Guide to Using a Computer System for Keeping Patient Records
# Table of Contents

Preface ................................................................................................................. 1

Introduction ........................................................................................................... 2

1. Record keeping ................................................................................................ 3

2. Use of the computer system ............................................................................. 5

   2.1 Security and confidentiality of information ................................................... 5

   2.1.1 User code and password ........................................................................ 5

   2.1.2 Access to confidential or sensitive data ............................................... 6

   2.1.3 Back-up procedure ............................................................................... 6

   2.1.4 Archiving data ..................................................................................... 6

   2.1.5 Restoring data in case of technical difficulties .................................... 7

   2.1.6 Printing reports and records .................................................................. 7

   2.1.7 Replacing computers or record-keeping software ............................... 7

   2.2 Authentication and ability to retrace information ...................................... 7

       2.2.1 Inalterability of information and attached documents ...................... 8

       2.2.2 Transferring computerized patient records ...................................... 8

Appendix 1 .......................................................................................................... 11

Appendix 2 .......................................................................................................... 13

Appendix 3 .......................................................................................................... 41
A growing number of professionals use computers in their practices, and dentists are no exception. Many have said that they would like to use a computer system for keeping patient records, while others have been doing so for some time already.

The type of system used makes no difference to dentists’ obligations and rights under the applicable acts and regulations, in particular those concerning record keeping.

The Ordre des dentistes du Québec, whose main mission is public protection, has analyzed the use of computer systems for record keeping, to ensure that patients’ rights are respected.

The purpose of this guide is to help dentists choose a computer system that will meet their legal obligations with regard to record keeping and comply with the rules governing professional secrecy.

The guide will be updated periodically to reflect advances in computer technology.

The Order wishes to thank everyone who contributed to producing this guide, and the Stratégica 2000 inc. firm for its help in drawing up the technical specifications. The Order also wishes to thank all the computer service suppliers who took part in this study. Their assistance allowed us to validate the feasibility of the project as it evolved.
Introduction

Before choosing a computer system, you must consider a number of factors:

- the security and confidentiality of the data stored in the system;
- the authentication of the data entered and the ability to retrace its entry, modification and deletion;
- the inalterability of data and attached documents;
- the inalterability of images produced by digital imaging software, digital X-rays and scanned study models;
- the transfer of patient records.

This guide sets criteria that must be met by computer systems used by dentists practising in Quebec. It also includes a reminder of rules concerning patient record keeping.

The technical specifications in Appendix 2 were developed according to ODQ requirements and reflect the provisions of applicable legislation.
1. Record Keeping

The rules governing record keeping are the same regardless of the medium used. Records must be conserved and the confidentiality and security of the information they contain must be continually ensured. Dentists remain responsible for their patients' records at all times.

This section is a review of dentists' main obligations concerning the information contained in patient records, and how that information is to be gathered and recorded.

Dentists must draw up and keep a record for each patient they treat, and ensure the security and confidentiality of the information it contains. They must preserve their records or ensure that they are preserved in a room or cabinet to which the public does not have access, or that can be locked. Each record must be kept for five years from the date of the last entry, whatever it may be, or the last insertion in the file.

The information contained in the record may not be altered. Any correction or change requested by a patient or the dental team with access to the file must always be noted in the file and signed, initialled or otherwise identified by the dentist. The record must remain complete for its entire lifetime.

Dentists must enter or attach the following particulars in every record pertaining to a patient. When a computer system is used, it is very important that the software be able to record the following details, in a structured manner and in chronological order:

1. the date of the consultation;
2. the patient's medical and dental history;
3. the diagnosis;
4. the choice of treatment and prognosis;
5. a list of operations and a description of every form of treatment performed;
6. the material and medication used in the treatment;
7. written prescriptions for medications or treatments;
8. the significant elements of every verbal or written communication with or pertaining to the patient;
9. examination results, diagnostic features and, where applicable, X-ray reports, along with all models;
10. notes pertaining to information given to a patient concerning acceptance of treatment, and notes pertaining to receipt of the patient's consent for the treatment;
11. the name, concentration and quantity of anaesthetics used in the case of a general, regional or local anaesthetic or conscious or total sedation;
12. information and recommendations with respect to the treatment administered to the patient;
13. the date on which the patient was referred to a health professional, the name of the professional, the purpose of the referral and the report issued after the referral consultation;
14. notes, correspondence and other documents relating to services rendered by the dentist, and copies of all documents or certificates issued to the patient;
15. information concerning the professional fees and any sums invoiced to the patient;
16. a note signed by the patient or his representative, where the patient has requested the removal of an item or document, indicating the nature of the item or document and the date on which it was removed.

At each consultation, the dentist must note any changes to the elements listed above.

All information entered in patient records is confidential. Patients may request access to their files and the modification or removal of certain personal information.¹

Although some computer systems are capable of collecting a great deal of information, only the details essential for treating patients are to be collected. Regardless of the type of system used for record keeping, the information must be collected in a space specifically for this purpose, rather than in a public area where others can hear what is said or see the information being entered on the screen.

X-rays or images produced with digital imaging equipment are also placed in the patient’s record; they must be authentic and conserved in their entirety.

---

¹ “Personal information is any information which relates to a natural person and allows that person to be identified.” (Section 2 of the Act respecting the protection of personal information in the private sector).
2. Use of the Computer System

Dentists are responsible for keeping their records. When several dentists practise in the same office and choose a computer system for keeping their records, they must define the operating rules for the system so as to guarantee the security, confidentiality and completeness of the data to be placed in each record. It is important to appoint a system administrator, who may be a dentist or a computer technician. The administrator must ensure that the staff and software comply with the rules defined by the dentists.

As mentioned earlier, when a computer system is used for record keeping, some aspects are particularly important. This section deals with the criteria to be taken into account by dentists and their staff and met by software.

2.1 Security and confidentiality of information

2.1.1 User code and password

A user code and password are required for every person with access to records. It is up to the system administrator for the computer system in the dental office to ensure that each person using the software has his or her own code.

The same code may not be used by more than one staff member, for this makes it impossible to identify the person who entered or modified information in the file if necessary at a later date.

Each user code is unique and may not be assigned to more than one person. If a dentist or employee leaves the practice or is temporarily absent (owing to illness, vacation, radiation, etc.), his or her code may not be assigned to another person under any circumstances.

In addition, the use of the code must be protected by a confidential password. The user must memorize the password and not divulge it to anyone else.

