GUIDELINES

Electronic Records Management

Approved by Council – March 2012

The Guidelines of the Royal College of Dental Surgeons of Ontario contain practice parameters and standards which should be considered by all Ontario dentists in the care of their patients. It is important to note that these Guidelines may be used by the College or other bodies in determining whether dentists have maintained appropriate standards of practice and professional responsibilities.

CONTENTS

INTRODUCTION 2

ELECTRONIC RECORDS MANAGEMENT 4
- What are Records? 4
- Electronic Records 4
  - Authenticity 4
  - Reliability 4
  - Useability 4
  - Integrity 4

REQUIREMENTS OF ELECTRONIC RECORDS MANAGEMENT SYSTEMS 5
- Physical Access Controls 7
- Logical Access Controls 7
  - Identification and Authentication 7
  - Authorization 7
- Audit and Accountability Controls 8
  - Individual Accountability 8
  - Reconstruction of Events 9
  - Intrusion Detection 9
- Data in Motion 9
  - E-Mail 9
  - Laptop Computers and Other Portable Storage Devices . . . 9
  - Wireless Devices 10
  - Teleworking 10
- Back-Up and Contingency Planning 10
- Data Migration 11
- Retention and Disposal 11

SECURITY POLICY FOR THE DENTAL OFFICE 12

PRIVACY REQUIREMENTS UNDER PHIPA 13

ADDITIONAL ISSUES 14

APPENDIX 15
- Additional Resources and Reference Materials Available on the Internet 15

Royal College of Dental Surgeons of Ontario

Ensuring Continued Trust

6 Crescent Road
Toronto, ON Canada M4W 1T1
T: 416.961.6555 F: 416.961.5814
Toll-free: 800.565.4591 www.rcdso.org

Introduction

Professional, ethical and legal responsibilities dictate that dentists must create and maintain records documenting all aspects of each patient's dental care. The extent of these records will vary, depending on the conditions with which the patient presents and the complexity of the treatment that is required. However, certain baseline data should be kept for all patients, as described in the College's Guidelines on Dental Recordkeeping. This information includes:

- accurate general patient information;
- a medical history that is regularly updated;
- a dental history;
- an accurate description of the conditions that are present on initial examination, including an entry such as "within normal limits" where appropriate;
- a record of the significant findings of all supporting diagnostic aids, tests or referrals such as radiographs, study models, reports from specialists;
- a diagnosis and treatment plan;
- a notation that informed consent was obtained from the patient for treatment;
- a notation that patient consent was obtained for the release of any and all patient information to a third party;
- a description of all treatment that is provided, materials and drugs used and, where appropriate, the outcome of the treatment;
- an accurate financial record.

In addition to their content, the manner in which records are created and maintained will vary and, in many respects, this is currently changing. Historically, dentists have used paper charts and ledgers to keep records for their patients.

However, the use of electronic records by dentists, including digital radiography, has grown substantially in Ontario, and the sophistication of hardware and software has evolved significantly since the Guidelines on Dental Recordkeeping were originally issued in June 1995.

Dentists are permitted to use electronic records for their patients, but they must comply with all requirements of traditional dental records. Moreover, the nature of electronic records raises additional issues for both dentists and patients, particularly with respect to accuracy, authenticity and access.

According to Health Canada, patient management software fits the definition of a medical device and must be classified in accordance with the rules under the Medical Devices Regulation.

Any patient management software that is used only for visualizing, acquiring, transferring or storing data or images is considered a Class I medical device.

Any patient management software with capabilities beyond basic data visualization, acquisition, transfer and storage is considered a Class II medical device, which requires a valid ISO 13485:2003 Quality System Certification, as well as a valid licence for sale, importation and distribution in Canada. This includes any patient management software involved in data manipulation, data analysis, data editing, image generation, determination of measurements, graphing, flagging of results, identifying a region of interest or performing calculations.

There is increasing pressure on all health care professionals to convert from paper records to electronic records. The province of Ontario has committed to implementing a comprehensive electronic health record for all Ontarians, and similar efforts are being made in other provinces and nations.

Electronic records offer many benefits to dentists and patients. They require less space and fewer administrative resources to maintain, while supporting improved clinical decision-making, leading to more effective diagnosis and treatment, greater patient safety and increased efficiency. On the other hand, electronic records present unique security and privacy risks, such as the potential for exposing the personal health information of patients to hackers and others with malicious intent. The design and implementation of an electronic records management system requires careful consideration in order to address these risks, including the use of access controls, audit trails, encryption and other safeguards.

