

How the New Privacy Legislation Affects You and the Practice of Veterinary Medicine in Ontario

Richard Steinecke
January 29, 2004

Some Views on Privacy

- "Secrecy is the badge of fraud." Sir John Chadwick (b. 1941), British judge.
- "Secrecy is a disease and Chernobyl is its symptom, a threat both to the Soviet Union and its neighbors." New York Times Editorial, May 1, 1986
- "Three may keep a secret if two of them are dead." Benjamin Franklin *

Some Views on Privacy

- "Friends, if we be honest with ourselves, we shall be honest with each other." George MacDonald
- "The price of justice is eternal publicity." Arnold Bennett (1867 - 1931)
- "He who trusts secrets to a servant makes him his master." John Dryden *

Privacy vs. Confidentiality

- Gather only what you need vs.
 - Keep what you gather secret
- Use info only for purpose gathered vs.
 - Use info for internal purposes only
- Keep info for minimum time for purpose vs.
 - Keep info forever *

Privacy vs. Confidentiality

- Access by person to info about them vs.
 - No access to info unless your rights in jeopardy
- Right to correct wrong info vs.
 - Keep info as originally gathered
- Accountable both internally and externally vs.
 - Very limited accountability, to courts only *

PIPEDA

- *Personal Information and Protection of Electronic Documents Act*
- PIPEDA sets out rules for how private sector may collect, use or disclose personal information in the course of commercial activities
- As of January 1, 2004, PIPEDA covered commercial activities within all provinces
- Provincial legislation is being introduced for personal health information only *

Who is Covered by PIPEDA

- PIPEDA covers:
 - A. Any organization
 - B. That engages in a commercial activity
 - C. Involving personal information
- Very few exceptions *

7

A. Any Organization

- An organization can be:
 - a single individual (e.g., a sole proprietorship)
 - a partnership
 - a corporation
 - an association of individuals, partnerships and/or corporations
- Some flexibility and choice by parties
 - E.g., multiple or related practices
- See Checklist page 1 *

8

B. Commercial Activity

- “Commercial Activity” is defined, sort of
 - “means 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”
- Intended to capture as broad a range of transactions involving the collection, use or disclosure of information as possible *

9

B. Commercial Activity

- Likely includes:
 - Private practice of veterinary medicine
 - Even if paid by the government
- Likely does not include
 - Employed by the government
 - Employment by a University
 - Except for private services offered on the side
 - What if the University operates a hospital that charges
 - Hiring & firing employees (except federal sector) *

10

B. Commercial Activity

- It is the nature of the activity that is most important, rather than the nature of the organization
- A non-profit organization is still capable of engaging in commercial activity
 - If it did, then that particular transaction would be subject to PIPEDA *

11

B. Commercial Activity

- Exceptions
 - Government activities
 - Covered by own privacy legislation
 - Household use only
 - E.g., personal address book, if no work entries
 - Artistic, journalistic or literary activities
 - Freedom of expression under Charter
 - E.g., news organizations, novels
- See Checklist page 2 *

12

C. Personal Information

- “Personal Information” is defined, sort of
 - “means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization” *

13

C. Personal Information

- Extremely broad definition
- Open-ended, no list of examples
- Not limited to recorded information
 - E.g., unrecorded information
 - E.g., tissue samples
 - E.g., live feed videotape *

14

C. Personal Information

Likely includes:

- Home contact information
- Identification numbers (SIN, driver’s licence)
- Information about a person’s pet
- Human rights characteristics (e.g., age, race)
- Financial information
- Health information about a person
- Criminal history
- Misconduct history

See Checklist bottom of page 2 *

15

Requirements of PIPEDA

- Every organization must have a Privacy Code that meets the 10 principles of PIPEDA
- Form the basic rules for the collection, use and disclosure of personal information *