Insofar as possible, the password must respect these criteria:

- contain from five to eight alphanumeric characters;
- contain at least one numeric character; and
- not be a common noun or well-known proper noun.

It is also recommended that the password include both upper- and lowercase letters and non-alphanumeric characters (e.g. &, %, $) to make it more difficult to decode.
For greater security, the system administrator could require that the software ask users to change their passwords frequently, ideally once a month. Finally, to protect the confidentiality of their passwords, users must make sure that the password does not appear on the screen when they are entering data. Although this is a very basic security measure, it ensures that only authorized users will have access to the software and the data it is used to manage.

Other security measures can also be worthwhile, such as the use of magnetic cards with a personal identification number (PIN) or smart cards.

2.1.2 Access to confidential or sensitive data

The dentist responsible for the record must specify which people have access to the record and which part of the record each person can access. The software must make it possible to prevent access to certain data for users who do not need to enter, modify or view this information in the course of their duties.

2.1.3 Back-up procedure

A back-up procedure is essential when software is used for record keeping. Dentists must ensure that a copy of the data entered is backed up every day, preferably at the end of the working day. The back-up copy must necessarily be kept elsewhere than at the office, so that the data can be restored quickly in the event of a disaster or theft of computer equipment.

A fairly large volume of data may eventually be stored on the system, so it is best to use an incremental back-up procedure, copying only the data entered or modified since the previous back-up. Since a complete copy of the data has already been saved previously, only the data that have been modified from day to day need be added in order to generate a complete and up-to-date copy.

Software suppliers may include back-up systems in their software; there are also many reasonably priced back-up programs available on the market.

2.1.4 Archiving data

It is recommended that data be archived when a patient’s record becomes too large or is closed. Archiving makes it possible to reduce the size of the files in the database and improves its efficiency and speed. Archived data must remain easily accessible.
The information placed in a record, whether it is archived or not, must be kept for five years from the date of the last entry, whatever it may be, or the last insertion in the file.

2.1.5 Restoring data in case of technical difficulties

Dentists must ensure that the software used for record keeping includes data retrieval and restoration functions in case of technical difficulties that could cause the alteration or loss of stored data.

Restoration must be possible quickly, without the help of the software supplier.

Back-up copies must be used as a last resort in the event of technical difficulties, since the data entered or modified during the day will have to be entered again after the system is restored, with the attendant risk of errors or omissions.

2.1.6 Printing reports and records

The software must make it possible to print reports and complete records. A complete record includes all the information placed in the record, information on the entry, modification or deletion of data, and digital X-rays. This information, once it has been printed, must be understandable and legible. Printouts must be on paper of acceptable quality.

The confidentiality of patient information must be respected when handling and using printed reports and records.

2.1.7 Replacing computers or record-keeping software

When replacing computers or software, dentists must ensure that unused confidential data have been completely destroyed and are not accessible to third parties. Reformatting the hard disk is the safest way of ensuring that data have been completely removed from the system.

2.2 Authentication and ability to retrace information

Dentists must ensure that the software they use can identify the user who initially entered information or later modified or deleted any data, and indicate the exact nature of the changes made to data.

In addition to the user code and the nature of the change made, the software must record the date and time of the operation.
Generally speaking, only the last information entered appears on the screen. The software must allow users to view and print the complete history of operations on a computerized record (information modified or deleted). The entry sequence must be shown in this history, which must be added to incrementally and automatically and must not be modifiable. A chronological list of all changes made to a file must be available and must clearly and precisely indicate the nature of the changes or deletions made, and identify the person who did so.

This requirement applies to data stored in the software as well as documents attached to a record, such as X-rays and other scanned data. Original X-rays must always be kept by the software and remain available for future consultation.

Only the dentist who performed a treatment may delete or modify data relating to that treatment.

The system administrator must ensure that the software makes it impossible to modify the system date or time.

2.2.1 Inalterability of information and attached documents

Dentists must ensure that the software prevents anyone from maliciously viewing, modifying or deleting data with external or internal data manipulation tools.

All the information in the database and all attached documents (X-rays or scanned documents) that can identify a patient must be encrypted. Encryption is an operation that makes the information illegible for malicious third parties. Only the supplier of the information can handle the information in the database, as the only one that knows the encryption method used.

Dentists may use digital X-ray equipment even if they do not use a computer system for record keeping. In that case they must ensure that the equipment they use to produce scanned X-rays complies with the DICOM standard, a recognized standard that ensures the integrity and inalterability of X-rays. All photos produced with other types of equipment that are also to be placed in the record must be placed there and signed by the dentist. Dentists who use a computer system for record keeping may place these photos in the computerized record.

2.2.2 Transferring computerized patient records

Dentists must ensure that the software can be used to transfer records if they sell their practice, close records, are struck from the roll or die. At the patient’s request, they must also be able to provide patients with a copy of their records that is legible by another computer system. To simplify the transfer of
computerized patient records among different authorized parties, the Ordre des dentistes du Québec has worked with three software suppliers to draw up a standardized patient record format containing information on the patient and on the treatments received. The categories of data considered include the 16 elements listed in section 1 (see p. 3), odontograms, scanned X-rays and other files from imaging equipment.

Detailed definitions of the content of the computerized record and the technical specifications are given in Appendix 2, so that all software suppliers can comply with them.

It must be possible to retrieve all these data, which are normally managed with recognized software, and to store them in a computer file. The file must be encrypted to ensure its confidentiality. Data must be retrievable:

- for a specific patient (complete record);
- for a specific patient, including only information on treatments performed by a specific dentist (partial record);
- for a patent, including all the records concerning the patient;
- for all the patients treated by a specific dentist;
- for all records required by the Ordre des dentistes du Québec in the exercise of its mandate to protect the public.

In addition, the software must be able to recognize data in a file imported from an external source (other software or other office). The software must be able to read this information and integrate it into the database.

The transfer of computerized patient records is authorized in the following cases:

- when a dentist leaves a dental office to join a new office, he or she may obtain in computerized form all the information concerning the patients he or she treated at the former office, and may then add these files to the software used by the new office;

- when files are transferred or upon the death of a dentist, the information concerning patients taken on by another dentist may be retrieved from the software and imported into that dentist’s software. A paper copy of patient records may also be produced, provided that it is complete, legible and printed on paper of acceptable quality;

- when the Professional Inspection Department or the Syndic of the Ordre des dentistes du Québec so requests, a dentist must retrieve the data requested and submit them as soon as possible;

- when the Secretary of the Order becomes the provisional custodian of a dentist’s records;
• when a patient so requests of his or her dentist.