The risk of exposing personal health information may be greatest during the transition from paper records to electronic records. Many factors converge to increase this risk:

- Staff may not be fully trained on using the new electronic records management system, increasing the likelihood of human errors.
- During the initial implementation phase, the new electronic records management system may not be fully functional, and the security and privacy features of the system may be either turned off or set to a default minimal standard of protection.
- The conversion of existing paper records to electronic format may require more frequent access to records of personal health information by a broader range of persons than would normally be the case.
- Records may be duplicated in both paper and electronic formats, potentially doubling the volume of records that need to be protected.
- The archiving, retention and disposal of paper records, if not carried out in a secure manner, may also pose a threat to security and privacy.
- Dentists may require assistance from third-party service providers to make the transition, creating an additional layer of complexity to the security and privacy risks that must be managed.

To date, there have been few guidelines regarding electronic records management for health care professionals. Those dentists who wish to use electronic records should implement these guidelines as soon as practicable. The purpose of this document is to describe the essential principles in managing and protecting electronic records from the moment of their creation or capture, as well as the minimum requirements of related electronic records management systems.

IMPORTANT

In this document, the following assumptions have been made:

1. Electronic records comply with all recordkeeping principles and requirements, as outlined for traditional dental records.
2. The electronic records management system is based on a private computer and network infrastructure (e.g. privately managed local area or wide area networks), where the ultimate control and responsibilities remain with the dentist, and does not involve any hosting or management of patient records with an external service provider (e.g. cloud computing).
3. All electronic copies of patient records in all locations are appropriately secured.
4. The electronic records management system has no wireless access points, unless they are appropriately secured.
5. The term “user” encompasses any entity that may access the electronic records management system, including a person, a computer services account, a software application or a computer system.

Electronic Records Management

WHAT ARE RECORDS?

In dentistry, a record is any item of information, regardless of form or medium, that is created or received by a dentist, dental office or health profession corporation, and that is maintained in the pursuit of providing care to patients and conducting business. Records are maintained as a valuable resource in the safe and efficient delivery of dental services, to provide evidence of the dentist's clinical and financial interactions with patients, to ensure practice continuity in the event of a disaster, and to satisfy legal and regulatory requirements.

ELECTRONIC RECORDS

An electronic or digital record is any item of information that is created, recorded or stored on any medium in or by a computer system or other similar device. Electronic records include, but are not limited to, computer files (e.g. documents and spreadsheets), digital images (e.g. JPG, BMP, TIFF), digital video (e.g. MPG, AVI), e-mails in their original format and any attachments, databases (e.g. SQL, Microsoft Access, FileMaker), and all back-up copies.

Electronic records are produced and used for the same purposes as traditional dental records. Therefore, it is essential that they are securely created, stored, accessed and managed so as to ensure and preserve their documentary and evidentiary value, as well as the privacy of personal health information.

Electronic records management is a framework of policies, procedures and processes that leads to the creation and maintenance of authoritative electronic records, which have the following characteristics.

Authenticity
An authentic electronic record can be proven to be what it purports to be. This includes being able to prove who created it and when. To provide for authenticity, adequate controls are necessary to ensure that the creator of an electronic record is identified and authorized, and that the record is protected against unauthorized use, alteration or concealment.

Reliability
A reliable electronic record can be trusted as a full and accurate representation of the facts. The record should be created at the time of or soon after the event to which it relates by a person who has direct knowledge of the facts.

Useability
A useable electronic record can be located, retrieved, presented and interpreted. As well, the links between records that document a sequence of activities should be maintained.

Integrity
The integrity of an electronic record refers to its being complete and unaltered. To provide for integrity, a record must be protected against unauthorized alteration. Any authorized annotation, addition or alteration to a record should be explicitly indicated and traceable.

Requirements of Electronic Records Management Systems

An Electronic Records Management System (ERMS) captures and organizes electronic records, manages and protects them from unauthorized use or alteration, and provides access to all relevant records and related information over time. An ERMS should be designed and implemented to assist health information custodians in meeting their privacy requirements under Ontario's Personal Health Information Protection Act (PHIPA).

