The Confidentiality and Security of Computer Based Dental Records.

William R. Hiltz BSc MBA CET william@prosperident.com

Introduction

The computer based oral health record is one of the most significant events to happen in dentistry since the introduction of the computer. Computer based systems are increasing in popularity in North America and it is expected the majority of dental offices will be using them in the near future. While the dental profession seeks accountability in health care, society expects – both implicitly and explicitly – the profession to maintain high ethical standards. The foundation of the dentist – patient trust relationship is based on informed consent and confidentiality. Traditionally, dentists have used paper-based systems to record patient information and the release of information to second and third parties are defined by professional and legal boundaries. While computer-based patient records have distinct advantages over paper-based records, they often are subjected to a higher level of scrutiny than the conventional paper based record. The computer based patient record introduces concerns regarding the confidentiality and security of patient information. The Canadian Government has passed Bill C-6 that addresses the rights of privacy for personal information. The Bill regulates commercial activity associated with the collection, use, disclosure, retention and disposal of personal information. Readers may know this piece of legislation as PIPEDA.

Confidentiality is one of the hallmarks of the dental profession and security of computer based record systems is essential. These issues must be carefully planned to meet the dental professions own standards and also to consider the new privacy regulations. Security standards for computer based patient records have been developed, but they are slow to take root with the developers. Nevertheless, computer based patient record systems are available however they rarely exist as a single application. Instead, they are usually formed from a suite of applications, which increases the need for quality assurance when implementing these systems in the dental practice.
Computers in Dentistry

The Computer-based Oral Health Record

The electronic dental record and the Computer-based Oral Health Record (COHR) are terms that often are interchanged to describe the same thing. The COHR classification is becoming widely used and it represents one of the most significant developments in applying computer technology to dentistry.

The lowest level, or basic form of COHRs contain all the information that is now stored in hardcopy records. Since this information can include text, numbers, drawings, images, objects and video, it is stored and represented on the computer in a multi-media format.

Computer-based patient records have distinct advantages over paper-based records. Paper-based patient records are typically fragmented, passive, and rarely longitudinal and cumulative. COHRs can store all the information in one place and still allow multiple accesses by patients, dentists, hygienists and office personnel. Paper based records cannot easily be reorganized or distributed to multiple providers concurrently. Information in the COHR can easily be reorganized. Diagnostic information retrieval, such as specific radiographs taken of an individual during a precise time period, is faster than the paper-based process. Since COHRs are not fragmented like paper-based patient records, they are able to provide a single source for dental care data; however this assumes that standards are in place for secure data transfer between providers. Finally, COHRs enable dental professionals to track the oral health of single individuals, practice populations, and the public in ways that the paper record cannot.

Properly implemented, the computer-based patient record can avoid many of the drawbacks associated with paper-based records. Paper based records often lack quality controls and they are almost never replicated for archival back up. The paper-based record is susceptible to physical loss, fire, tampering and falsification. Therefore the implementation of the COHR must not only focus on delivering an enhanced system to manage information, but also provide mechanisms to counter loss, fire, tampering, falsification and protect patient confidentiality. This is best accomplished when dentists,
suppliers, consultants and office staff all enforce robust quality assurance and security procedures.

The typical COHR is subdivided into broad categories or functional modules. The following modules are considered to form the basic components of a COHR:

1. Patient registration
2. Medical/dental history
3. Treatment planning
4. Patient provider encounter
5. Patient care assessment
6. Management modules
7. Appointment scheduling
8. Consultation and referral management
9. Financial management
10. Charting
11. Imaging

While the logical structure of computer-based patient record imitates the hierarchical structure of a conventional paper records, the functionality of COHRs is still not very well defined. Different vendors sell products that form only a part of the COHR. For example, one company may provide digital radiography modules, while another provides clinical charting and a third provides financial management systems.

**Standards and Guidelines**

Computer based patient record systems are not new to the healthcare industry. The installation of these systems within hospitals and more recently, the shift towards large healthcare information networks, has created a need for authentication guidelines. These standards exist to ensure reliability, confidentiality, and security of this information.

It was not until 1992 that there was interest in standardizing dental information systems. Since that time, various proposals and frameworks have been developed for the implementation of COHRs; however these have not been widely adopted by vendors and integration of the various components remains a non-transparent process.