16

10 Principles

- 1. Accountability
- 2. Identifying Purpose
- 3. Consent
- 4. Limiting Collections
- 5. Limiting Use, Disclosure and Retention *

17

10 Principles

- 6. Accuracy
- 7. Safeguards
- 8. Openness
- 9. Individual Access
- 10. Challenging Compliance
- Those 10 principles have been operationalized for you into 6 steps *

18

Step 1 – Information Officer

- Must have an “Information Officer”
 - Often called a Privacy Officer
- Information Officer must:
 - Review organization’s information practices
 - Develop and implement Privacy Plan
 - Train staff
 - Monitor compliance
 - Be contact person for information questions *

19

Step 1 – Information Officer

- Characteristics of a good Information Officer
 - Senior position in the organization
 - Familiarity with how information is collected, stored, used and disclosed in the organization
 - Experience with human resources management
 - Experience with customer relations
 - Comfort level with legal matters
- See Checklist page 1 *

20

Step 2 – ID Personal Information

- What personal information do you collect?
 - See Checklist page 5
 - May have to review files
 - Both paper and electronic
 - May have to survey staff
 - List needs to be complete and exhaustive
 - Can use categories
 - E.g., info from health assessment
 - Try to note where information is kept *

21

Step 2 – ID Personal Information

Categories of individuals you collect info about

- Pets of Clients
- Clients
- Prospective clients, general public
- Contract staff
 - E.g., non-employees, volunteers, students
- Investigations, audits etc.
 - E.g., insurance consults, third party assessments
- Other *

22

Step 3 – Identifying Purpose

Reasons for identifying purpose:

1. Need to set out, in writing, in privacy policy
 - People have the right to know
2. Need to limit as much as possible
3. Need authority to collect, use and disclose
 - Most common authority is consent
 - Some exceptions where consent not required *

23

Step 3 – Identifying Purpose

- Types of purposes for collecting, using and disclosing personal information
 - Primary purpose
 - E.g., assessing and treating pets of clients
 - Related purpose
 - E.g., billing clients, recall visit notices
 - Secondary purpose
 - E.g., QA, special offers, regulatory accountability
- Must identify all purposes *

24

Step 3 – Identifying Purpose

- Example of a primary purpose - veterinary
 - Purpose: Our primary purpose for collecting personal information about you is to provide your animal with veterinary services
 - Description: We collect information about your animal's history, physical condition and function in order to help us assess what their needs are, to advise you of your options and then to provide the veterinary care you choose.
- See Guide p. 20 *

25

Step 3 – Identifying Purpose

- See Guide, Pp. 20-21: veterinary sample for
 - Clients
 - Members of the General Public
 - Contract Staff, Volunteers and Students *

26

Step 3 – Identifying Purpose

Related and secondary purposes

- Invoicing and collection
- Recall visits
- Special offers and promotions
- Quality control and risk management
- External regulation
- Third party billing
- Responding to questions
- Sale of business *

27

Step 3 – Identifying Purpose

- Related and secondary purposes tend to apply to everyone
 - No choice about some, like external regulation
 - People need to know even if there is no choice
 - Some, like invoicing and collection, only apply to some categories of people
- See sample at Guide, Pp. 21-22 *

28

Step 3 – Identifying Purpose

Collect only what is necessary for the purpose

- Probably does not prevent collection of usual baseline information
 - Probably liberally applied in veterinary context
 - Might need to explain, so client has choice
- But no need to collect SIN in most cases
 - No need to collect financial info if no credit
- Review what is a "necessary" part of history*

29

Step 3 – Identifying Purpose

- Must limit use and disclosure to what is reasonably necessary for purpose
- Need to continually rethink processes
 - Do we need to include name on every page?
 - What is necessary for report back to referring veterinarian?
 - Is a report back necessary?
 - Can we reasonably restrict staff access to files? *

