PIPEDA in the Dental Office

INDEX

PAGE

PREFACE

This discussion paper, **PIPEDA IN THE DENTAL OFFICE**, is produced by the Nova Scotia Dental Association. It is produced for the members of the Association and their staff. Its purpose is to assist our members comply with the federal Personal Information Protection and Electronic Documents Act.

This discussion paper has been prepared by staff of the Association. Staff has carried out a review of the Act and has reviewed numerous discussion papers and commentaries produced by various organizations across the country including the Privacy Commission and the Canadian Standards Association. The interpretations, advice, counsel and suggestions contained in this discussion paper are the staff's best efforts at applying the requirements of the Act to the dental office. The Act and Privacy Commission reference material are available as follows: The Privacy Commissioner of Canada 112 Kent Street, Ottawa, ON K1A 1H3 Tel.: 1 (613) 995-1376 Fax 1(613) 947-6850 Email:info@privcom.gc.ca.,www.privcom.gc.ca.

Legal Disclaimer:

The information provided in this discussion paper is intended to be used for guidance and assistance and is for general information purposes only. The material reflects interpretations and practices regarded as valid as of the date the document was released based on the available information at that time. It is not intended as legal advice on any particular fact or activity. Members and others should consult legal counsel on any specific matter related to the requirements of the dentist to comply with any law.

******Reproduction or use of the material and contents in whole or in part by any person other than a member of the Nova Scotia Dental Association is prohibited without written consent and a published acknowledgement.******

INTRODUCTION

On January 1, 2004, PIPEDA (Personal Information Protection and Electronic Documents Act) becomes effective for all **commercial organizations** and will affect a dentist as a provider of dental services. Accordingly, you are required to actively participate by protecting the **personal information** of patients in accordance with the Act. Failure to comply may result in a Privacy Commission investigation and confirmed contraventions carry strict penalty.

Personal Information includes

but is not restricted to name, age, weight, height, health information, medical records, income, race, ethnic origin, religion, blood type, DNA code, fingerprints, marital status, education, spending habits, home address, home phone and fax numbers, and home email.

An Organization is

any association, partnership, person or trade union engaged in a commercial activity. This includes a dentist conducting a dental practice.

Commercial Activity is

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 membership lists.
This includes practicing Dentistry.

What You Must Do…. & Suggestions For How To Do It….

As a Provider of Dental Services

As a Dental Care Provider here is a description of what you must do and suggestion for how to do it, to comply with the Personal Information Protection and Electronic Documents Act (PIPEDA).

A. GENERAL

1) Privacy Officer

The Act requires each organization be responsible for the management of personal information within its possession by complying with the 10 principles of PIPEDA.

(**APPENDIX 1**)

What you must do is….

Designate a person to ensure compliance and oversee the dental office's collection, retention, use and disclosure of personal information. This person will be the internal advisor on all privacy related matters, and will have the authority to intervene when necessary and will be the public's first contact for privacy matters.

Suggestions for how to do it…

The person can be the dentist or an employee. If the person is not the dentist, delegate the responsibility for privacy issues to a specific employee who will be responsible to the

dentist for overall compliance with the Act. Give the designated privacy officer the authority to intervene on privacy issues. Communicate the name of this individual internally and externally on forms, websites, etc. It must be noted that designating a privacy officer does not relieve the dental practice from complying with the Act. In other words, a dentist would not be able to defend a complaint on the basis that his or her privacy officer was in charge of ensuring compliance.

2) Privacy Policy

Each organization must develop and implement policies and procedures to protect personal information in its possession.

What you must do is….

develop a written privacy policy for your dental office that includes identification of a privacy officer and identifies the practice's obligations for protecting information. It will need to address policies in place concerning consent, distribution, retention and safeguards for personal information. The policy must state the individual's right to access their information and note the existence of a complaint mechanism available to them.

Suggestions for how to do it…

Sample Privacy Policy (APPENDIX II)

Analyze personal information handling practices in your office and prepare a policy document reflecting the practice's commitment to each of the 10 key principles of PIPEDA. Define the purposes for collecting data as clearly and narrowly as possible explaining how information will be used and disclosed.

3) Accuracy of Information

The Act states that organizations have a responsibility to keep information accurate, complete and up-to-date.

What you must do is….

ensure patients review their personal information regularly. You should advise patients to contact the dental office if there are changes to their information.