The computer system installed in the dental office must include the equipment required to quickly and securely transmit data over the Internet or, at least, be equipped with a CD burner to record the data to be transferred on a compact disc.
Main purchase criteria for record-keeping software

1. **Security and confidentiality of information**

   User code and password:
   - each authorized person has his or her own user code;
   - the user code is protected by a confidential password;
   - the software frequently asks users to change their passwords;
   - the password is not legible on the screen.

2. **Limited access to confidential or sensitive data**

   The software makes it possible to prevent certain users from accessing certain data.

3. **Backing up**

   The software allows data to be backed up incrementally.

4. **Archiving data**

   The software allows data to be archived.

5. **Printing reports and patient records**

   The software allows only authorized users to generate and print reports;

   The software can be used to print complete and legible patient records.

6. **Restoring data in case of technical difficulties**

   The software must have data retrieval and restoration functions in case of technical difficulties;

   It must be possible to restore data quickly and without the help of the software supplier.
7. **Authentication and possibility of retracing information entered**

The software records information on users each time data is modified (initial entry, modification or deletion);

The software records the date and time whenever data are modified;

The software records the exact nature of the modifications to data (before and after images);

The software can be used to view a complete history, in chronological order, of all transactions in a record;

The software must keep the original of all X-rays and scanned documents relating to a record;

The software allows only the dentist who performed a treatment to delete or modify information relating to that treatment;

The software does not allow a user to change the system date or time.

8. **Inalterability of information and attached documents**

The software can be used to encrypt data relating to patient records;

The software can be used to encrypt X-rays and scanned documents.

9. **Transferring computerized patient records**

The software can be used to export and import information in the patient’s record:

- for a specific patient (complete record);
- for a specific patient, including only information on treatments performed by a specific dentist (partial record);
- for a patient, including all the records concerning the patient;
- for all the patients treated by a specific dentist.

The computer system can be used to quickly transmit data over the Internet or burn the data to be transmitted onto a compact disc.
TECHNICAL SPECIFICATIONS

1. Introduction ................................................................................................................... 14
   1.1. Purpose of the guide ..................................................................................... 14
   1.2. Associated documents .................................................................................. 14
2. Namespace .................................................................................................................... 15
   2.1. Language ...................................................................................................... 15
   2.2. Elements in the medical record .................................................................... 15
3. The patientRecord root ................................................................................................. 16
   3.1. Element: fileCreation ................................................................................... 17
   3.2. Element: office .............................................................................................. 18
   3.3. Element: patient ........................................................................................... 19
   3.3.1. Sub-element: annotation ........................................................................... 20
   3.3.2. Sub-element: treatment .............................................................................. 23
   3.4. Element: attachment ..................................................................................... 24
   3.4.1. Sub-element: document ............................................................................ 25
4. ##other .......................................................................................................................... 26
5. Modification journal ..................................................................................................... 27
6. Transfers to third parties ............................................................................................... 30
   6.1 Detecting corrupt and altered documents ...................................................... 30
   6.2 Errors and exceptions .................................................................................... 30
   6.2.1 Content of the error report ........................................................................... 31
   6.3. Creating the XML medical record and attached documents ........................ 32
   6.3.1. XML file name ........................................................................................... 32
   6.3.2. Names of attached documents ........................................................................ 32
   6.3.3. Export history ............................................................................................. 33
   6.4. Aggregation (coding) ................................................................................... 34
   6.5. Electronic signature ...................................................................................... 35
   6.6. Encryption ................................................................................................. 35
   6.7. Compression ................................................................................................. 35
   6.8. Transfer ........................................................................................................ 35
Appendix A – Example of an XML file ........................................................................... 36
Appendix B – Calculating the MD5 message digest ........................................................ 39
Microsoft .NET ................................................................................................... 39
ASP, JavaScript and VB6 .................................................................................... 39
Java ................................................................................................................ 40
Testing the algorithm........................................................................................... 40
1. Introduction

The software used in dental offices makes it possible to manage a wide variety of information relating to routine dental operations and the medical records of the patients treated.

The different duly authorized parties must be able to consult the information in the patients’ medical records.

There are a multitude of software programs on the market, each one with its own data structure. Accordingly, it is important to define a specific framework and a unique format so as to simplify reliable and efficient transfers of information in medical records and to protect the integrity and confidentiality of the data transferred.

This framework must be both well structured and expandable. Well structured, to simplify the development of a system able to read the computerized records produced by different software programs. Expandable, so that it can be easily adapted to future needs.

The XML (eXtensible Markup Language) standard was chosen to define the structure of a dental medical record. XML can be used to describe structured information and to exchange data with different platforms, applications, data formats and protocols.

1.1. Purpose of the guide

This Guide defines the format of a medical record in XML format using XML Schema 1.0. notation (See documents [2] and [6].)

The Guide is intended for technical staff responsible for developing computer systems for managing patient records in a dental office.

Readers are invited to familiarize themselves with the XML standard and XSD schemas used to define the content of an XML file.

1.2. Associated documents

[2] ODQPatientRecordV0.9.1.xsd: XSD schema
[4] demo.xsl: file for converting an xml file into HTML for viewing in a browser (Internet Explorer 6.0.28 required)
[5] The \ 051234567-DEFJ-002773 directory contains images to accompany the test file
[6] [html]/patientRecord0.9.html: documentation in the format generated by the schema
2. Namespace

The XML file uses the domain [http:www.odq.qc.ca/namespace. This is not a Website to be visited for each evaluation, but rather a way of distinguishing elements in the medical record defined by the Ordre des dentistes du Québec from possible extensions defined by other organizations.

```xml
<xs:schema targetNamespace="http://www.odq.qc.ca/namespace"
elementFormDefault="qualified" attributeFormDefault="unqualified">
```

2.1. Language

To simplify the adoption of this format by other organizations, the elements are defined with English terms (e.g. `firstName`, `toothCode`, etc.).

2.2. Elements in the medical record

The medical record in XML format consists of a number of nested elements, beginning with the `patientRecord` root element. An XML file must contain one and only one root element.

For the medical record, each file contains the record of a single patient.
3. The *patientRecord* root

This the root of the XML file. The only attribute of this element is “version”, which represents the version of the schema used to create the file. This attribute must be generated by the software when the XML file is exported.