An ERMS is comprised of software applications and supporting hardware that automates and integrates the records management principles. The ERMS should:

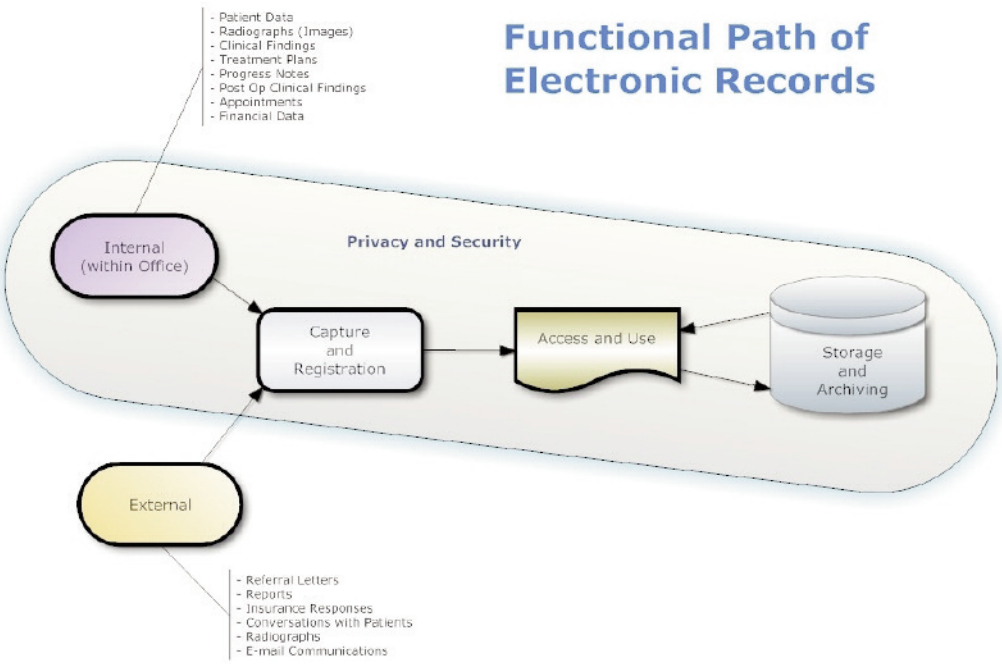
- be robust and capable of regular use, and the reliability of its operation should be documented;
- have adequate processing power and storage to meet the capacity demands of the dental office;
- be capable of periodic upgrades to reflect the changing requirements of the dental office.

Documentation should be kept of any servicing and maintenance of computer equipment and other elements of the system.

An electronic record may be created within the dental office or received from an external source in a variety of media. The record must be captured by the ERMS through a formal registration process that assigns it a unique identifier and persistently associates it with relevant information, also known as metadata, which should be validated.

Metadata provide a brief description about the electronic record that facilitates organization and retrieval, and link it to other records for the patient. As a minimum, metadata should include the following:

- the unique identity of the creating user;
- the unique identity of the patient;
- an accurate date and time stamp;
- the nature of the record (e.g. document or image);
- the access status assigned to it.



Each patient must be assigned an identifier or patient ID that can uniquely identify the patient within the ERMS. The patient's health or social insurance number must not be used for this purpose.

Following their capture, electronic records must be stored and preserved by the ERMS for as long as they are needed, and under conditions that will protect them from unauthorized access, loss or corruption.

The retrieval and use of electronic records is managed through the application of access controls for authorized users of the ERMS, as described in the following sections on physical and logical access controls.

The ERMS must be capable of the following:
- providing a secure means of access to all recorded clinical and financial information for each patient by the patient's name;
- visually displaying, printing and exporting by secure means all recorded information for each patient promptly and in chronological order.

Authorized alterations to an electronic patient record are permitted through the application of auditable controls, in which the original record is maintained in a read-only format and cannot be modified or deleted, and is merely demoted by a more recent or current version. The ERMS should be capable of providing an accurate visual display of all previous versions of any record, as well as the associated metadata, at any point in the past.

Electronic financial records must provide an accurate statement of each patient's account and minimally provide the date and amount of all:
- fees charged;
- commercial laboratory fees that were incurred;
- payments received, including the method of all payments;
- adjustments to the account.

As well, electronic financial records should provide an accurate reflection of the current status or running balance of each patient's account, in keeping with standard accounting practices.