Suggestions for how to do it…

Keep each patient's personal information up to date. Review current records in advance of a patient's arrival for treatment and encourage each patient to provide an update if information has changed. On the patient record make a note of the date the personal information was changed or updated and record the method of information gathering (i.e. personal visit, by telephone, email).

4) Complaint Process

You are required to investigate privacy complaints and to provide recourse via the privacy officer

What you must do is….

develop written procedures for addressing a challenge to the dental office's compliance with its privacy obligations. Encourage patients to address concerns with the collection, use or disclosure of their personal information.

Suggestions for how to do it…

Complaint System Considerations (APPENDIX III)

Prepare a written statement, using the checklist, which describes the complaint process in existence in your dental office. Investigate all complaints received through the Privacy Officer. Record the date a complaint is received and the nature of the complaint (e.g. improper release, incomplete consent). Acknowledge receipt of complaint promptly and clarify the nature of the complaint. Provide the patient access to all relevant records. Notify the complainant of the outcome of investigations and inform them of the steps you have taken to resolve their complaint. Note decisions in the patient record. Your complaint investigation and resolution processes must be consistent (from complaint to complaint).

5) Patient Access

Patients have the right to access all of their personal information held by you.

What you must do is….

establish procedures to respect the patient's right to access information held by the dental office.

Suggestions for how to do it…

Ensure that all staff are made aware of the patient's right to access personal information and that staff actions respect the policy of openness. Provide assistance to individuals requesting access to their personal information. Respond to requests as quickly as is reasonably possible, no later than 30 days after receipt of the request. Give access at cost recovery or no cost to the individual and if there is a cost notify the individual before processing the request. Make sure the information you supply is understandable and does not use acronyms,

abbreviations or dental jargon. Methods of access can be personal review of the record or copies of the record. The patient has a right to the information in their record but does not own the physical record. Patients may be denied access in specific cases only. Seek further counsel before denying access.

B. CONSENT

1) Privacy Statement for Patients

You are required to provide a privacy statement to every patient that describes and explains the policies and procedures for administration of personal information, of patients of the dental office.

What you must do is….

prepare a statement addressing the use, disclosure and retention of personal information collected from a patient assuring openness and compliance under the Act.

Suggestions for how to do it…

See Privacy Statement/Consent Form (APPENDIX IV)

Create a privacy statement to be provided to every patient or that is made visible to patients in the dental office. The privacy statement will explain your processes and procedures for collecting, using, storing and disclosing the patient's personal information. Examples of purposes for dental offices to collect, use, store or disclose personal information include; providing care, opening an account, referrals to a specialist or sending information to a benefit provider.

2) Provide a Consent Form

The privacy statement and the consent form may be combined. Written consent is the preferred manner to gain patient consent for collection, use, disclosure, and retention of personal information. Wherever possible, obtain written consent. Other forms of consent, including implied consent, may be acceptable in some circumstances however, the safest alternative is written consent. Parents and guardians may provide consent for a minor.

What you must do is….

obtain written consent for the collection, use, disclosure and retention of patient information.

Suggestions for how to do it…

Create and provide a consent form which contains a patient agreement to allow the dental office to collect, use, store and disclose the patient's personal information. Obtain written consent from each new patient and from existing patients when they present for treatment at their next visit. Once you have obtained consent you need not gain consent at each subsequent patient visit. Never obtain consent by deceptive means. Ensure that employees collecting personal information are able to answer questions about why information is collected and why it is needed.

3) Information Collected

Collection of personal information must be limited to what is reasonably necessary for the delivery of dental care and its administrative processes and should not be collected indiscriminately. Collecting less information reduces the risk of unauthorized uses and disclosures.

What you must do is….

Determine the kind of personal information you require in your delivery of oral health care.

Suggestions for how to do it…

Review you current patient information/patient history form. Identify the general information needed for all patients and collect that information. Consider each patient's oral health care requirements and the practice's administration needs and only collect additional information reflecting those needs.

C. SECURITY

1) Access to Personal Information

Offices must limit the access to personal information to those individuals and other organizations who have a need-to-know, and who have not been specifically restricted.

What you must do is….

use or disclose information only for the purpose for which it was collected. Keep information only as long as necessary to satisfy the purposes for which it was collected. Only staff with a "need to know" should have access to a patient's personal information

Suggestions for how to do it…

Safeguard personal patient information, taking into consideration the sensitivity of information, the amount of information, the extent of distribution, the format of information (electronic, paper etc.) and the types of storage in your office. Implement security measures that all staff must abide by. Health and/or financial information will always be considered very sensitive and require a high degree of security.

