PRIVACY GUIDE FOR ALBERTA DENTISTS

This Guide is not intended to provide legal advice.

The Guide provides general information with respect to the impact of privacy legislation on dentists. Privacy legislation is open to interpretation and there is some uncertainty as to how it will be interpreted by the provincial and federal Privacy Commissioners with respect to health professionals such as dentists.

This Guide is based on information that is available as of December 2003.

Dentists should be aware that the recommendations in this Guide could be affected by subsequent changes in privacy legislation and by Privacy Commissioner rulings.

Dentists should consult their own legal advisors to obtain advice with respect to any specific issues concerning compliance with the legislation.

Introduction

This package is intended as a guide for dentists in Alberta regarding compliance with privacy legislation that recently came into effect for dentists. The Alberta government recently passed private sector privacy legislation, the *Personal Information Protection Act*. (" PIPA") which will be effective January 1, 2004 and which applies to dentists in Alberta. The federal government previously passed privacy legislation, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). This federal legislation applies to commercial activities in the private sector across Canada effective January 1, 2004 unless a province passes privacy legislation that the federal cabinet considers "substantially similar." At the time this Guide was prepared, the federal cabinet had not yet officially declared whether PIPA would be declared substantially similar. PIPEDA will also apply to situations in which personal information is transferred across provincial boundaries for consideration. For example, if a dentist submitted personal information about a patient to an insurance company in another province, then it is likely that PIPEDA would apply to the information. PIPEDA may also apply to personal information related to dental services under a federal government program.

So, both PIPA and PIPEDA may apply to personal information in dental offices in Alberta depending on the particular circumstances. While this mix of applicable legislation presents a challenge, the ADA&C has attempted to simplify matters for dentists by developing this Guide which is designed to help dentists in Alberta meet the requirements of both PIPA and PIPEDA.

Why is Privacy Important?

PIPA is important legislation to Albertans. According to Alberta Government Services, "a public opinion poll conducted in December 2002 showed overwhelming support for privacy legislation. Over 96% of Albertans feel they should be informed about the purpose of information collected about them, they should have access to this information and the information should be used for the purpose for which it was collected and not used by a third party. Over 95%"of Albertans feel that all companies in Alberta should adhere to the same minimal standard of protecting personal information and that there should be laws in place to ensure compliance." Privacy is clearly a public "trust" issue for Albertans.

Privacy has been defined by the Privacy Commissioner of Canada as, "the right to control access to one's person and information about oneself." Recognizing its importance to the public, business and public leaders in Alberta see privacy not just as a technical matter, but as a "common sense" issue that revolves around reasonableness in the collection, use and disclosure of personal information relative to the purpose and circumstances at hand.

The Alberta privacy legislation is about finding that 'reasonable balance" between the rights of an individual to have their personal information protected, and the need of organizations to collect, use, retain or disclose personal information for purposes that are reasonable. A copy of PIPA may be found at www.psp.gov.ab.ca and a copy of PIPEDA can be found at www.privcom.gc.ca.

Public Policy Themes in Privacy Legislation

The five important themes of privacy legislation are:

- **accountability** for the protection of personal information
- **reasonableness** in the collection, use and disclosure of personal information
- **limiting** collection, use, disclosure and retention of information to stated purpose
- **obtaining express consent** where necessary, and
- **openness and transparency** about access and challenges to compliance.

These themes reflect the public policy intent of PIPA and PIPEDA, and support the fair information practices set out in the Canadian Standards Association for the Protection of Personal Information. These practices, listed in Appendix 1, form the principles behind both pieces of privacy legislation. Together, they give rise to a number of steps dentists should take to get ready for compliance with PIPA and PIPEDA.

In addition to providing you with general guidance, we also include in this Guide some tools to assist you in meeting the requirements of the legislation. The Guide includes:

- a sample privacy policy for a dentist's office or facility
- a sample dental office personal information consent form, and
- a sample privacy agreement for third party contractors or service providers.