Electronic images (e.g. digital radiographs, digital photographs) must be captured and maintained to the same standard as all other electronic records for the patient, including registration of metadata, and should be exportable in a format compatible with the International Standards Organization (ISO) referenced Digital Imaging and Communications in Medicine (DICOM) Standard.

For convenience, a paper record, dental radiograph or study model for a patient may be converted to electronic format by scanning it. A tamperproof digital image should be captured by the ERMS, which serves as a copy of the original. The paper record, dental radiograph or study model may then be placed into storage and archived.

Although they may be copied by scanning, it is important to note that original paper records, dental radiographs and study models for a patient must be retained and maintained as required by the regulations.

In order to ensure that authoritative electronic records are captured and maintained, an ERMS must employ a variety of safeguards or controls that regulate who may gain access to the system and what they may do.

If access is the ability to do something with a system resource, access control is the function of enabling or restricting this ability, which may be accomplished through both physical and technical safeguards.

PHYSICAL ACCESS CONTROLS

Physical access controls are physical safeguards that are taken to limit persons from entering or observing designated areas of the dental office that contain computer equipment and other elements of the system (e.g. servers, workstations, telephone and data lines, back-up media, etc).

Examples of physical access controls include:

- locked doors and security systems to restrict after-hours entry to the dental office;
- positioning servers and workstations in areas of the dental office that are secure during normal business hours;
- positioning or shielding monitors so that their displays are not observable by persons in other areas, such as waiting rooms;
- using logout and/or automatic timeout at unattended or idle workstations.

LOGICAL ACCESS CONTROLS

Logical access controls are technical safeguards that are taken to limit the information persons and other users can access, the modifications they can make and the software applications they can run. These safeguards may be designed into computer and network operating systems, incorporated into software applications and system utilities or carried out by add-on security programs.

Logical access controls are the means by which policy decisions are implemented and enforced. They enable staff to have access to the information they need to carry out their duties, while controlling the kind of access they are allowed and restricting their access to information that is not job-related.

Most access controls are based on who is attempting to use the system (i.e. identification and authentication) and what privileges they have to use a system resource (i.e. authorization).

Identification and Authentication

Identification is the means by which a user provides the system with a claimed identity or user ID. Authentication is the means by which the user establishes the validity of this claim. There are three primary methods of authenticating a user's identity, which should be used in combination. The user may provide:

1. a secret, such as a password or personal identification number (PIN);
2. a token, such as a swipe or security card;
3. a biometric, such as a fingerprint or retina scan.

> THE USE OF MINIMUM TWO-FACTOR AUTHENTICATION (I.E. A COMBINATION OF TWO METHODS) IS STRONGLY RECOMMENDED.

Identification and authentication are essential to computer security, as they are the basis for most access controls, which must recognize authorized users of the system and differentiate between them. In addition, they provide for accountability by linking specific users to their activities on the system, whether they are accessing the system from within the dental office or remotely.

Ideally, the identity of a potential user is established once and registered with the system, before access control decisions are made and privileges assigned to a unique user ID.

Authorization

Authorization is the means by which a user is granted permission to access a system resource. Most systems use role-based access controls that rely on staff job titles to define privileges. In this way, staff are provided access to information on a need-to-know basis. In addition, staff are limited in their ability to perform certain functions, based on the kind of access they require to carry out their duties.

There are three basic types of functions:

1. Read – The user can read information in a system resource, such as a patient record, but cannot alter it.
2. Write – The user can add information in a system resource.
3. Execute – The user can run a program.

These privileges may be used alone or in combination. For example, an individual staff member may be given read and write access to patient records, but not execute privileges to run programs.

In appropriate circumstances, an individual staff member may be registered with more than one non-overlapping role in the dental office, each with a unique user ID, in order to carry out specific tasks. In all circumstances, the ERMS should ensure that a user may access applications and services in only a single role at a time.

Although privileges are assigned to authorized users at initial registration, they should be reviewed at least annually and changed as required. Further, the system must support the revocation of access privileges; that is, a user must be immediately prevented from accessing the system once his/her privileges have been revoked.

FULL ACCESS TO THE SYSTEM MUST BE STRICTLY LIMITED AND NEVER GRANTED TO ANYONE WITHOUT ABSOLUTE NEED. THE DENTIST MUST RETAIN ULTIMATE CONTROL OVER THE SYSTEM AND ASSUMES FINAL RESPONSIBILITY FOR ENSURING THAT ITS RESOURCES ARE APPROPRIATELY USED.