This lack of transparency, or inability to integrate some products, is steadily declining and the not too distant future looks very promising. The industry is becoming standardized; however problems still exist in view of the size and scope of the COHR. Taken as a whole, it is not uncommon for the components of the ‘paperless dental office’
to come from as many as 12 hardware and 20 software suppliers.* In some areas, the suppliers are intrinsically motivated to provide compliance products, (digital radiography) while in other areas, the suppliers are extrinsically motivated to maintain proprietary technology (financial management, charting). In some areas the technology is mature (financial management) while in other areas the technology is emergent (digital radiography).

The changes that are occurring within the industry lag behind the publication of new and revised standards. The scope of dental informatics is expanding. This is evidenced by no less than three journals dedicated to the topic of how computers enhance dental research, care and education. (1) In the United States, several universities have added dental informatics graduate programs to their curriculum. The author is unaware of any university in Canada offering this program.

At present, it appears the U.S. that is shaping, defining and advancing COHR standards. The U.S. leads the way through cooperative efforts between the American Dental Association (ADA) and other dental academies and organizations to identify and standardize nomenclature. The ADA, through the ANSI Accredited Standards Committee MD156, have created five working groups which promote the concept of the COHR and focus on the technical issues related to standardization of different hardware and software components. Within each working group, subcommittees are responsible for specific projects. For example, one of the subcommittees of Working Group 4 is working on the development of a common data model for oral health care. (2) (Also see Appendix A)

Working Group 2 is working on the development of DICOM supplements for digital imaging and communications. DICOM stands for Digital Imaging and Communications in Medicine. In 1985, the American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA) published a standard that addressed the issue of

* By the authors count, based on a complete system containing hardware and software required for: network operating system, financial management, image retrieval and management (x-ray and photo), patient education, communications, charting and clinical notes.
vendor-independent data formats and data transfers for digital medical images. ACR and NEMA have recently completed the third version of the standard, which has been renamed DICOM V3.0. The V3.0 refers to the fact that there were two prior versions of the standard.

**Current State of Affairs**

While the ADA continues to promote the development of standards, the industry continues to lag in adopting them. For many suppliers of dental software, the standardization process can be expensive and create delays in product release. The costs of this delay are measured against their competition. In the high technology marketplace, a company’s survival may depend on a ‘first mover advantage’. This means, those developers who get their product to the market first, will gain a greater market share and increase the probability of future success. The expense of rigorous compliance testing coupled with pressure to provide an early release of software, often result in non-compliant, non-transparent and proprietary product releases. Nevertheless, even with a first mover advantage, these companies are marketing to a profession that is characteristically a late adopter of computer technology. There appears to be a ‘wait and see’ attitude on both sides. The dental profession is aware that the COHR is available, yet is reluctant to move *en masse* to this new technology. The industry, in order to maintain product recognition by the profession, appears to be concentrating on market presence today in order to realize greater product sales tomorrow. Therefore, COHR product enhancement and compliance trickles in at a rate equal to the amount of sales, which at present is low, compared to the market potential.

Recall that the COHR consists of various sub-systems or modules, which together, are capable of forming a system that can create a paperless dental office. It is important to note that already, some components of the COHR are widely used within the profession. In Canada, over 76% of dental offices have computer systems (CDA.net, 1998) and within these offices only limited numbers use COHRs. For example, a recent survey published in *Dental Products Report* (August/99) shows that only 4% of dental offices in the U.S. use computerized charting systems.
In contrast to the high use of practice management systems, the complete COHR system is largely unaccepted. Many of the early systems were unsuccessful and lowered confidence in the technology. This has shifted many dentists into complacency with their present paper systems. There exists a general lack of enthusiasm to purchase COHRs until the technology fully matures.