30

Step 3 – Consent to Purpose

- General rule, must obtain consent for collection, use and disclosure
- Means explaining to clients what information you are collecting and why
- Implications for indirect collection (e.g., consults)
 - How do you get consent?
- What about animal family histories?
 - Probably characterized as info about patients, not other pets per se *

31

Step 3 – Consent to Purpose

- Manner of obtaining consent, varies with
 - Sensitivity of the information (e.g., health information, financial information)
 - Reasonable expectations of the individual
 - Context (e.g., a written consent is difficult to obtain over the phone)
- Can be implied, verbal or written
 - Risk of implied consent for related purposes
- Opt out consent inappropriate in many cases
- See Consent Form – Guide page 16 *

32

Step 3 – Consent to Purpose

Rare exceptions to consent principle

- E.g., collection is in interest of person & timely consent not possible (i.e., emergency)
- E.g., to investigate breach of law / agreement
 - E.g., collection of unpaid accounts
- E.g., publicly available information specified in regulation (e.g., telephone directories, professional directories, statutory registries, court or tribunal records) *

33

Step 3 – Consent to Purpose

Public Information Exceptions

- (a) personal information consisting of the name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory *

34

Step 3 – Consent to Purpose

Public Information Exceptions

- (b) personal information including the name, title, address and telephone number of an individual that appears in a professional or business directory, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the directory, listing or notice *

35

Step 3 – Consent to Purpose

Public Information Exceptions

- (c) personal information that appears in a registry collected under a statutory authority and to which a right of public access is authorized by law, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the registry *

36

Step 3 – Consent to Purpose

Public Information Exceptions

- (a) personal information that appears in a record or document of a judicial or quasi-judicial body, that is available to the public, where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document
- E.g., HPARB *

37

Step 3 – Consent to Purpose

Public Information Exceptions

- (e) personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information *

38

Step 3 – Consent to Purpose

- Process to follow in identifying purpose
 - See Checklist, page 4
 - Fill in primary purposes
 - For each category of individuals
 - Purposes
 - Authority
 - Type of personal information collected
 - Fill in related and secondary purposes (Pp. 6-12)
 - For each purpose applicable to your organization
- Then do Privacy Policy (Guide, Pp. 20-22) *

39

Step 3 – Consent to Purpose

- Principles of Use and Disclosure
- Personal information can only be used or disclosed for the purpose for which it was obtained unless:
 - Further consent is obtained, or
 - There is legal authority to use or disclose the information without consent
- Thus need for a complete consent at the start
 - E.g., if want to sell business later *

40

Step 3 – Consent to Purpose

Use of personal information without consent

- An emergency that threatens the life, health or security of an individual
- For the investigation of a breach of law in Canada or elsewhere
- Publicly available information specified in regulation (e.g., telephone directories, professional directories, statutory registries, court records & info volunteered to newspapers, magazines & books)
- Specific research situations (obtain legal advice) *

41

Step 3 – Consent to Purpose

Disclosure of personal info without consent

- To the organization's lawyer
- For debt collection purposes
- To comply with subpoena, warrant or court order
- At the request of a government institution for national security, law enforcement or administration
- To a specified investigative body relating to law enforcement *

42

Step 3 – Consent to Purpose

Disclosure of personal info without consent

- Where there is an emergency that threatens the life, health or security of an individual
 - Must then advise in writing right away
- Publicly available info specified in regulation
- 20 yrs after death or 100 yrs after record made
- Specific research situations (get legal advice)
- Where disclosure is required by law *

43

Step 4 – Safeguards Etc.

- Safeguards must include
 - Physical measures
 - E.g., restricted access areas, locked cabinets
 - Organizational measures
 - E.g., need-to-know & other employee policies
 - E.g., security clearances
 - Technological measures
 - E.g., passwords, encryption, virus protection, firewalls
- See Checklist Pp. 14-17 *

44

Step 4 – Safeguards Etc.