AUDIT AND ACCOUNTABILITY CONTROLS

An audit trail is a record of events or actions concerning the activity of the operating system, a software application or a person using the system.

A system may have several audit trails, each devoted to maintaining a record of a specific type of activity.

Audit trails are the means by which several security-related objectives are accomplished, including individual accountability, the reconstruction of events and intrusion detection.

Audit trails should contain the necessary information to answer the following questions:

- For a given user, what patient record did the user access, create or alter, what did the user do and when?
- For a given patient record, what users have accessed, created or altered the patient record, what did the users do and when?

AT MINIMUM, AN AUDIT TRAIL MUST CONTAIN THE FOLLOWING INFORMATION:

A) THE UNIQUE IDENTITY OF THE ACCESSING USER;

B) THE ROLE THE USER IS EXERCISING;

C) THE PRACTICE LOCATION AND SPECIFIC COMPUTER IDENTIFICATION OF THE ACCESSING USER;

D) THE IDENTITY OF THE PATIENT;

E) THE ACTIVITIES PERFORMED BY THE ACCESSING USER;

F) AN ACCURATE DATE AND TIME STAMP.

Individual Accountability

Audit trails ensure that users are accountable for their actions by recording their activities on the system. They work in concert with logical access controls, which limit the ability of users to access system resources. While users cannot be prevented from accessing resources to which they have legitimate authorization, audit trail analysis can be used to examine their activities.

For example, an audit trail should be capable of displaying the content of a patient record at any point in the past, as well as the associated metadata of who accessed the record, what alterations were made and when this was done.

Reconstruction of Events
Audit trails may be used to reconstruct events after a technical problem occurs in order to identify how, when and why normal performance or functionality of the system ceased. Audit trail analysis of the activity of the system can often distinguish between user-induced errors (during which the system may have performed exactly as instructed) or system-created errors.

For example, if the system fails or the integrity of a patient record is questioned, an analysis of the audit trail can reconstruct the series of steps that were carried out by the system, a software application or any user.

In addition, audit trails may aid in the recovery process. For example, if a patient record is corrupted, an audit trail analysis can be done to ascertain the alterations made and reconstruct it.

Intrusion Detection
Audit trails may be used to detect users attempting to gain unauthorized access to the system. They may also be used to detect changes in the system's performance or functionality, which might indicate a virus or worm attack. Attention can then be focused on damage assessment or reviewing controls that were attacked.

It is important to note that the use of audit trails is fundamental in establishing the authenticity and integrity of stored records. Therefore, access to audit trails must be strictly limited to protect them from tampering. In addition, audit trails:

- must be operational at all times;
- must not be modifiable;
- must be retained for the entire retention period of the records audited;
- must be exportable by secure means and able to provide evidence when necessary;
- must be printable.

DATA IN MOTION

E-Mail
The use of e-mail in our society is commonplace. It is a convenient, inexpensive and quick means of communication. However, as a general rule, e-mail is not a secure means of communication, and may be vulnerable to interception and hacking by unauthorized third parties.

Accordingly, dentists should **avoid** using e-mail to communicate the personal health information of patients, unless they are employing a secure e-mail service with strong encryption.

The Information and Privacy Commissioner of Ontario (IPC) has advised that even if patients are willing to accept the risk of unauthorized disclosure of their personal health information in exchange for the convenience of communicating via e-mail, this does not alleviate health information custodians of their duty to take steps that are reasonable in the circumstances to safeguard personal health information in their custody and control.

There are several products and services that are available to permit dentists to communicate with each other and their patients via secure e-mail.

Laptop Computers and Other Portable Storage Devices
Once a patient record is available in electronic format, it can be easily transferred to a laptop computer or other portable storage device (e.g. USB flash drive, PDA, Smartphone) and transported outside of the workplace. Despite the convenience they offer, only the minimum necessary data should be stored on such devices.

Moreover, due to their potential for loss or theft, dentists must ensure that all patient records stored on these devices are either strongly encrypted or de-identified.

The term "strong encryption" does not refer to a particular technical or design specification, or a distinct encryption feature. Rather, a variety of circumstances and factors need to be considered in order to ensure that personal health information is adequately protected.

