check-off box) must be clear and unambiguous



Privacy best practices: consent

- Consent
 - implied
 - where consent is reasonably inferred from the action or inaction of the individual
 - whether the individual would reasonably expect that the personal information would be used or disclosed in the proposed manner
 - e.g., sensitive v. non-sensitive information
 - context will dictate whether appropriate!



Privacy best practices: grandfathering

- Consent is required for this information
- However, *express* consent is not always required
 - purge older files if no legal requirement to retain
 - consent - express or implied
 - reasonable expectation of individual?
 - new purposes/unanticipated secondary use?
 - contact client base to advise of privacy policy



Privacy and research

- Interagency Advisory Panel for Research Ethics
 - *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TPCS)*
 - Ethics review - consent
 - Section 3: "Privacy and confidentiality"
 - personal interviews
 - surveys, questionnaires and collections of data
 - secondary use
 - data linkage



Privacy and business

- Third party disclosures of personal information
 - insurance companies
 - employers
 - government
 - contractors with your practice (e.g., computer support)
- Make sure your client consents and/or privacy policy covers disclosures to third parties
- Analyze each disclosure
 - Do I have consent?
 - If not, is there an exception under PIPEDA for disclosure which applies to this disclosure?



Privacy and business


- Disclosure/Personal Information agreements
 - key terms
 - scope of disclosure
 - restriction on use
 - return or destruction
 - notification of leaks or complaints against third party
 - indemnity
- Limit the amount of information disclosed to third parties to only that which is “reasonably necessary” in the circumstances
- Use secure methods of information transfer



Respecting privacy and personal information is just good practice!



End of Module 2

 PATERSON PALMER
Law


For More Information

Office of the Privacy Commissioner
<http://www.privcom.gc.ca>

Jennifer Gray
Business and Technology Practice Group
jgray@pattersonpalmer.ca

 PATERSON PALMER
Law

Questions?

 PATERSON PALMER
Law