Location of Paper Information

- Office areas restricted to staff
- Office areas open to non-staff
 - Non-staff supervised at all times or
 - All personal info locked away when staff absent
- While in transit to another location
- Home office *

45

Step 4 – Safeguards Etc.

Location of Electronic Information

- Office areas restricted to staff
 - Non-staff permitted only with continuous monitoring
 - Non-staff with access (e.g., cleaners) must give confidentiality assurances
 - Password protection for each terminal
 - Password protection for screen saver on each terminal
 - For more sophisticated networks, unique user identifiers, audit trails, and intrusion detection systems
 - For wireless networks, consult an expert *

46

Step 4 – Safeguards Etc.

Transfer of Paper Information

- In sealed envelope, marked private and confidential, sent by Canada Post or reputable courier
- In sealed envelope, marked private and confidential, delivered by staff
- In sealed envelope to be picked up by person who asks for it by name of recipient (files kept out of sight in reception area until picked up) *

47

Step 4 – Safeguards Etc.

Transfer of Electronic Information

- Through a direct line that is password protected
- Through email or other internet communication where
 - Consent of the person to whom info relates
 - E.g., the client requests email communication
 - Where the message is anonymized
 - Encryption is used
- Through a disk, CD or other storage medium
 - Treated with the same safeguards as paper info *

48

Step 4 – Safeguards Etc.

Faxes

- Through fax with a cover sheet identifying the recipient with privacy clause on it and where
 - Fax number has been approved by the recipient
 - Recipient says fax machine is securely located
 - Privacy of the recipient can reasonably be inferred
 - E.g., to an organization that is expected to keep information private, like a law office
 - Recipient has a Privacy Policy
- Your incoming fax machine is securely located *

49

Step 4 – Safeguards Etc.

Websites

- Website use of personal information is:
 - Encrypted
 - Appropriate website cookies policy *

50

Step 4 – Safeguards Etc.

Staff (including temporary workers) training on:

- Importance of the privacy of personal information
- Access on a need-to-know basis
- On the organization's Privacy Policy
- Sensitivity in conversations where others overhear
- Remove or mask unnecessary personal information
- Recognize and avoid being "pumped" for information
- Shred info, not regular garbage or blue box
- Avoid discussing personal information in public
- Breach of policies will result in discipline
 - Even dismissal *

51

Step 4 – Safeguards Etc.

- Duty to ensure accuracy
- Must take reasonable steps to ensure information is accurate
- Implications
 - Confirm with client?
 - Update with client on subsequent visits?
 - Can you rely on certain laboratory results? *

52

Step 4 – Safeguards Etc.

Privacy and security agreements with

- Temporary workers
- Cleaners
- Information technology consultant
- Marketers
- Lawyers
- Bookkeepers and accountants
- File storage service
- Credit card companies
- Website manager
- Premises security agency
- Building maintenance
- Landlord *

53

Step 4 – Safeguards Etc.

- Regular and systematic monitoring of compliance with the organization's policies by the Information Officer
- Regular and systematic auditing of the electronic safeguards by an external company
- Policy to notify individuals where their personal information is misused or misappropriated
- Review physical layout and procedures
 - E.g., use rooms rather than cubicles for interviews
 - E.g., waiting room concerns *

54

Step 4 – Safeguards Etc.

Retention of Client Files (see page 18 of Checklist)

- Minimum and maximum retention period
 - working notes & unnecessary copies destroyed earlier

Retention for General Correspondence

Retention for Newsletters, Seminars & Marketing

- Minimum and maximum retention period
- Remove upon request or when notice is not needed
 - Impractical to regularly remove information *

55

Step 4 – Safeguards Etc.

Destruction of Personal Information

- Shredding (paper files)
- Deletion (electronic records where hard drive or storage vehicle is retained)
- Physical destruction or complete reformatting (where hard drive etc. is discarded)
- Return all or part of the file to client *

56

Step 4 – Safeguards Etc.