The Information and Privacy Commissioner of Ontario (IPC) has provided a working definition for strong encryption, as well as guidance on the minimum technical and functional requirements for a health care environment. For more detailed information, refer to Fact Sheet 16: Health-Care Requirement for Strong Encryption, which is available on the website of the IPC at www.ipc.on.ca.

Wireless Devices

Wireless devices broadcast information via radio waves, which radiate in all directions from the point of transmission. As a result, the signal may be intercepted by any receiver within range that is tuned to the same frequency.

For this reason, dentists must ensure that the personal health information of patients transmitted using wireless devices is either strongly encrypted or de-identified.

Teleworking

The use of teleworking (i.e. working remotely, such as from a home computer or wireless device, via external internet connection to the ERMS) in dentistry is increasing and offers many advantages. However, it also raises significant security and privacy concerns for dentists, due to the nature of the external connection to the ERMS.

The use of teleworking should be prohibited, unless a clear security policy is in place and the user agrees to abide by it. See the section on Security Policy for the Dental Office on page 12. Even so, it should be strictly limited to authorized users, and restrictions may be imposed on the connection duration and window (e.g. time-of-day, day-of-week). In addition, the use of teleworking must require minimum two-factor authentication and employ strong encryption.

BACK-UP AND CONTINGENCY PLANNING

All existing electronic patient records and critical data must be backed-up on a routine (i.e. daily) basis and stored in a physically secure environment off-site. Further, recovery procedures should be periodically tested to ensure that all patient records and critical data can be retrieved and reliably restored from the backup copy.

Appropriate measures should be taken to ensure the confidentiality, integrity and availability of all patient records and critical data during storage, such as by employing strong encryption.

Appropriate detection and prevention controls should be implemented to protect the ERMS against malicious software (e.g. viruses, worms, etc.). In addition, it is important to regularly check for and install updates for operational systems and software programs that protect the ERMS from known security risks.

In the event of a security incident, all staff should know the dental office's security management protocol to ensure that the necessary steps are taken to ensure a rapid, effective and orderly response to minimize any loss of confidentiality or data and system integrity.

The physical setup and environment of the ERMS should be evaluated to protect it from environmental threats and hazards, such as fires and floods, as well as power failures or surges and other electromagnetic disruptions.

In the event of a disaster or catastrophic failure of the ERMS, business continuity may be at significant risk. It is important to have a contingency plan in place to provide for business continuity, both from the perspective of the safe treatment of patients and the maintenance of required dental recordkeeping.

Copies of all ERMS software programs should be kept to facilitate recovery and consideration should be given to equipping a standby system. In addition, traditional paper records and dental radiographs should be available, in case they are needed for a period of time until the ERMS can be reliably restored.

DATA MIGRATION

As noted above, the ERMS must be capable of periodic upgrades to reflect the changing requirements of the dental office. There will come a time, however, when a decision is made to switch to a new ERMS, at which point the dentist must consider how to maintain the integrity of existing electronic patient records and critical data.

Options include migrating the patient records from the old ERMS to the new ERMS or archiving the patient records on the old ERMS.

Regardless of how the switch to a new ERMS is accomplished, the dentist must ensure that a secure means of access to all recorded information for each patient is maintained, and that the recorded information and related metadata is not compromised or otherwise changed in the process.

RETENTION AND DISPOSAL

The regulations governing the retention of patient records are the same, regardless of the form or medium in which they are kept. In general, all clinical, financial and drug records, and radiographic and consultant reports that are made in respect to an individual patient must be maintained for at least 10 years from the date of the last entry in that record. In the case of a minor, these records must be kept for at least 10 years after the day on which the patient reached the age of 18 years. This includes appointment records, lab prescriptions and invoices.

Once the retention period has been satisfied, the records for a patient may be disposed of in a manner that maintains confidentiality.

The disposal of electronic patient records must be authorized by the dentist.

Effective disposal of electronic patient records requires that they be permanently deleted or irreversibly erased, including any back-up or other copies (e.g. copies created by the ERMS for system purposes). An audit trail should maintain a record of the name of the patient whose personal health information was disposed, the time period to which the information relates, and the person responsible for authorizing the disposal of the information.

In the event that electronic media (e.g. hard drives and other storage devices found in computers, servers, photocopiers, fax machines, scanners, printers, etc.) are to be disposed, dentists must ensure that all patient records are permanently deleted or irreversibly erased from them. Alternatively, the device may be physically destroyed.