Step 1:
Become Familiar with the Legislation

This Guide will provide a good summary of the legislation. For further information you should review two brief yet very helpful guides to the provincial legislation which are attached to assist you with this starting point. The Personal Information Protection Act on a Page (Appendix 2) and Getting Ready for the Personal Information Protection Act (Appendix 3) are both also available online at www.psp.gov.ab.ca. You may also wish to review *"A Guide for Businesses and Organizations on the Personal Information Protection Act*" available at www.psp.gov.ab.ca. You can also seek advice and assistance from the Alberta Government Privacy Help Desk by phoning them at 780-644-7472 (toll free dial 310-0000 first) or e-mailing them at privacyhelpdesk@gov.ab.ca. If you wish to review a guide to the federal PIPEDA please see "*Guide for Businesses and Organizations to Canada's Personal Information Protection and Electronic Documents Act*" which is available at www.privcom.gc.ca.

STEP 2:
Identify the Personal Information in Your Practice

Your next step is to identify the personal information you currently collect, use, retain and disclose about anyone including patients and employees. It helps to categorize this by groups, and also to identify any particularly sensitive information.

What is personal information? Personal information is information about an identifiable individual but does not include business contact information. Personal information that might be collected by a dental office about patients includes:

- Names
- Age
- Gender
- Marital status
- Insurance benefit coverage
- Employer name
- Home address, home phone numbers, and other contact information.
- Financial information.
- Family information.
- Medical history.
- Dental treatment information.

Remember that this list is not exhaustive. Personal information is any information about an identifiable individual. It is important that you identify the personal information that you collect, use, or disclose in your particular dental office. Be very thorough here, as this step becomes critical when designing your personal information protection regime in the office going forward. Identify types of information from all sources and through all media (paper, telephone, online).

Identify the personal information for which you currently do and do not have express or written consent. Also note any third party consultants or contractors that may have access to personal information as a result of their work with you.

During this early overview, you may also notice personal information that is not really tied to or necessary for your primary or related service purposes. If you learn that you are collecting personal information that is not really required for your practice, then you should cease collecting this information.

Step 3:
Appoint a Privacy Officer

The **accountability theme** dominates here. The Privacy Officer assumes accountability for overall compliance with PIPA and PIPEDA at your practice. The Privacy Officer must have the authority to exercise this accountability. If the Privacy Officer is not yourself, you must delegate to your designate the authority to oversee policy and implementation and to intervene for issues resolution. The name of the Privacy Officer in your practice must be expressly declared and made known to patients and employees. It is not assumed that you would hire someone just for this role.

Your Privacy Officer carries out the following roles and activities:

- Oversees development of your privacy policy and procedures
- Ensures your privacy policy is made public to patients and employees
- Ensures adequate training of staff with respect to privacy policy and procedures
- Ensures adequate forms are used obtaining informed consent for information collection, retention and disclosure
- Ensures environmental safeguards are in place for personal information protection
- Responds to questions and concerns regarding personal information protection
- Liaises with external groups and ensures third parties protect the privacy of personal information.
- Processes complaints regarding personal information practices in your office.

Your Privacy Officer should have the following attributes:

- Respect for privacy and the importance of personal information protection
- An understanding of the legislation
- Clear communication and good listening skills
- A comfort level with resolving issues and managing conflict
- Experience in dealing with the practical application of legislation
- Respected by the staff in a change management role.

Step 4:
Establish and Publicly Display Your Privacy Policy

The **accountability and transparency themes** dominate here. Policies are not just rules. Policies are principle-based and about commitment. Make sure your policy communicates commitment to implementation. Patients and employees will need to know from your policy statement that:

- you value their privacy
- you are committed to protecting their personal information as the principal means to protecting their privacy
- you will limit the collection, use, retention, and disclosure of their personal information to that which is reasonable given your disclosed purposes
- you will only disclose to third parties with their express consent or as otherwise permitted by law
- they can opt out of information collection that includes implied consent for disclosure
- you will ensure the physical safequards are in place to secure their personal information
- they can access their personal information, and seek consideration for changes if they have concerns about accuracy or currency of the information
- they have access to the privacy officer to ask questions or express concern regarding your privacy policy and procedures or their personal information
- they can challenge your compliance with the legislation

Ensure you have the processes and tools in place to implement the commitments expressed in your policy.

Be sure to monitor your policy implementation from time to time and especially in the first year, and document the monitoring and any changes made as a result.