For the current version, version= "0.9"

```
<patientRecord xmlns="http://www.odq.qc.ca/namespace"
xmns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.odq.qc.ca/namespace
ODQPatientRecordV0.9.xsd" version="0.9">
```

The dotted rectangles represent elements that may be omitted.

0..∞ represents an optional element that can be repeated indefinitely (0 to infinity).

The solid rectangles with no instructions as to occurrence must appear in the XML file only once (at the position specified).

##other means any element that belongs to another XML namespace than the current one (
(http://www.odq.qc.ca/namespace) and lets extensions be added.
3.1. Element: *fileCreation*

This element is mandatory and must appear only once, as the first child of the ‘*patientRecord*’ root.

It contains information on the software and the person who generated the medical record.

Example:

```xml
<patientRecord xmlns="http://www.odq.qc.ca/namespace"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.odq.qc.ca/namespace ODQPatientRecordV0.9.xsd" version="0.9">
  <fileCreation>
    <date>2002-03-15T10:30:47-05:00</date>
    <user>STF001</user>
    <comment>File created manually for demonstration. Not all XML file fields are displayed here; see the XML file for more details. Farid Agharabi</comment>
    <vendorName>Fournisseur X Systems inc.</vendorName>
    <softwareId>Simple Denturex V1.02 Build 43220. 03-04-2004</softwareId>
  </fileCreation>
```

...
3.2. Element: *office*

This element is mandatory and must appear only once, as the second child of the ‘*patientRecord*’ root, immediately after the ‘*creation*’ element.

It contains information on the office and its employees (dentists and office staff).

In theory, there may be more than one ‘office’.

Year 1, Day 1: treatment at office A

Year 2: Patient’s record is transferred to a new dentist, treatment at office B
3.3. Element: patient

This element is mandatory and must appear only once, as the third child of the ‘patientRecord’ root, immediately after the ‘office’ element.

It contains information on the patient and the person or organization responsible for his or her billing/insurance.
3.4. Element: *entry*

The ‘entry’ element may be repeated indefinitely (0 – infinity).
The first element must appear immediately after the ‘patient’ element.
Each ‘entry’ contains an ‘annotation’ type or ‘treatment’ type element (not both)
This element contains medical information on the patient.

3.4.1. Sub-element: *annotation*

This element appears only once in the ‘entry’ element. It contains an annotation, generally entered by the attending dentist.

When the ‘annotation’ element is included, the ‘treatment’ element may not appear in the same ‘entry’.
The different types of annotations are defined by the ‘type’ element, which is an enumeration:

The ‘content’ element contains a block of text that is normally entered by the person who made the observation or annotation.

An ‘annotation’ element may contain an indefinite number of attached documents. Note that the attached document to be defined in an ‘attachment’ element is specified (see below), but the document itself is never included in the XML file.
The following table lists the types of annotations.

<table>
<thead>
<tr>
<th>Annotation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>medicalHistory</td>
<td>Patient’s medical history or an update to the medical history</td>
</tr>
<tr>
<td>dentalHistory</td>
<td>Patient’s dental history or an update to the dental history; must contain the principal complaint and its history</td>
</tr>
<tr>
<td>odontogram</td>
<td>Original odontogram and evolving odontogram</td>
</tr>
<tr>
<td>examination</td>
<td>Dental examination performed</td>
</tr>
<tr>
<td>emergency</td>
<td>Emergency examination (emergency examination only, and not treatment)</td>
</tr>
<tr>
<td>examinationResult</td>
<td>Any examination performed or request for consultation and report from another professional; may be a blood test, pathological analysis of a biopsy, response to consultation by a specialist, etc.</td>
</tr>
<tr>
<td>Radiovisiography</td>
<td>Should include everything having to do with original and modified X-rays, intra-oral images, scanned study models, predictions and modifications of images created with software such as Cosmet-X, software-generated cephalogram plots, etc.</td>
</tr>
<tr>
<td>diagnosis</td>
<td>Diagnosis</td>
</tr>
<tr>
<td>prognosis</td>
<td>Prognosis: prediction of the length, evolution and end of a pathology; patient’s probable reaction to treatment</td>
</tr>
<tr>
<td>treatmentPlan</td>
<td>Treatment plan suggested to the patient; should include alternative treatment plans as well as their estimated cost</td>
</tr>
<tr>
<td>Treatment</td>
<td>Description of treatments performed: a description of everything that occurred during a treatment, including the type of anaesthesia, its quantity and concentration</td>
</tr>
<tr>
<td>Prescription</td>
<td>Written prescription for medication or treatment</td>
</tr>
<tr>
<td>Communication</td>
<td>The significant elements of every verbal or written communication with or pertaining to the patient, information and recommendations with respect to the treatment administered to the patient Notes, correspondence and other documents relating to services rendered by the dentist, and copies of all documents or certificates issued to the patient</td>
</tr>
<tr>
<td>Consent</td>
<td>Notes pertaining to information given to a patient concerning acceptance of treatment, and notes pertaining to receipt of the patient's consent for the treatment</td>
</tr>
<tr>
<td>Referral</td>
<td>The date on which the patient was referred to a health professional, the name of the professional, the purpose of the referral and the report issued after the referral consultation</td>
</tr>
<tr>
<td>Request</td>
<td>A note signed by the patient or his representative, where the patient has requested the removal of an item or document, indicating the nature of the item or document and the date on which it was removed</td>
</tr>
<tr>
<td>Other</td>
<td>Other annotations that the dentist is required to add under any applicable legislation</td>
</tr>
</tbody>
</table>
3.4.2. Sub-element: treatment

This element appears only once in an ‘entry’ element. It describes a treatment performed. Each treatment must appear in a separate ‘entry’ element.

When the ‘treatment’ element is included, the ‘annotation’ element may not appear in the same ‘entry’.
3.5. Element: attachment

The ‘attachment’ element may be repeated indefinitely (0 – infinity).
The first ‘attachment’ element must appear immediately after the last ‘entry’ element.
Each ‘attachment’ element contains information on an attached document.
Attached documents may be binary files, documents or images.