2) Information Protection

Appropriate safeguards must be in place to protect personal information against loss, theft and unauthorized access.

What you must do is….

develop and implement security policies and procedures to ensure protection.

Suggestions for how to do it…

Protect patient's privacy by not having charts and other private personal information in view and by not discussing a patient's personal information in the presence of others who do not have a need to know. Take particular precautions with fax machines, computer screens and call display monitors so that unauthorized individuals are not able to see the personal information of others. Be cautious of faxing personal information to ensure the personal information will arrive at the intended destination.

Make certain to use physical measures such as locked filing cabinets and alarm systems and restrict access to offices. Computerized offices require technological tools to be used, such as passwords, encryptions and firewalls. Limit access, in particular behind front office counters where personal information may be present, to those who have a need to know or a need to be there. The Privacy Officer should ensure staff are aware of and understand these measures. Employ verbal or written confidentiality agreements with staff. For other regular visitors (e.g. equipment repair people, computer technicians, bookkeepers, cleaners, and students who are job shadowing) who may be required to be in areas where there is personal information, a

confidentiality agreement should be signed. Review and update security measures on a regular basis. **(APPENDIX V)**

3) Destruction

Destroy, erase or render anonymous information that is no longer required for an identified purpose or for a legal requirement.

What you must do is….

Determine information that needs to be disposed of, taking into consideration legal requirements and restrictions.

Suggestions for how to do it…

Dispose of patient information that does not have a specific purpose or no longer fulfills its intended purpose and is not required to be maintained by Statute (i.e. Canada Customs and Revenue, Statute of Limitations). Shred paper and erase electronic files when they are no longer required.

D. DISTRIBUTION OF INFORMATION

1) Responsibility for Distribution

You are responsible for personal information provided to others including but not limited to general practitioners, specialists, other health care providers, benefit providers, accountants, bookkeepers, laboratories, legal counsel, regulatory agencies, employees and so forth.

What you must do is….

Ensure personal information distributed to others reflects the level of consent provided by the individual, and its distribution is to those who have a need to know.

Suggestions for how to do it…

Ensure consent is obtained prior to disclosing information to an outside party, if that consent is not covered by your consent form. Ensure patients are advised in writing, as per their consent form, that their personal information may be distributed to insurance companies, other dentists etc., and explain why. Distribute only information that is relevant to the reason it is being disclosed (i.e. do not send information on marital status or medical conditions to a dental lababoratory). Do not discuss your patient's personal information with any other individual including the patient's family members unless consent has been given to do so. Patients have the right to determine who may or may not receive their personal information.

What You Must Do…. & Suggestions For How To Do It….

As An Employer

What you must do….

Employees are protected by provincial legislation and therefore the personal information held by their employer (the dentist) does not fall under PIPEDA. However, supplying an employee's personal information for commercial purposes would make that information subject to PIPEDA and a dentist using or supplying employee personal information for commercial purposes would have to comply with the 10 principles of PIPEDA as describe in this document.

Suggestion for how you must do it….

Treat employee personal information as sensitive. Do not provide employee personal information for commercial purposes.

ERRATA

1) Information may be used without individual's knowledge or consent :

- For a life threatening, health or security emergency
- For statistical or scholarly study or research (the Privacy Commission must be notified prior to this use).

2) Information may be disclosed without an individual's knowledge or consent :

- To a lawyer representing the dental practice
- To collect a debt the individual owes to the dental practice
- To comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction to compel the production of personal information such as the Provincial Dental Board.
- In an emergency threatening an individual's life, health, or security (the organization must inform the individual of disclosure).
- 20 years after the individual's death or 100 years after the record was created.
- If required by law.

3) Organizations must refuse an individual access to personal information:

- If it would reveal personal information about another individual unless there is consent or a life threatening situation.
- If the dental office has disclosed information to a government institution for

law enforcement or national security reasons. Upon request, the government institution may instruct the dentist to refuse patient access or not to reveal that the information has been released. The dentist must refuse the patient's request and notify the Privacy Commissioner it has done so. The dentist cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

CHECKLIST
PREPARING YOUR OFFICE FOR PIPEDA

Are We Ready ?	Comments and Notes
Who is the designated privacy officer?	
Have we provided staff with PIPEDA briefing/training?	
Have we considered all 10 PIPEDA principles and how they apply in our office? Accountability; identifying purpose; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access and challenging compliance	
What information is collected from our patients? What is collected, Why? How is it collected? Who has access? Is it kept secure? How and when is it disposed of? Is there a complaint process in place?	
Is there a Privacy Statement in Place? Does it include a consent form? Has each and every patient given consent as they arrive for treatment?	
Is our Privacy Policy accessible Where is it posted – public areas, websites, patient information forms.	
Is there a Confidentiality Agreement with a privacy clause for others who access the dental office? What outside parties have access to charts and personal information?	