Your policy should fit the circumstances of your own dental office. However, a sample policy, “Protecting Your Privacy While Promoting Your Oral Health” containing the above elements is attached as Appendix 4. You will note that the name and contact information for your Privacy Officer needs to be inserted into the policy. Your policy should be on display and available in your office. We also recommend that you provide all new patients a copy of your privacy policy. You should also provide current patients a copy of your privacy policy the next time they visit your office.

Step 5:
Limit your Personal Information Collection

The **limiting and reasonableness themes** dominate here. Ensure that you collect only the information you need to service your patients and facilitate the other supportive processes necessary to complete transactions, such as direct billing or third party collection.

Dental offices generally collect three kinds of personal information about patients:

- contact information
- health information, and
- financial information.

Consider the information you currently collect and ensure that you can demonstrate it is reasonable to collect it. If you conclude that you are collecting personal information that you do not need for the purposes of providing dental services, then stop collecting this information.

Consider the sensitivity of the personal information you collect. Be cautious about comments made about subjective areas such as patient opinions or attitudes.

Ensure that the purpose of collecting personal information is expressly stated on any forms you use for collecting the information. It is a good idea to do so right on the form you use to obtain the consent for the collection, use, retention and disclosure of the information.

Collect personal information about an individual directly from the individual unless they consent to you receiving the information from some other source.

Step 6:
Provide for Express Informed Consent

The **accountability and express consent themes** dominate here. Informed consent also has a significant **limiting** effect on personal information.

The concept of informed consent is not new to dentists. However, the practice of separate consent for information collection use and disclosure may be.

The general rule of the legislation is that consent is required for the collection, use, and disclosure of personal information. While the legislation has many exceptions to this general rule, dentists should wherever possible obtain written informed consent for personal information collection, use, retention and disclosure.

A review of all of the exceptions in the legislation in which personal information may be collected, used, retained or disclosed without consent is beyond the scope of this Guide.

For advice with respect to specific situations contact your legal advisor or review the documents referenced under Step 1: Becoming familiar with the legislation.

Written informed consent requires a privacy statement telling the patient the purpose(s) of the information collection to begin with, including how it will be used and disclosed. We recommend that you have each new patient sign a Dental Office Personal Information Consent Form. We also recommend that you have current patients sign a Dental Office Personal Information Consent Form the first time they visit your office after January 1, 2004. You should keep a copy of the signed Consent Form on the patient's file and also provide a copy to the patient.

The specific content of the Dental Office Personal Information Consent Form will depend on the personal information that you collect, use and disclose in your dental office. .Appendix 5 provides an example of a consent form that could be used provided that it fits the particular circumstances of your office. It is very important that the Consent Form that you use meet the needs of your own office.

Please note that the consent form in Appendix 5 only deals with Personal Information and does not address consent for dental treatment. As a separate matter you must ensure that you have obtained informed consent for dental treatment.

With respect to mail outs regarding follow-up, special promotions or educational materials, you should give patients the opportunity to "opt out" of being on the circulation list for those purposes.

Step 7:
Provide Safeguards for Personal Information Protection

Personal information is by nature sensitive information. Health information and financial information are considered very sensitive by most. Once again, **the limiting and accountability themes** dominate.

Appropriate safequards must be in place to prevent unintended access to or loss of personal information.

Ensure that records are kept only in places where authorized individuals have access.

If cupboards containing personal information are not locked, make sure they are not left unattended and available to the public.

Passwords, encryptions and firewalls are important security measures for computerized files.

Ensure that monitor screens are not open to unauthorized view.

Curtail telephone discussions that can be overheard by others to avoid unauthorized disclosure of personal information.

When destroying personal information, make sure paper sources are shredded, electronic sources are deleted, and hardware products are destroyed beyond repair.

In the course of carrying out their day-to-day activities, dental offices may disclose personal information to third party contractors or service providers. Examples of such third parties include: billing service providers, software providers, information technology specialists or accountants.

The dental office has an obligation to ensure that any personal information in its custody or under its control is handled in accordance with the requirements of all applicable privacy legislation. This includes personal information collected by the dental office which is disclosed to third party contractors or service providers.

To ensure that the requisite privacy protections are observed by third party contractors or service providers, dental offices should consider entering into privacy agreements with any third parties to whom personal information is disclosed.

At Appendix 6 you will find some sample privacy clauses which may form the basis of a stand-alone privacy agreement or which may be modified for insertion into contractual agreements with third parties. It is important to note that these are sample clauses only and your legal advisor should be consulted for advice specific to your particular needs.