The different types of annotations are defined by the ‘type’ element, which is an enumeration:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScannedXray</td>
<td>Scanned X-ray</td>
</tr>
<tr>
<td>ScannedImage</td>
<td>Scanned image</td>
</tr>
<tr>
<td>GeneratedImage</td>
<td>Image generated by software (e.g. odontogram)</td>
</tr>
<tr>
<td>Video</td>
<td>Video</td>
</tr>
<tr>
<td>ScannedDocument</td>
<td>Scanned document (text + image)</td>
</tr>
<tr>
<td>Document</td>
<td>A binary or text document (e.g. an RTF or PDF document)</td>
</tr>
<tr>
<td>XmlGenerationReport</td>
<td>A document in text format that is to be used to report generation statistics and errors encountered (when generating the XML file)</td>
</tr>
</tbody>
</table>

See section 6.2 Errors and exceptions
3.5.1. Sub-element: document

The ‘document’ element defines the information necessary to rebuild the attached document, detect whether it has been corrupted or modified, and view it.

When a document (image or other) is attached to a patient record, the software must calculate a number representing the document “fingerprint” or message digest. This is done using the MD5 algorithm, [http://www.faqs.org/rfcs/rfc1321.html](http://www.faqs.org/rfcs/rfc1321.html), which produces a 128-bit number, regardless of the size of the document. In addition, the number must be stored in the database (DB) in an unalterable way. This makes it possible to detect any alteration or corruption of the attached document.

The storage format in the XML file is “xs:string”. The MD5 message digest must be stored with a string of 32 hexadecimal characters equivalent to 16 bytes (i.e. 128 bits). Each byte is coded with two characters from 00 to FF.

It is advisable to store the MD5 message digest in the same format in the database. When the XML file is generated, the field stored is entered as is in the ‘recordDigest’ attribute. Another MD5 message digest is recalculated when the export file is created, and its value is entered in the ‘currentDigest’ attribute.

The stored value and the calculated value should be the same, of course; otherwise the document has been altered or corrupted since it was stored in the database. Similarly, the recipient of the exported file can recalculate the MD5 message digest to ensure that the document has not been altered after being exported.
4. ##other

All ‘##other’ type fields denote elements that belong to another XML namespace than the current namespace (http://www.odq.qc.ca/namespaced). This makes it possible to add extensions to the current format or to mix elements belonging to different namespaces with no risk of conflict.
5. Journal

For each record that is to be protected from alteration, there must be a list of all modifications made.

The journalGroup list of fields makes it possible to keep track of all changes made to the record.

The ‘creation’ element defines information on the creation of the record.
The ‘modification’ element defines the fields of the record that have been modified. Each element may be repeated as many times as necessary. Each element represents one modification session.

The repeated ‘field’ elements are used to define the fields that have been modified, added or deleted during a modification session.
Finally, the ‘deletion’ element specifies the date of deletion and the user who deleted the record. Note that records do not disappear even once they have been deleted, for a ‘deleted’ indicator marks deleted records. See the ‘deleted’ attribute for the following elements:

patientRecord/attachment
patientRecord/attachment/document
patientRecord/entry
patientRecord/patient
patientRecord/patient/responsible/policy
patientRecord/office/users/provider
patientRecord/office/users/staff
patientRecord/patient/responsible
6. Transfers to third parties

6.1 Detecting corrupt and altered documents

When an image or other document is attached to a patient record, the software calculates a number representing the document’s message digest. This calculation is done when the document is entered in the DB, and again when the XML patient record is generated.

See the attachment/document/recordDigest and attachment/document/currentDigest elements and section 3.5.1. Sub-element: document.

The algorithm for calculating the MD5 message digest is available free of charge on the Internet. (See Appendix B.)

Detecting alterations in the exported XML file

In order to be able to detect altered or corrupt export files, the software proceeds in the same way as for attached documents: it calculates an MD5 message digest for the patient record generated (the XML file only), displays it to the user and stores it in its export history with the export date and time.

The recipient or sender may check at any time that an exported XML file is the intact and uncorrupted file and that it has not been modified since it was generated.

6.2 Errors and exceptions

If, when an XML file record is being generated, the software detects an anomaly in the DB or in the program itself, this incident must be noted in a report file and attached to the medical record, like any other attached file.

Remember to update the ‘errorDetected’ and ‘errorDescription’ attributes (see the recordAttributGroup in schema [2]) of the XML element to be generated, even if there is an error.

The following is a non-exhaustive list of errors:

<table>
<thead>
<tr>
<th>Nature of error</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB record corrupt</td>
<td>Report the error in the report file and generate the XML element if possible.</td>
</tr>
<tr>
<td></td>
<td>For instance, if the treatment date is known but the rest of the information is illegible, create an ‘entry/treatment’ element and indicate the date, but leave all the other fields blank.</td>
</tr>
<tr>
<td>Document or image cannot be found</td>
<td>Create an ‘attachment’ element with all available information and report the error.</td>
</tr>
<tr>
<td>The MD5 message digest calculated for a document does not correspond to the message digest calculated and stored in the DB when it was first scanned.</td>
<td>Create the element and report the error.</td>
</tr>
</tbody>
</table>
6.2.1 Content of the error report

An error report must be generated whenever the software detects an error. This is a text file containing:

- Generation information (see section

- A list of the errors detected, with explanations.
- The number of elements generated (e.g. 1 patient 14 entry 12 attachments).
- The number of elements containing errors.
- The report file must be attached with an ‘attachment’ element, like any other document attached to the file, with ‘type’ xmlGenerationReport.

6.3. Creating the XML medical record and attached documents

The medical record is created on request, with an XML format patient record export menu. The software must create the main file in XML format in a working directory and place the scanned documents and X-rays to be attached there.

6.3.1. XML file name

The name of the XML file is coded so as to identify the file without disclosing information on the patient.

nnnnnnnnn-AAAB-cccccc.XML

nnnnnnnnn: permit number of the dentist owning the file (9 Alpha Num)
AAA: first three letters of the patient’s family name
B: first letter of the patient’s first name
cccccc: Code unique to this patient in the office (patient’s unique alphanumerical file identifier), e.g. 051234567-DEFJ-002773.XML

6.3.2. Names of attached documents

The name of the attached document should be an anonymous code that does not identify the patient, e.g.:

02773-201120.DOC
02773-922-2022120.JPG
02773-924-222x20.DICOM
6.3.3. Export journal

The software must have an export journal so as to be able to identify the recipient of the export and the reason for it. The array must contain at least the following fields:

- Export date and time
- Status: success, failure
- Export recipient: e.g. “ODQ”, “dentist name”, “patient name”
- Comment: reason for export
- MD5 message digest: calculated for the XML file when it was exported (see section 6.1 Detecting corrupt and altered documents)
6.4. Aggregation (coding)

The aggregation process consists of combining the XML file and attached documents in a single file.