TIPS

- Patient charts should not be left unattended or in view of personal who have no reason to know chart content.
- Position computer screens and call display monitors so that they can only be viewed by persons who need to know.
- Discuss patient personal information (i.e. treatment plans) in operatories not reception areas.
- Avoid the use/collection of Social Insurance Numbers as identifiers.
- In multiple dentist practices, only the treating dentist and his/her staff should have access to a patient's personal information (i.e. records, charts, appointment books/software).
- Members with dental practice websites should discuss security issues (i.e. "cookies") with their website developer
- Electronic patient files should be password protected.
- When replacing file storage systems purchase locking cabinets
- Private offices should be secured when unattended.
- Make it a habit to enquire if a patient's personal information is in need of updating.
- Avoid verbal consent for disclosure of personal patient information. Obtain written consent whenever possible and practical.

APPENDIX I

PIPEDA – 10 Principles of Privacy Protection

The obligations set out in PIPEDA represent the 10 principles of privacy protection, and are presented here, as edited by NSDA staff, for member information.

Principle 1 Accountability Organizations, including dental offices, are responsible for personal information under their control and shall designate an individual or individuals accountable for compliance with the ten PIPEDA principles.

Principle 2 Identifying Purposes An organization must identify for which purposes personal information is collected, at or before the time the information is collected.

Principle 3 Consent An individual's knowledge and consent are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 Limiting Collection The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization and shall be collected by fair and lawful means.

Principle 5 Limiting Use, Disclosure, and Retention An organization shall not use, disclose or retain personal information for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall only be retained for long as necessary to fulfill those purposes.

Principle 6 Accuracy Personal information shall be as complete, accurate, and as up to date as necessary for the purposes for which it was collected.

Principle 7 Safeguards Personal information shall be protected by security safeguards. The safeguards must be appropriate to the sensitivity of the information collected.

Principle 8 Openness An organization shall make specific information about its policies and practices, relating to the management of personal information, readily available to an individual.

Principle 9 Individual Access An individual, upon request, shall be informed of the existence, use, and disclosure of his/or her personal information. The individual shall be given access to that information and shall be able to challenge the accuracy and completeness of the information. The individual may request to have information amended as appropriate.

Principle 10 Challenging Compliance An individual shall be able to challenge compliance concerning the above principles to the designated individual or individuals responsible and accountable for the organization's compliance.

APPENDIX II

PRIVACY POLICY

This dental practice's Privacy Policy reflects the obligations set out in PIPEDA and includes the 10 principles of privacy protection.

Accountability

The **practice/dental office/clinic/practitioner** is responsible for personal information under our control and shall designate an individual or individuals accountable for compliance with the ten PIPEDA principles.

Identifying Purposes

The **practice/dental office/clinic/practitioner** will identify for which purposes personal information is collected, at or before the time the information is collected.

Consent

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

Limiting Collection

Collection of personal information shall be limited to that which is necessary for the purposes identified by the **practice/dental office/clinic/practitioner** and shall be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention

The **practice/dental office/clinic/practitioner** will not use, disclose or retain personal information for purposes other than those for which it is collected, except with the consent of the patient or as required by law. Personal information shall only be retained for long as necessary to fulfill those purposes.

Accuracy

Personal information shall be as complete, accurate, and as up to date as necessary for the purposes for which it was collected.

Safeguards

Personal information shall be protected by security safeguards. The safeguards will be appropriate to the sensitivity of the information collected.

Openness

The **practice/dental office/clinic/practitioner** will make specific information about its policies and practices, relating to the management of personal information, readily available to a patient.

Individual Access

A patient, upon request, shall be informed of the existence, use, and disclosure of his/or her personal information. The patient shall be given access to that information and shall be able to challenge the accuracy and completeness of the information. The patient may request to have information amended as appropriate.

Challenging Compliance

A patient shall be able to challenge compliance concerning the above principles to the designated individual or individuals responsible and accountable for **practice/dental office/clinic/practitioner** compliance.