Step 8:
Train Your Staff in the Policy Intent and Requirements of the Relevant Legislation.

The **accountability and transparency** themes operate here.

Train your staff in communication patterns that limit information collection, provide for active listening, and manage conflict in a responsive manner.

Provide values clarification and attitude change support regarding individuals' right to access their personal information and challenge the office's compliance with privacy legislation requirements.

Provide staff the tools and forms to effect privacy compliance.

Reward staff performance that supports privacy compliance and sanction behaviour that does not.

Hold all staff accountable for being transparent about the office's privacy policy and procedures, access to the Policy Officer to ask questions, express concerns, or handle complaints about personal information protection.

Step 9:
Ensure Personal information in Files is Complete, Accurate and Up to Date.

The **accountability, reasonableness and access** themes dominate here.

Ask patients each time if any of their personal information needs updating.

When checking medical status, ensure you have up to date information on record.

Invite patients to comment on completeness, accuracy and currency of the personal information in their file.

Provide open access of individual's to Privacy Officer to ask questions or express concerns about their personal information.

Step 10:
Identify the Processes through which Individuals Can See Their Personal information or Request Consideration of Changes in Their Personal information

Openness and transparency are paramount here.

You do not have to make unwarranted changes to personal information in a file

Document the request for change to a file. Document the change, if made.

Professional opinions do not have to be automatically changed just because of a request.

If you do not consider that a change requested by a patient is warranted, seek professional advice at that time to ensure that you follow appropriate processes in the legislation. If a patient expresses concern or dissatisfaction regarding a failed request for change, be open about the written complaint route internally to the Privacy Officer, or externally to the Office of the Information and Privacy Commissioner.

In responding to requests by an individual to see their personal information, you must ensure that you do not inadvertently disclose personal information about another person.

Step 11:
Institute and Describe Openly a Process for Expressing Concerns or Complaints Verbally, or Submitting Written Complaints Regarding the Collection, Use, Retention and Disclosure of Personal Information.

Accountability and transparency dominate here.

Identify the Privacy Officer as the complaints investigator.

Ensure confidentiality of the complaint process.

Ensure a respectable and ”listening approach” to the airing or voicing of a complaint.

Give the complaint a thorough and fair hearing.

Match the level of formality in complaint handling with the nature of the complaint.

Express an interest to learn from complaints.

As long as the privacy principles are not breached and the legislative requirements are not sacrificed, seek a collaborative solution wherever possible.

Document the complaint resolution.

Document any impact on future policy or procedures.

Step 12:
Review and Update your Privacy Policy and Other Privacy Forms on An Ongoing Basis

All five themes should be monitored here.

Have a written policy and procedure review described and documented.

Implement the review.

Involve the staff in the review findings.

Invite stakeholder input into policy and procedural changes.

Make the decided changes and document the resultant impact.

Remember that this Guide is based on legislation and its interpretation as of December 2003. Check for any subsequent changes in the legislation or its interpretation.

Once you are "up and running", when a privacy problem occurs, consider the following checklist as a first order assessment.

- Is the Privacy Officer named, known, and "in the job"?
- Is the privacy policy stated and made public?
- Do the staff value privacy, understand the legislation and show commitment to the policy implementation?
- Do the collection, use, retention and disclosure of personal information in your office meet the reasonableness test?
- Are appropriate and useful consent forms being used?
- Is access to personal information by third party contractors appropriately controlled?
- Are secure privacy protection safeguards in place in the environment?
- Is the personal information we collect updated regularly?
- Do patients and staff understand the process to request access or changes to personal information in their records?
- Is a privacy complaints management process in place?

Personal Employee Information

While the steps set out above focus on personal information from patients, PIPA also applies to "personal employee information. PIPA defines "personal employee information" as meaning:

…in respect of an individual who is an employee or a potential employee, personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing, or terminating

(i) an employment relationship, or
(ii) a volunteer work relationship

between the organization and the individual but does not include personal information about the individual that is unrelated to that relationship.