How can X-rays and other binary documents be added to XML?

The attached documents are NOT actually included in the XML file; they are included in a compressed file that contains all the files exported for a patient. The XML file refers to the attached documents and an MD5 message digest calculation system ensures that the documents are not tampered with.

The final result of the export is a .zip file containing the main file in XML format and attached documents in binary format (images, video, etc.) or text format. In addition, each element is encrypted with the recipient’s public key.

This means that it is always possible to ensure that the file (in .zip format) is complete without having access to the file content.

The result is a .zip file that can be stored on a computer or transmitted by e-mail with no risk of disclosing confidential information.

---

You can always list the directory contents of a .zip file, or give the command to verify its contents, but since each file is encrypted, it is not possible to examine the contents without decrypting it.
6.5. Electronic signature

In the current format version, dentists are not obliged to electronically sign the patient record. The compressed and encrypted file may simply be sent to the recipient.

6.6. Encryption

During the aggregation operation, the XML file and all attached documents are encrypted with a randomly created symmetric key. The symmetric key is then encrypted in turn with the recipient’s public key (the ODQ’s key, for purposes of the prototype) and the result is added to the compressed export file. Last, the file is saved on computer with a file name identical to the .XML file and the extension .DP for dossier patient (patient record).

Who can read an encrypted patient record?

- To decipher the patient record, you must have the recipient’s (ODQ) private key and the password associated with the key. So only the ODQ can decipher the record.

What organization issues certificates and public/private keys?

- For the purposes of the prototype, the certificates will be created by Stratégica for the ODQ. A production version will have to use the services of a recognized registrar like Verisign or Entrust.

6.7. Compression

Compression is done at the same time as aggregation (see above sections).

6.8. Transfer

Note that the unencrypted XML file or attached documents may not be transmitted directly to the recipient. Only the encrypted patient record may be transferred to a third party. In addition, the work directory and temporary files must be deleted.

Files may be transferred to a third party by e-mail or on a portable magnetic, electronic or optical medium.
Appendix A – Example of an XML file

<?xml version="1.0" encoding="UTF-8"?>
<patientRecord xmlns="http://www.odq.qc.ca/namespace"
xmllns:stra="http://www.strategica2000.com"
xmllns:odq="http://www.odq.qc.ca/namespace"
ODQPatientRecordV0.9.xsd" version="0.9" cda:extension="A">
<fileCreation>
  <date>2002-03-15T10:30:47-05:00</date>
  <user>STF001</user>
  <comment>File created manually for demonstration. Not all XML file fields are
displayed here; see the XML file for more details. Farid Agharabi</comment>
  <softwareId>Simple Denturex V1.02 Build 43220. 03-04-2004</softwareId>
</fileCreation>
<office>
  <name>Super Clinique Dentaire</name>
  <address>
    <line>Clinique médical Test</line>
    <city>Montreal</city>
    <postalCode>2V3 5V9</postalCode>
    <province>QC</province>
    <phone location="main">514-555-4454</phone>
    <phone location="fax">514-555-4456</phone>
    <phone location="other" note="Emergency: ">514-555-0991</phone>
    <email>info@descarries.qc.ca</email>
  </address>
  <users>
    <provider role="dentist" userId="STF001" recordId="us2">
      <title>Dr</title>
      <firstName>Marie</firstName>
      <lastName>Desjardins</lastName>
      <licenseNumber>05552273</licenseNumber>
    </provider>
    <provider role="dentist" userId="STF002" recordId="us6">
      <title>Dr</title>
      <firstName>Frank</firstName>
      <lastName>Walters</lastName>
      <licenseNumber>05560001</licenseNumber>
    </provider>
    <staff role="clerical" userId="STF003" recordId="us4">
      <firstName>Louise</firstName>
      <lastName>Tremblay</lastName>
    </staff>
    <staff role="technicalSupport" userId="STF999" recordId="us5">
      <firstName>Support technique</firstName>
    </staff>
  </users>
</office>
<patient disabled="false" recordId="pat001" deleted="false">
  <ownerProvider>STF001</ownerProvider>
  <lastVisit>2001-01-17</lastVisit>
  <firstName>Jean</firstName>
  <lastName>De Florette</lastName>
  <birthday>1967-08-13</birthday>
  <address>
    <line>523 Rue Béole</line>
    <city>Saint-Hubert</city>
    <postalCode>J3Y 9P1</postalCode>
    <province>QC</province>
  </address>
  <phone location="main">450-555-3212</phone>
</patient>
</patientRecord>
Complete examination
X-rays - 4 interproximal and 2 periapical and panoramic
Appendix B – Calculating the MD5 message digest

The MD5 algorithm [http://www.faqs.org/rfcs/rfc1321.html](http://www.faqs.org/rfcs/rfc1321.html) produces a 128-bit number, regardless of the size of document it is applied to.

The MD5 message digest must be stored with a string of 32 hexadecimal characters equivalent to 16 bytes (i.e. 128 bits). Each byte is coded with two characters from 00 to FF.

E.g.: 0x01, 0xae, 0x03, 0x9a... is transformed into "01ae039a..."

Here are some references on MD5 algorithms available on the Internet:

*All algorithms must be able to read the content of an attached document and produce the MD5 result in the format of a 32-character string.*

**Microsoft .NET**

NET Framework Class Library MD5 Class


**ASP, JavaScript and VB6**

This site contains tools and their sources for calculating the MD5 message digest:

[http://www.frezz.co.uk/freecode.htm#md5](http://www.frezz.co.uk/freecode.htm#md5)

**C language**

[http://theory.lcs.mit.edu/~rivest/md5.c](http://theory.lcs.mit.edu/~rivest/md5.c)
Java

Here is an example of Java code for calculating the MD5 message digest with the MessageDigest classes in Java..

```java
MessageDigest md = MessageDigest.getInstance("MD5");
FileInputStream fis = new FileInputStream(file);
DigestInputStream dis = new DigestInputStream(fis, md);
int ch;
while ( (ch = dis.read()) != -1)
{
    byte digest[] = md.digest();
}
```

Here is an example of Java code for transforming the message digest (16-byte array) into a character string.

```java
static private String byteToHex(byte b)
{
    Integer I = new Integer( ( ( (int) b) << 24) >>> 24);
    int i = I.intValue();
    if (i < (byte) 16)
        return "0" + Integer.toString(i, 16);
    else
        return Integer.toString(i, 16);
}
```

```java
/**
 * Transforms the array 'b' into a string of hexadecimal values
 * @param b byte[]
 * @return String
 */
static public String toHex(byte[] b)
{
    if (b==null) return "";
    StringBuffer s = new StringBuffer("\n    int i;
    for (i=0; i<b.length; i++)
        s.append(byteToHex(b[i]));
    return s.toString();
}
```

Testing the algorithm

You can test your algorithm by running it on the `\samples\odontol.png` file (included in the kit accompanying this guide).