The explanation for the high use of computers, but low use of a complete COHR system can be explained by examining the nature of the profession. Dentistry has always had a commercial component and since the introduction of the personal computer, it has required software to handle the complexities of patient account management. Thus, the most common use for a computer system in the dental practice is for account management and insurance claim processing. Dentists first introduced computer systems into their practices to manage these day-to-day activities. This is why computer systems in dentistry are most often called ‘practice management systems’. Many of the early computer systems in dental practice were simple billing packages adapted from medical practices and modified to perform billing and insurance processing in a dental setting. Today, most practice management systems are sophisticated and have gained wide acceptance by the dental profession. This accounts for the high rate of utilization of these systems in the dental office. Practice management systems have been around for nearly two decades and these are mature products as compared to other COHR modules, such as charting and imaging. Another reason why practice management systems prevail and why the COHR has only a 4% market share is because the majority of dentists practice in isolation or small groups. The need to share information outside the practice is almost non-existent; therefore when they select a practice management system, proprietary technology is not a major constraint.

Practice management systems can be quite sophisticated and often exceed the clinics expectations as they relate to billing, insurance claim processing and appointment scheduling. The practice management system then forms the complete base of computer technology in most clinics. Therefore, when dentists consider adding other modules (like digital radiography and charting) they call for these systems to be compatible with their
existing financial system. This is often where worlds collide. Practice management software vendors often form unlikely alliances with other suppliers. It is not uncommon to have four separate software applications (financial, charting, imaging and digital radiography) working concurrently or consecutively. The non-financial modules are often integrated into the practice management software by its developer. This integration process is often not seamless because of database incompatibilities between the different software applications. Moreover, these companies often hesitate to share the technical details of their software with each other to the extent where an effective interface is possible.

Given that complete and seamless integration is difficult, many dentists still use traditional paper charts and film-based radiography systems. Paper based clinical charts are easy to use and present lower initial capital outlays as compared to computer based systems. In contrast, computer systems that are designed to replace traditional paper charts and film-based radiography require a substantial upfront investment.

The trend to computerizing patient records is advancing and in spite of the professions characteristic late adoption, these systems will prevail over the coming years. With extended capabilities far beyond simple financial management, the COHR requires additional and prudent security to address the confidentiality and legal concerns over the management of this information.

Confidentiality and Security of Patient Records

Confidentiality and Privacy

Security, privacy, and confidentiality are all interrelated. Privacy here is understood as the right of an individual to control disclosure of his or her medical-dental information. Confidentiality is the understanding that this information will only be disclosed to authorized users and security is the underlying principles that limits disclosure. Privacy and confidentiality cannot be assured without security measures.
The issue of confidentiality and privacy is of paramount importance in society. In our contemporary information age, the issue takes on a new perspective given the ease at which information can be accessed. These issues surrounding confidentiality and privacy will require that dentists adhere to stringent rules in order to protect the patient’s information. Government policy focuses on the protection of society and the individual while the dental profession focuses on protection of the patient. In Canada, these two agencies are at odds in their policies and presently are debating this at the national level.

**National Protection of Personal Privacy in Canada**

Canada has legislation to protect personal information that is collected and used by the federal and provincial governments (except PEI) and Quebec is the only province to date that has introduced privacy legislation to the private sector.

The proposed Federal Bill C-6 is a right of privacy for personal information that is collected, used and disclosed in the private sector. It received a First Reading in the Senate on November 2, 1999. (3)

“The Bill defines personal information as "information about an identifiable individual", and includes things such as their race, ethnic origin, colour, age, marital status, religion, education, medical, dental, criminal, employment or financial history, address and telephone number, numerical identifiers such as the Social Insurance Number, fingerprints, blood type, tissue or biological samples, and their views or personal opinions.” (4)

Protection of this information is accomplished by requiring organizations to comply with the obligations in the Canadian Standards Association's (CSA) Model Privacy Code. (See Appendix B)

The Bill will eventually apply to every organization that collects, uses or discloses personal information in the course of commercial activity. Without amendments, CSA Model Privacy Code will apply to the dentists and regulate, in part, the accountability of
the profession. It will also set policy as to how individuals are identified, how consent policy and collection of information is to be performed. It will limit the use of information, the disclosure & retention of information and provide guidelines for accuracy, safeguards, openness, and individual access. From a legal perspective, this also opens the door for challenging compliance.