The general rule with respect to personal employee information, is that this type of information may be collected, used , or disclosed by an organization without the consent of an individual if the individual is an employee of the organization and:

1. the collection, use, or disclosure is reasonable for the purpose for which it is collected, used, or disclosed, and
2. the personal employee information includes only personal information that is related to the employment or volunteer work relationship of that individual, and
3. with respect to employees of an organization, the organization has, before collecting, using, or disclosing the information, provided the employee with reasonable notification the information is going to be collected, used, and disclosed and of the purposes for which the information is going to be collected, used or disclosed.

There are other specific rules with respect to personal employee information which are beyond the scope of this Guide. For information with respect to specific situations either contact your legal advisor or review the information referred to in Step 1.

Health Information Act

Dentists should be aware that health information arising from publicly funded dental procedures may be subject to the privacy rules in the Health Information Act. An analysis of the Health Information Act is beyond the scope of this Guide. For further information on the Health Information Act please see the guides at www.oipc.ab.ca/publications/hia.cfm or available from the Office of the Information and Privacy Commissioner of Alberta.

APPENDIX 1

Privacy Principles in Summary

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Both PIPA and PIPEDA are based on these.

1. **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.

2. **Identifying Purposes**

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

3. **Consent**

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

4. **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.

5. **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.

6. **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.

7. **Safeguards**

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

8. **Openness**

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

9. **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.

10. **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.

APPENDIX 2

The Personal Information Protection Act
On a Page

- Obtain consent for collecting, using and disclosing personal information, except when inappropriate (for example, in an emergency or when consent would compromise the availability or accuracy of the information). Obtain the consent in a form appropriate to the kind of information concerned. If an individual modifies or withdraws his or her consent, respect the changes.
- Collect personal information only for reasonable purposes and only as much as is reasonable for those purposes. Except when inappropriate, collect personal information directly from the individual concerned and inform the individual of how you will use and disclose the information.
- Use and disclose personal information only for the purposes for which it was collected, unless the individual consents or the Act permits the use or disclosure without consent.
- On request, provide an individual with information about the existence, use and disclosure of the individual's personal information and provide access to that information, if reasonable. On request, correct information that is inaccurate.
- Ensure that any personal information is as accurate as necessary for the collection purposes; ensure that personal information is secure; and keep the information only as long as reasonable for business and legal reasons.
- Designate an individual to make sure you comply with the Act and make information about the organization's management of personal information available on request.

Note

The Alberta government introduced Bill 44, the *Personal Information Protection Act*, in May 2003. The Act is expected to pass during the fall session of the legislature. This document was prepared to help organizations prepare for private sector privacy legislation as it is assumed that Bill 44 will come into effect on January 1, 2004. Once the Bill is passed, the document will be revised to reflect the content. This document is not a substitute for legal advice. Please direct your comments or questions to:

Privacy Help Desk
Information Management, Access and Privacy, Alberta Government Services
E-mail: privacyhelpdesk@gov.ab.ca
Phone: 780-644-PIPA (7472) Toll free dial 310-0000 first
Web site: www.psp.gov.ab.ca

APPENDIX 3

Getting ready for the *Personal Information Protection Act*

Alberta's *Personal Information Protection Act* (PIPA) sets out the rules for handling the personal information of an organization's customers and employees. The Act is expected to be in effect in Alberta on January 1, 2004.

In the Act, *organizations* include corporations, unincorporated associations, trade unions, partnerships, and individuals running their own businesses. There are special rules that apply to non-profit organizations and self-governing professional organizations. PIPA does not regulate the collecting, using, or disclosing of personal information for domestic, artistic, literary, or journalistic purposes.

To prepare for the new Act on private sector privacy, follow these steps:

1. Put someone in charge

Put someone in charge with enough authority and resources to do the job. This employee would be the contact for the public and employees when privacy issues arise.

You may want to assign other staff to help prepare the organization for the Act. A team is likely more effective since areas such as information technology, records management, legal services, human resources and operations will be affected.

2. Become familiar with the Act

The staff working on privacy matters will need to be familiar with the Act. Resources are available on the private sector privacy Web site at www.psp.gov.ab.ca.