The MD5 message digest must be:

"cd7b3febf72e958996d3c5c7360defdb"

Note that the algorithm must open the file in binary mode and handle CR/LF characters like other characters; otherwise the calculation will give a different message digest.
Appendix 3

REGULATION RESPECTING THE KEEPING OF DENTAL OFFICES AND RECORDS AND THE CESSATION OF PRACTICE OF A MEMBER OF THE ORDRE DES DENTISTES DU QUÉBEC

Professional Code
(R.S.Q., c. C-26, s. 91)

THIS DOCUMENT IS NOT THE OFFICIAL VERSION
THE TRANSLATION IS NOT OFFICIAL

DIVISION I
GENERAL PROVISION

1. Nothing in this regulation shall be interpreted as excluding the use of computers or other technological means in drawing up, keeping or preserving records or registers.

DIVISION II
KEEPING OF DENTAL OFFICES AND MAINTENANCE OF EQUIPMENT

2. A dentist shall display his permit and proof of enrolment on the roll of the Ordre des dentistes du Québec, as well as the permits and proofs of enrolment of other members of professional orders employed by him, in public view in every office in which he practises.

3. A dentist shall have a waiting room for his patients.

4. A dentist’s office must be designed so as to ensure confidentiality.

5. A dentist’s office must be arranged so that:

   (1) Medications and volatile inflammable or toxic substances are stored securely;

   (2) Medications are stored in accordance with the standards prescribed by the manufacturer;
(3) Drugs and other substances within the meaning of the Controlled Drugs and Substances Act (S.C., 1996, c. 19) are stored under lock and key.

6. In arranging his office, a dentist shall ensure that standards of asepsis, cleanliness and safety are applied in accordance with generally recognized scientific standards in the profession, in order to avoid any danger of contamination or transmission of infection.

7. A dentist shall take the steps required to dispose in an environmentally secure way of the biomedical waste generated by the operation of his office.

8. A dentist shall have, in his office, the equipment and products required to ensure the sterilization of his instruments and the disinfection of his equipment and premises.

9. A dentist shall have, in his office, in a place that is accessible to and known by all persons working for him, the materials, including medications, required to provide appropriate treatment in an emergency. He shall also ensure that the materials are in perfect working order, and shall renew the medications periodically.

10. A dentist shall see to the maintenance of any equipment he uses to ensure that it is in perfect working order.

11. Any piece of equipment that may be inspected, calibrated or tested, including sterilization, X-ray and sedation equipment, shall be checked as often as its optimum efficiency requires, taking into account equipment specifications and generally recognized scientific standards.

12. A dentist shall keep up-to-date a register containing the date of the verification, the equipment identification, the results obtained and the name and signature of the person who carried out the verification. The dentist shall preserve the register for a period of at least five years from the date of the last entry.

13. A dentist shall keep up-to-date a register identifying the prescription medications and volatile inflammable or toxic substances held by him, along with the dates on which they are used and, where applicable, the dates on which they are disposed of. The dentist shall preserve the register for a period of at least five years from the date of the last entry.

DIVISION III
KEEPING OF RECORDS

14. A dentist shall draw up and keep a record for each patient he treats and shall preserve the record in accordance with the provisions of this Division.

The same applies to a dentist who practises in an institution within the meaning of the Act respecting health services and social services (R.S.Q., c. S-4.2) and the Act respecting health services and social services for Cree Native persons (R.S.Q., c. S-5), unless such a record is drawn up and preserved by the institution and the dentist is able to comply with the provisions of this division.

15. The name of the dentist who drew up the record, the date on which it was drawn up, and the name, gender, date of birth, address and telephone number of the patient shall appear clearly in each record.

16. Where applicable, the dentist shall enter or attach the following particulars in every record pertaining to a patient:

(1) the date of the consultation;
(2) the patient's medical and dental history;
(3) the diagnosis;
(4) the choice of treatment and prognosis;
(5) a list of operations and a description of every form of treatment performed;
(6) the material and medication used in the treatment;
(7) written prescriptions for medications or treatments;
(8) the significant elements of every verbal or written communication with or pertaining to the patient;
(9) examination results, diagnostic features and, where applicable, X-ray reports, along with all models;
(10) notes pertaining to information given to a patient concerning acceptance of treatment, and notes pertaining to receipt of the patient’s consent for the treatment;
(11) the name, concentration and quantity of anaesthetics used in the case of a general, regional or local anaesthetic or conscious or total sedation;
(12) information and recommendations with respect to the treatment administered to the patient;
(13) the date on which the patient was referred to a health professional, the name of the professional, the purpose of the referral and the report issued after the referral consultation;

(14) notes, correspondence and other documents relating to services rendered by the dentist, and copies of all documents or certificates issued to the patient;

(15) information concerning the professional fees and any sums invoiced to the patient;

(16) a note signed by the patient or his representative, where the patient has requested the removal of an item or document, indicating the nature of the item or document and the date on which it was removed.

Every note written in the record must be legible.

At each consultation, the dentist shall note any changes to the elements listed in the first paragraph.

17. The dentist shall sign, initial or identify any information or entry made in the record by himself or by any other person. He shall ensure the integrity and permanence of the information contained in the record.

18. The dentist may, at any time and with the authorization of the patient or his representative, transfer the original or a copy of all or part of the record to another dentist.

The dentist shall draw up and preserve a list of the items and documents contained in the record or part thereof that was so transferred. A copy of the list shall be sent to the other dentist with the items and documents in question.

19. Where an item or document contained in the record is given to the patient, the dentist shall insert a note in the record, signed by the patient or his representative, indicating the nature of the item or document and the date on which it was removed.

20. The dentist shall take all necessary steps to ensure that the information contained in the record is transferred or handed over in a confidential manner.