Dentists must not sell or give away electronic media device that have stored patient records.

Security Policy for the Dental Office

The dentist must assume responsibility for setting and enforcing a security policy for the dental office, dealing with the roles and responsibilities of staff and third-party contractors who are authorized to access the ERMS.

In order to ensure that the security policy for the dental office adequately addresses all necessary criteria, a logical and deliberate process should be followed. The first step is to conduct a comprehensive threat and risk assessment of the ERMS, and create an inventory of all assets. This should be repeated on an annual basis. The next step is to develop and maintain a written security policy for the dental office. It should address the following:

- the responsibility of all staff for the security and privacy of the personal health information of patients;
- education and training of all staff in security and privacy policies and procedures;
- the security roles and responsibilities of all users by job definition;
- the access control policies for the dental office, including the precautions to be taken when:
  - working in the dental office on the local network;
  - producing copies of electronic patient records (e.g. all electronic copies must be authorized and appropriately secured by employing strong encryption, and all printed copies must be labelled to disclose the confidential nature of their content);
  - removing copies of electronic patient records, equipment or software from the dental office;
  - using portable storage and wireless devices;
  - teleworking is permitted.

If services are provided by a third-party contractor, there should be a formal written agreement in place, which addresses the following:

- the responsibility for the security and privacy of the personal health information of patients;
- all repairs, changes and upgrades to the ERMS must be authorized and documented;
- all planned new information systems, upgrades and new versions must meet acceptance criteria;
- functional and security tests of the ERMS must be carried out prior to acceptance;
- all existing electronic patient records and critical data must be continually safeguarded during upgrades.

The terms and conditions of employment for all staff and third-party contractors should include a statement about their responsibility for the security and privacy of the personal health information of patients, which should survive the termination of employment or contract.

Privacy Requirements Under PHIPA

Regardless of the type of records that are used, health care providers have a duty to ensure that the personal health information of patients is protected at all times.

Ontario's Personal Health Information Protection Act (PHIPA) permits all health information custodians, including dentists, to collect, use and disclose personal health information for the purposes of providing health care, or facilitating the provision of health care, to patients. However, PHIPA also requires health information custodians to take steps that are reasonable in the circumstances to ensure that the personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure, and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

In particular, PHIPA requires health information custodians to:

- appoint a contact person, who is accountable for privacy matters;
- prepare and make available to the public a written statement setting out the custodian's information practices;
- ensure that their agents (i.e. employees and other persons acting on their behalf) only collect, use and disclose personal health information as permitted by the custodian and in accordance with the rules set out in PHIPA;
- ensure that personal health information is only collected, used and disclosed with the consent of the patient or as permitted by PHIPA;
- provide patients with the ability to access and request correction of their own personal health information.

If personal health information is lost, stolen or accessed by unauthorized persons, health information custodians must notify the affected patients at the first reasonable opportunity. In addition, health information custodians must ensure that records of personal health information in their custody or control are retained, transferred and disposed of in a secure manner.

The Information and Privacy Commissioner of Ontario (IPC) has issued an Order (HO-004), warning health information custodians about the risks of storing personal health information on portable media. The IPC stated that in the event a portable storage device was lost or stolen, it would not be regarded as a privacy breach if sufficient safeguards were in place to ensure that the personal health information was not disclosed, such as strong encryption.

The College has published a useful resource for members entitled "Compliance with Ontario's Personal Health Information Protection Act," which is available at www.rcdso.org.

For more detailed information, refer to the Personal Health Information Protection Act, 2004, and the regulations made under the Act, which is available on the website of the IPC at www.ipc.on.ca.

Additional Issues

As the use of electronic records and digital technology in health care is increasing, issues are emerging that raise new medico-legal questions, which are still to be addressed.

For example, software programs and devices have been developed that allow a person to electronically sign a document, such as a medical history questionnaire. The term "electronic signature" refers to electronic information that a person creates or adopts in order to sign a document, and that is attached to or associated with the document. One method involves the use of a special pen with a computer screen or touchpad, which captures a digital image of a handwritten signature. Other methods involve the use of letters, numbers or symbols that are attached to or associated with the document.

In order to be accepted as valid, dentists must be able to demonstrate that the person's electronic signature was unique, and that it was properly associated with the document in question via auditable means.