Note

The Alberta government introduced Bill 44, the *Personal Information Protection Act*, in May 2003. The Act is expected to pass during the fall session of the legislature. This document was prepared to help organizations prepare for private sector privacy legislation as it is assumed that Bill 44 will come into effect on January 1, 2004. Once the Bill is passed, the document will be revised to reflect the content. This document is not a substitute for legal advice. Please direct your comments or questions to:

Privacy Help Desk
Information Management, Access and Privacy, Alberta Government Services
E-mail: privacyhelpdesk@gov.ab.ca
Phone: 780-644-PIPA (7472) Toll free dial 310-0000 first
Web site: www.psp.gov.ab.ca

3. Review how your organization handles personal information

Look at how you handle personal information in the organization, from when it is collected to when it is destroyed. Ask these questions:

- What personal information do we collect? Is any of it particularly sensitive information?
- Why do we collect it?
- Are individuals likely to be aware that we collect this information? Do they know why it is collected?
- How do we collect it? Does it come from the individual at the cash register, a form, a survey, loyalty program, or on-line transaction?
- What do we use it for? Where do we use it?
- Who is it disclosed to? Does the organization contract out any functions or activities involving personal information? Does it go to any business partners?
- Where do we keep it? Is it stored in one place or in several places?
- How is it secured?
- Who has access to or uses it? Who needs to have access?
- When it is disposed of? How is it disposed of?

4. Put your practices to the test

Consider whether your organization's information handling processes measure up against the Act. Develop a plan to overcome any deficiencies, starting with the most problematic areas. These include your handling of the most sensitive personal information collected or of the most vulnerable to improper use or disclosure.

5. Develop privacy policies and practices

Consult the staff who handle personal information when developing privacy policies and practices to comply with the Act. Information on these policies will need to be available to the public on request.

Consider policies and practices in the following areas:

- Protecting employee and customer personal information, and ensuring its accuracy, storage, and disposal.
- Ways to obtain and record consents, and handling withdrawals of consent.
- Ways to record uses and disclosures of personal information.
- Ways to keep information as accurate as is needed for decision-making.

- Adequate security measures to protect personal information, including information on-site, with staff traveling for business, or in the custody of contractors.
- Developing keep-and-destroy procedures so you can destroy personal information no longer required in a secure manner.

6. Train staff

Ensure you adequately train staff for their responsibilities. Training may cover such areas as:

- The principles of privacy protection.
- The organization's policies and practices.
- How the Act affects their specific job and the personal information they handle or are responsible for.
- How to handle or re-direct questions received under the Act.

7. Develop an access and complaints handling process

Employees or the public may send PIPA-related questions and complaints to you or to the Office of the Information and Privacy Commissioner. Set up sound, specific practices to handle these inquiries, as well as requests for access to, or for correcting, personal information.

8. Review and revise forms, and create notice statements

In most situations when an organization collects personal information, the organization needs to give notice of the purposes for the collection. Add these notices to forms and web sites as necessary. Make sure the paper and on-line versions of the forms and notices are kept current and say the same thing.

9. Review and revise contracts

Your responsibility to protect personal information continues when the organization provides personal information to a contractor for processing. Contracts should contain clauses to clarify that the organization is legally responsible for that personal information. They should set out expectations regarding the collecting, using, and disclosing of personal information on the organization's behalf.

Your organization can develop standard wording for agreements with contractors when personal information is disclosed for processing.

10. Consider employees' personal information

Personal employee information is also covered by the Act. An organization will need to decide when it requires an employee's consent to collect, use, or disclose personal information. Build these processes into your normal business practices.

APPENDIX 4

Our Privacy Policy

At the (Dr. xxxx and/or Clinic name), we protect the privacy of our patients by:

- collecting only the personal information that is reasonable for our purposes in serving you
- obtaining your consent for how we disclose or share your personal information
- having safeguards in place to protect your personal information at times of collection, use, storage, disclosure, and exchange with others
- sharing your personal information only for the purposes and with those agreed to in a signed consent form, or otherwise permitted by law
- ensuring that any contractors we hire who may have access to any of your personal information also take steps to protect the privacy of your personal information
- training our staff and adapting our physical, telephone and electronic environment to protect your personal information
- processing the necessary forms and documentation to protect your personal information
- ensuring the personal information we keep on you is complete, accurate, and up to date
- letting you see and request corrections to the personal information we have on your record
- making our Privacy Officer available to answer your questions and concerns about our Privacy Policy and to deal with written complaints regarding personal information, and
- periodically reviewing implementation of our Privacy Policy to ensure fulfillment of our commitment to your privacy protection while we promote and protect your oral health!