21. The dentist shall preserve his records or ensure that they are preserved in a room or cabinet to which the public does not have access, or that can be locked or otherwise secured to ensure the confidentiality of the records.
22. The dentist shall keep each record for at least five years from the date of the last entry, whatever it may be, or the last insertion.

Upon the expiry of the five-year period, the dentist may destroy the record, provided he does so in a manner that ensures the confidentiality of the information contained therein.

23. A dentist who changes his principal place of practice or any other place of practice shall, within 30 days of the said change, publish a notice in a newspaper serving the region of the place in which he practised, indicating his name, the address of the new place of practice, and his telephone number.

The notice shall, where applicable, also indicate:

(1) that he continues to hold and keep the records of the patients who have consulted him;  

(2) that he has entrusted the records of the patients who have consulted him to another dentist, whose name, principal place of practice and telephone number are mentioned.

A copy of the notice shall be sent to the secretary of the Order.

DIVISION IV

DISPOSAL OF RECORDS WHERE THE DENTIST CEASES TO PRACTISE

1. Permanent cessation of practice

24. A dentist who decides to cease to practise permanently, or who ceases to practise permanently because he has agreed to perform a duty that prevents him from completing the mandates entrusted to him shall, at least 15 days before the date on which the cessation is to take effect, notify the secretary of the Order by registered mail, of the date of cessation and of the name, address and telephone number of the dentist who has agreed to be the transferee of his records, and shall send a copy of the transfer agreement to the secretary of the Order.

Where the dentist has been unable to arrange for a transfer, the notice shall indicate the date on which the dentist will hand over the records to the secretary of the Order.

25. Where a dentist dies or is permanently struck off the roll, or where a dentist's permit is revoked, the secretary of the Order shall take possession of the dentist's records within 15 days following the event, unless the dentist had arranged for a transfer, in which case a copy of the transfer agreement shall be sent to the secretary of the Order within the same time.
26. Where a transfer had been arranged for but cannot be carried out, the secretary of the Order shall take possession of the dentist’s records.

27. Where a dentist permanently ceases to practise, the transferee or the secretary of the Order, as the case may be, shall, within 30 days following the date on which the transferee or the secretary of the Order takes possession of the dentist’s records, give one of the following notices:

(1) A notice published twice, at a 10-day interval, in a newspaper serving the region where the dentist practised; the notice shall state:

a) the date of taking of possession and the reasons therefor;

b) the time available to patients to accept the transfer, to take back their record or to request that the record be transferred to another professional;

c) the address and telephone number of the transferee or the secretary of the Order, and the office hours during which that person can be reached; or

(2) A notice in writing to each patient of the dentist who has ceased to practise, stating the information prescribed in subparagraph 1.

Where the notice has been published, a notice in writing stating the information prescribed in subparagraph 1 shall also be sent to any patient whose interests so warrant.

Where the notice is sent by the transferee, a copy shall be sent to the secretary of the Order.

28. Where a transferee or the secretary of the Order is in possession of the records of a dentist, that person shall take the necessary measures to safeguard the interests of the dentist’s patients.

29. A transferee or the secretary of the Order, as the case may be, shall respect a person’s right to consult and obtain copies of documents concerning the person and contained in a record made in the person’s regard. The cost of obtaining such copies shall be paid by the person who requests them.

30. Where a transferee or the secretary of the Order takes possession of the records of a dentist, that person shall keep them for a period of not less than five years.

During that period, the secretary of the Order may transfer the records to a transferee, in which case the transferee is bound by the requirements of section 27.
2. Temporary cessation of practice

31. A dentist who decides to cease to practise for a period of more than six months, or to cease to practise temporarily because he has agreed to perform a duty that prevents him from completing the mandates entrusted to him shall, at least 15 days before the date on which the cessation is to take effect, notify the secretary of the Order, by registered mail, of the date of cessation and of the name, address and telephone number of the dentist who has agreed to be the provisional custodian of his records, and shall send a copy of the provisional custodianship agreement to the secretary of the Order.

Where the dentist has not been able to arrange for provisional custodianship, the notice to the secretary of the Order shall indicate the date on which the secretary of the Order or the provisional custodian appointed for that purpose by the Bureau will take possession of the records.

Where a dentist ceases to practise for a period of not more than six months, he shall take the steps required to safeguard the interests of his patients.

32. Where a dentist is temporarily struck off the roll or where a dentist's permit is suspended, the secretary of the Order shall take possession of the records within 15 days of the event, unless the dentist has arranged for provisional custodianship by another dentist, in which case a copy of the provisional custodianship agreement shall be sent to the secretary of the Order within the same time.

Where the dentist has not been able to arrange for provisional custodianship within that time, the secretary of the Order shall take possession of his records, unless a provisional custodian has been appointed for that purpose by the Bureau.

33. Where provisional custodianship had been arranged for but cannot be carried out, the secretary of the Order shall take possession of the dentist's records.

34. Sections 28, 29 and 30, as the case may be, shall apply to a provisional custodian or to the secretary of the Order where that person takes possession of a dentist's records pursuant to this Division.

35. The secretary of the Order or the provisional custodian shall return the records to the dentist immediately after the end of the temporary cessation period.

36. Where a dentist is temporarily struck off the roll or where a dentist's right to practise is suspended for more than six months, the provisional custodian or the secretary of the Order is bound by the requirements of section 27.
3. Restriction of the right to practise

37. Where a decision has been rendered against a dentist, restricting that person’s right to practise and determining the professional acts that the dentist is not authorized to perform, the dentist shall find a provisional custodian within 15 days of the date on which the restriction is to take effect, and shall notify the secretary of the Order, by registered mail, of the name, address and telephone number of the dentist who has agreed to be the provisional custodian of his records or parts thereof relating to the unauthorized professional acts, and shall send a copy of the provisional custodianship agreement to the secretary of the Order.

Where the dentist has not been able to arrange for provisional custodianship, the notice to the secretary of the Order shall indicate the date on which the secretary of the Order or the provisional custodian appointed for that purpose by the Bureau shall take possession of his records or the parts thereof that relate to the unauthorized professional acts.

38. Sections 28, 29 and 30, as the case may be, apply to a provisional custodian or to the secretary of the Order where that person takes possession of a dentist’s records pursuant to this Division.

DIVISION V

FINAL PROVISIONS


40. This regulation comes into force December 23, 2004.