Recurring problems

- Non-compliant organization sends you private personal information by email and wants you to reply by email
- Exempt organization (e.g., non-profit) wants an email that will contain lots of private personal information
- Client consents to email communication but your message refers to third parties *

57

Step 5 – Access & Correction

- Individuals generally have the right to access personal information you hold
- Individual need not be a client
 - E.g., prospective client
 - E.g., supplier (re personal performance)
 - E.g., contact directory (your address book)
- See Checklist page 19 *

58

Step 5 – Access & Correction

- Some Grounds for Refusing a Request
 - The information reveals personal information about a third party unless
 - Third party info cannot be severed
 - The third party consents or
 - An individual's life, health or safety is threatened
 - Information relates to a warrant, subpoena, disclosure to a government institution or to an investigative body (get legal advice)
 - Information is solicitor and client privileged *

59

Step 5 – Access & Correction

- Some Grounds for Refusing a Request
 - Information would reveal confidential commercial information, unless it can be severed
 - Revealing the information threatens life or security of another individual unless it can be severed
 - Information was collected without consent to investigate a breach of an agreement or law
 - Must tell Information and Privacy Commissioner
 - Information from formal dispute resolution process
 - E.g., CVO complaints procedure, ADR *

60

Step 5 – Access & Correction

Providing Access

- Must respond within 30 days
 - Some extensions are possible
- Must confirm the identity of person getting it
- Ensure that person can understand it
 - E.g., explain short forms or codes
 - E.g., provide in alternative format where disability
- Access to how you have used / disclosed info
 - Thus need to record this fact *

61

Step 5 – Access & Correction

Person has right to correct errors

- If agree you must make correction
- If disagree must file notice of disagreement
 - Just factual errors or also disputed opinions?
 - What about original entry?
- Must give notice of correction, or notice of disagreement, to third parties
 - Thus need to record this fact *

62

Step 5 – Complaints System

Internal complaints system

- Designated individual to receive and respond
- Accessible and simple complaints procedure
 - Acknowledge receipt of the complaint
 - Investigate the complaint
 - Provide a decision with reasons
- Respond appropriately where justified
- Notify public of external recourses
 - E.g., Information & Privacy Commissioner *

63

Step 5 – Complaints System

Information and Privacy Commissioner

- Investigates complaints about an organization's personal info handling practices
 - E.g., enter premises, interview staff, review records
 - E.g., summoning documents and witnesses
- Mediates and conciliates such complaints
- Audits personal information handling practices
- Makes public reports of abuses
- Seeks remedies for breaches in Federal Court *

64

Step 5 – Complaints System

- Federal Court of Canada remedies
 - Order for the organization to correct its personal information handling practices
 - Order for the organization to publish a notice of corrective action
 - Award of damages for any humiliation
- See Checklist page 20 *

65

Step 5 – Openness

- Must have a written privacy policy
 - Can have shorter and longer documents
- Must make available to public
 - E.g., brochure
 - E.g., website
 - E.g., on request
- To anyone, not just clients
- Staff must know policies and be able to answer questions
- See Checklist page 21 *

66

Step 6 – Implementing Your Plan

Initial Implementation

- Complete the Checklist
- Develop your consent form (Guide Form 1)
- Write out your Privacy Policy (Guide Form 3)
- Initial staff training
- Obtain assurances from external consultants and outsourced providers
- Privacy Policy document posted publicly *

67

Step 6 – Implementing Your Plan

Ongoing implementation

- Monitoring compliance with Privacy Policy
 - Prepare a report annually
- External information technology audit (annual)
- Refresher training session for all staff (annual)
- Review and update of Privacy Policy (annual) *

68

Other Resources

- Information & Privacy Commissioner of Canada
 - www.privcom.gc.ca
- Ontario Information & Privacy Commission
 - www.ipc.on.ca
- CVO website
 - www.cvo.org
- Our firm's website
 - www.sml-law.com

69