XYZ Dental Clinic

If you have a concern about your personal information that is not being resolved and wish to file a complaint, please do so in writing to our Privacy Officer.

Our Privacy Officer is xxxxxxxxx, who can be reached in the following ways:

Telephone
Email
Postal address

For more information about the Alberta Personal Information Protection Act (PIPA), or the federal Personal Information Protection and Electronic Documents Act (PIPEDA) , you may wish to visit the website of the Office of the Alberta Information and Privacy Commissioner at www.privcom.gc.ca/legislation, or the Office of the Privacy Commissioner of Canada at www.privcom.gc.ca.

XYZ Dental Clinic

Protecting Your Privacy While Promoting Your Oral Health

Our Personal Information Procedures

We have appointed a Privacy Officer, xxxxxxx as our principal advisor and issues manager regarding personal information protection. On your behalf, our staff are trained in personal information protection, we review our information collection procedures and consent forms on an ongoing basis, and we ensure that any contractors we hire who might have access to your personal information also take steps to protect the privacy of your personal information.

At the Dr. xxxxx , we have a privacy policy in place for patients and employees.

The Personal Information Protection Procedures below tell you how we fulfill the commitment to patients in our Privacy Policy at the Dr. xxxxxxx Dental Health Clinic.

The Personal Information We Collect and Share

We collect contact information, medical information and financial information about our patients. The reasons we collect this information are outlined on the Consent Form you sign at time of collection. The information is used and disclosed only for those purposes.

Contact Information is disclosed to third party health benefit providers and insurance companies with the consent of the patient, where the patient has submitted a claim for reimbursement or payment of all or part of the cost of dental treatment or has requested the dentist to submit a claim on the patient's behalf.

Patients' Medical Information is disclosed to third party health benefit providers and insurance companies, with the consent of the patient, where the patient has submitted a claim for reimbursement. Medical information is disclosed, with the consent of the patient, to other dentists and dental specialists, or to other health care professionals such as physicians.

Financial information is collected for payment processing purposes. It is not shared with third parties without your consent, unless permitted by law for outstanding bill collection purposes.

Protection of Your Personal Information in Our Records

Our records containing your personal information are stored in a secure place.

Our electronic records are stored on hardware that is secure. Passwords are used on all of our computers. We take care to protect screen monitors from public viewing in the office.

Paper records are transferred outside our office in sealed envelopes by secure methods and with reputable carriers.

Telephone discussions with patients in the office are carried out with sensitivity to protecting personal information.

Electronic information is transferred in secure files, and anonymized wherever possible.

We do not share your personal information outside our office for any marketing, promotional, publicity, educational or research purposes without your consent.

Our staff is trained to handle your information only through the protective measures outlined in our privacy procedures.

If we hire consultants or contractors who might have access to any of your personal information, we will take steps to ensure that the consultant or contractor takes steps to protect the privacy of your personal information.

Access to Your Personal Information

You can make a request to look at your personal information by asking the staff. They may refer you to our Privacy Officer. We will attempt to help you understand the reasons we have the information that is in your record.

You may request that we consider making changes to your personal information if it is not accurate, incomplete, or not up to date. If you believe there is a mistake in your personal information, you may ask for consideration that it be changed.

If you request a copy of your record, we will provide it in a reasonable time. If we charge you for the cost of copying, we will let you know in advance what the cost will be.

Storage and Destruction of Personal Information

We are required by legislation and regulation to keep records containing personal information for specified periods of time. We keep your records a maximum of 10 years from your last service, even if you move from our office.

We destroy personal information in paper records by shredding it. We destroy electronic personal information by deleting it. When discarding hardware, we make sure the hard drive is destroyed.

Our Privacy Protection Partnership

Privacy is a value. Privacy protection is a partnership. We hope you will support the culture of privacy protection we have built in our office. We have laid out our commitment to you. Here's how you can help.