Another example is cloud computing, which allows a user internet-based access to a shared pool of computing resources, which are rented from a third-party provider for a fee. In this model, the user does not own or manage the underlying physical infrastructure, and has varying degrees of control over the operating systems, software applications and storage of data.

Cloud computing raises significant security and privacy questions for dentists, who are responsible for the custody and control of personal health information. Dentists considering a cloud service provider should perform due diligence, assess the risks involved, minimize the amount of personal health information exposed and provide for appropriate remedies.

A further example relates to internet-based products for patients that allow them to create their own health records. Patients may collect health information about themselves, maintain it online and grant access to their healthcare providers.

Dentists should be cautious about relying on information contained in a patient-created health record, and take appropriate steps to verify that it is accurate and complete.

Appendix

ADDITIONAL RESOURCES AND REFERENCE MATERIALS AVAILABLE ON THE INTERNET

Electronic Health Record (EHR) Privacy and Security Requirements, 2005
Canada Health Infoway
http://knowledge.infoway-inforoute.ca

Electronic Records Handbook: Implementing and Using Electronic Medical Records (EMRs) and Electronic Health Records (EHRs), 2009
Canadian Medical Protective Association
www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/pdf/com_electronic_records_handbook-e.pdf

Using Email Communication with Your Patients: Legal Risks, 2009
Canadian Medical Protective Association
www.cmpa-acpm.ca/cmpapd04/docs/resource_files/infosheets/2005/pdf/com_is0586-e.pdf

Transition to Electronic Medical Records (EMR), 2004
College of Physicians and Surgeons of Alberta
www.cpsa.ab.ca

Medical Records (Policy Statement #5-05), 2006
College of Physicians and Surgeons of Ontario
www.cpso.on.ca/uploadedFiles/policies/policies/policyitems/medical_records.pdf

Standards for Record Keeping, 2008
College of Occupational Therapists of Ontario
www.coto.org/pdf/COTO_Standards_RecordKeeping_2008.pdf

Notice: Classification of Medical Devices Class I or Class II Patient Management Software, 2010
Health Canada
www.hc-sc.gc.ca/dhp-mps/alt_formats/pdf/md-im/activit/announce-annonce/md_notice_software_im_avis_logicels-eng.pdf

Fact Sheet 1: Safeguarding Personal Health Information, 2005
Information & Privacy Commissioner of Ontario
www.ipc.on.ca/images/Resources/fact-01-e.pdf

Fact Sheet 10: Secure Destruction of Personal Information, 2005
Information & Privacy Commissioner of Ontario
www.ipc.on.ca/images/Resources/fact-10-e.pdf

Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices, 2007
Information & Privacy Commissioner of Ontario
www.ipc.on.ca/images/Resources/up-fact_12e.pdf

Fact Sheet 14: Wireless Communication Technologies: Safeguarding Privacy & Security, 2007
Information & Privacy Commissioner of Ontario
www.ipc.on.ca/images/Resources/up-1fact_14_e.pdf

Fact Sheet 16: Health-Care Requirement for Strong Encryption, 2010
Information & Privacy Commissioner of Ontario
www.ipc.on.ca/images/Resources/fact-16-e.pdf

Get Rid of It Securely to Keep It Private – Best Practices for the Secure Destruction of Personal Health Information, 2009
Information and Privacy Commissioner of Canada
www.ipc.on.ca/images/Resources/neid.pdf

Personal Health Information: A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records, 2009
Information & Privacy Commissioner of Ontario
www.ipc.on.ca/images/Resources/phipa-toolforphysicians.pdf

Information and Documentation – Records Management, Part 1: General (ISO 15489-1), 2001
International Organization for Standardization
www.iso.org

Information and Documentation – Records Management, Part 2: Guidelines (ISO 15489-2), 2001
International Organization for Standardization
www.iso.org

An Introduction to Computer Security: The NIST Handbook, 1995
National Institute Of Standards and Technology
www.csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Guide to Using a Computer System for Keeping Patient Records, 2006
Ordre des dentistes du Québec
www.ordredesdentistesduquebec.qc.ca/publications/images/pdf/GuideInformatique_en.pdf

Royal College of
Dental Surgeons of Ontario

Ensuring Continued Trust

6 Crescent Road
Toronto, ON Canada M4W 1T1
T: 416.961.6555 F: 416.961.5814
Toll-free: 800.565.4591 www.rcdso.org

01/12_3100