APPENDIX III

COMPLAINT SYSTEM CONSIDERATIONS

To comply with PIPEDA, the dental office must have a complaint handling system. Each dental office has unique and distinct characteristics. Accordingly, each office should establish a complaint handling system reflecting the particular characteristics of that office.

To assist the dental office to create their complaint handling system the following considerations are suggested for inclusion:

- ✓ The individual responsible for receiving complaints is _____.
- ✓ Complaints will be investigated by_____.
- ✓ The complaint will be investigated within____ days of its receipt.
- ✓ The determination as to the validity of the complaint will be decided by_____.
- ✓ This decision is to be reported to_____.
- ✓ Recommended corrective action where necessary will be determined by_____.
- ✓ The corrective action will be carried out by_____.
- ✓ The corrective action was communicated to the complainant by_____.
- ✓ The corrective action was communicated to the complainant on_____.
- ✓ The corrective action is recorded in the following locations_____.
- ✓ Corrective action was initiated on_____.

Once the Complaint Handling System has been finalized it should be documented in writing and shared with all employees for understanding.

APPENDIX IV

PRIVACY STATEMENT FOR PATIENTS & CONSENT FORM

Privacy of our patient's personal information is important to us. We are committed to collecting, using, and disclosing personal information responsibly.

PERSONAL INFORMATION

Personal information for our purposes is; that information necessary for the provision of professional oral health care services provided to you, and information necessary to administer this dental practice. Personal information includes all that information provided by you to us on our patient information/health/medical history form at the first visit and any subsequent visits. Personal information may also include any information provided by you to us during the normal course of communication between patient and dental office staff. We will use and disclose only information provided to us by you or another person acting on your behalf.

INFORMATION PROTECTION

We are committed to protecting your personal information. We have established and implemented a variety of security measures to properly manage and safeguard your personal information from loss, theft and unauthorized access. Access to your personal information shall be on a "need to know" basis.

INFORMATION DISCLOSURE

Your personal information shall be disclosed to only those who have a need to know and the specific information disclosed shall be restricted to only that information relevant to the recipients need to know. Those who have a need to know include other dentists and health care providers (i.e. dental specialists, personal physicians). Further, the personal information disclosed to dental benefit providers is limited to only that personal information required by the

provider. You may at any time designate any restrictions as to whom we may disclose your personal information or restrict the content of a disclosure.

INFORMATION RETENTION AND DESTRUCTION

We will retain you personal information for the period necessary to continue providing oral health services to you, and for its related administration. We will destroy information in a secure manner when the information is no longer necessary for the provision of oral health services and is not required to be retained for compliance with provincial or federal regulations or statutes.

YOUR ACCESS TO YOUR RECORDS

We are committed to providing you with open access to your personal information held by us. You may at any time ask us to see your records held by us and to request amendments to that information. We will provide access to you within a reasonable timeframe recognizing your desire for the information and our need to carry on our practice with limited interruption.

COMPLAINT PROCESS

Should you wish to make a formal complaint regarding our privacy practices, please do so in writing to our privacy officer, _____.

CONTACT

Should you have any questions comments or concerns, please bring them to my attention or the attention of our privacy officer_____. We will be pleased to assist you.

SIGNATURE_____ DATE_____
DDS

CONSENT

ACKNOWLEDGEMENT

Having read and understood the PRIVACY STATEMENT FOR PATIENTS, I consent to the collection, use and disclosure of my personal information as presented in the STATEMENT, subject to the restrictions identified below.

No Restrictions_____

RESTRICTED ACCESS

My personal information shall not be provided to the following individuals or organizations:

_____
_____
_____
_____
_____
_____

RESTRICTED INFORMATION

Personal information disclosed from the personal information collected, shall not include:

_____
_____
_____
_____

SIGNATURE_____ **DATE**_____

APPENDIX V

CONFIDENTIALITY AGREEMENT

To be signed by all who are not employees of the dental office but who may, either intentionally or unintentionally, have access to personal patient information. This list includes but is not exclusive to: other dentists and their employees, landlords, maintenance workers, cleaners, information technicians, bookkeepers, accountants, file storage companies, building security, legal counsel, temporary staff, students on work term or job shadow.

I understand that in the course of my activities with _____(Dental Practice), I may encounter personal patient information. I agree to maintain confidentiality of this information to ensure its protection. I will not collect, use, disclose, or retain any of the personal patient information to which I have access.

Dated_____ Signed_____