1. Make sure the personal information you provide us is complete and accurate.
2. If you have questions or concerns about the purposes for collection, use, disclosure, sharing, storage or destruction of your personal information by us, please bring them to our attention.
3. Please complete the required consent forms for our collection, use, storage, disclosure, sharing and destruction of your personal information.
4. If you disclose personal information to another source that may need to share it with us, e.g. your doctor, your employer, or your dental plan carrier, please complete the required consent forms presented by them to affect that authorized information exchange.
5. Please respect the privacy of other patients in our office when you are here.
6. Please respect the privacy of our staff in dealings with our office.
7. If you wish to see or change the personal information on your record other than for updating purposes, please make that request to our Privacy Officer.
8. If you have concerns or a complaint about our privacy policies or procedures, please contact our Privacy Officer to discuss the procedure for communicating those to our office.

APPENDIX 5

Dental Office Personal Information Consent Form

We are committed to protecting the privacy of our patients' personal information and to utilizing all personal information in a responsible and professional manner. This document summarizes some of the personal information that we collect, use and disclose. In addition to the circumstances described in this form, we also collect, use and disclose personal information when permitted or required by law.

We collect information from our patients such as names, home addresses, work addresses, home telephone numbers, work telephone numbers, and e-mail addresses. (collectively referred to as "Contact Information"). Contact Information is collected and used for the following purposes:

- To open and update patient files.
- To invoice patients for dental services, to process credit card payments, or to collect unpaid accounts.
- To process claims for payment or reimbursement from third-party health benefit providers and insurance companies.
- To send reminders to patients concerning the need for further dental examination or treatment.
- To send patients informational material about our dental practice.

Contact Information is disclosed to third party health benefit providers and insurance companies where the patient has submitted a claim for reimbursement or payment of all or part of the cost of dental treatment or has asked us to submit a claim on the patient's behalf.

Financial information may be collected in order to make arrangements for the payment of dental services.

We collect information from our patients about their health history, their family health history, physical condition, and dental treatments. (Collectively referred to as "Medical Information") Patients' Medical Information is collected and used for the purpose of diagnosing dental conditions and providing dental treatment.

Patients' Medical Information is disclosed:

- To third party health benefit providers and insurance companies where the patient has submitted a claim for reimbursement or payment of all or part of the cost of dental treatment or has asked us to submit a claim on the patient's behalf.
- To other dentists and dental specialists, where we are seeking a second opinion and the patient has consented to us obtaining the second opinion.
- To other dentists and dental specialists if the patient, with their consent, has been referred by us to the other dentist or dental specialist for treatment.
- To other dentists and dental specialists where those dentists have asked us, with the consent of the patient, to provide a second opinion.
- To other health care professionals such as physicians if the patient, with their consent, has been referred by us to the other health care professional for either a second opinion or treatment.

If we are ever considering selling all or part of our dental practice, qualified potential purchasers may be granted access as part of the due diligence process to patient information in order to verify information important to the potential sale. If this occurs, we will take steps to ensure that the prospective purchaser safeguards all personal information.

Dentists are regulated by the Alberta Dental Association and College which may inspect our records and interview our staff as part of its regulatory activities in the public interest.

I consent to the collection, use and disclosure of my personal information as set out above.

_____	_____	_____
Date	*Print Name*	*Signature*

APPENDIX 6

Privacy Agreement

BETWEEN:

_____ (the "Dental Office") and _____ (the "Contractor")

1. The Contractor acknowledges that in the course of its activities with the Dental Office, it may receive or encounter personal information. Personal information means information about an identifiable individual which is collected, used or disclosed by the Dental Office but does not include business contact information ("Personal Information").

2. The Contractor agrees that in dealing with any Personal Information it will abide by and adhere to the terms of this Agreement and all applicable privacy legislation.

3. The Contractor agrees that it will use the Personal Information only to the extent that is reasonable for fulfilling the following purposes: [*insert purposes for which the Personal Information was disclosed to the Contractor*].

4. The Contractor agrees that, except as required by law, it will not disclose any Personal Information without the prior written consent of the Dental Office.

5. The Contractor must protect Personal Information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification or disposal.

6. The Contractor agrees to return any Personal Information to the Dental Office:

   (a) when the Personal Information is no longer required for fulfilling the purposes set out in clause 3 above; or

   (b) immediately upon written demand by the Dental Office.

7. If a Contractor receives a request for access to Personal Information from a person other than the Dental Office, the Contractor must promptly advise the person to make the access request to the Dental Office.

DENTAL OFFICE

_____ Per: _____
Date Signature

CONTRACTOR

_____ Per: _____
Date Signature