**Professional Association Protection of Patient Privacy in Canada**

However, Bill C-6 has not yet passed and the Canadian Dental Association is on record as opposing the “consent provisions” of the CSA Model Privacy Code as they relate to personal health data. The CDA feels this conflicts with their professional association policy on privacy. As such, the Canadian Dental Association (CDA) has been actively lobbying Senators to amend Bill C-6. “Our position is in direct contrast to a ‘health carve out’ position. We are arguing for stronger protection of health records.” (5)

Bill C-6 may accomplish various government priorities in the area of electronic commerce, but the CDA believes that the Bill must be clearly defined as it relates to personal health data. This cannot be overstated since, in almost all circumstances, a dentist will acquire an extensive health history for each patient before the commencement of dental treatment. The information captured is may be sensitive and it is communicated to the dentist under an implied agreement. In addition, dentists have an ethical responsibility of confidentiality. The foundation on which the Canadian dental profession privacy statement rests upon is based on the Supreme Court of Canada’s ruling which recognizes the patient as the final authority over the control of his or her own health record. (6)

Given that this contentious issue is presently unresolved, dentists should develop a policy that meets their professional association’s goals. At the moment, the goals of Bill C6 appear subordinate to the CDA principles.
Types of Confidential Data

As previously mentioned, the COHR consists of multiple modules or applications and within each subset of the COHR; different data is stored and classified. Dental offices routinely collect sensitive medical information such as disease state (physiological and psychological), age, marital status, medical, dental, employment and financial history. While we can say a person with a sexually transmitted disease deserves privacy, we may also say that every piece of information about a patient is confidential. However, non-patient specific information is not considered to be confidential in this context. For example: the names or addresses of insurance carriers, local fee guides, and treatment codes.

Data Security

Security is a means to help ensure confidentiality and privacy of information. This suggests that when we speak about threats to confidentiality and privacy, we are really referring to the weaknesses in our present security system and practices.

In the conventional sense, a threat to confidentiality arises when a trusted individual, like a dentist or staff member, releases information to another party without the consent of the patient. Threats to confidentiality then arise from ethical issues, which govern the trusted individuals, or security issues that control a trusted component of the computer system.

Trusted Computing

The foundation of any COHR system should be a ‘trusted computing base.’ This is the set of all hardware, software and procedures that implement security. Therefore, in order to breach security, an intruder must threaten one or more of the above.

In trusted computing, the term ‘trust’ has a unique meaning. In our everyday conversation, it implies that we rely on a person to do, or not to do, a particular thing. For example, when a patient when discloses confidential information with a provider, they expect (trust) that this information will not be shared with other parties without their consent. In this example, the provider is the trust component. Failure of the provider to
maintain trust creates a threat to confidentiality. It is the trusted component where confidentiality can be broken. In trusted computing, the same tenet holds true. It is the trusted component that can be threatened. It is the one that can break security. Therefore, a trusted component is one that requires robust security to ensure and maintain trust. Release of information from the trusted component must be controlled within the dental office and communications outside the office.

Presently, with so few offices using a complete COHR system, much of the disclosure to third parties arises from submission of insurance claims to carriers. The patient has a right to expect the exchange of this information is trusted. All major carriers in Canada require signed disclosure agreements between the patient, the dentist and the insurance carrier before any information is exchanged; however third party individuals do represent an external trust component. While dentists and other licensed oral health care providers are bound by professional codes of ethics, others are not. Outside of the dental profession, improper release of information can and does happen. Approximately forty percent of insurers disclose personal health information to lenders, employers or marketers without customer permission (7). The proposed Bill C-6, when passed, will legislate changes to prevent these types of occurrences.

The trusted computing base of a clinical information system should include computer security mechanisms which enforce user authentication and access control, communications security mechanisms to restrict access to information in transit across a network, and backup procedures to ensure that records are not destroyed by fire, theft or systems failure.

Most dentists do not have the technical background to ensure that trust computing is properly implemented in their office. Usually, an independent professional does the evaluation of trusted computing components. In Canada, independent evaluations are
done by large hospitals and government agencies, but these are oriented towards military systems and evaluations under them will be expensive†. (8)

**Trusted Computing in the Dental Office**

Providers should not immediately assume that a network (LAN, intranet or Internet) could be trusted, unless it is under their direct control. Wide area networks such as the Internet may not be trustworthy. The most important factor in getting security that works is not the choice of mechanisms but rather, the care taken to ensure that they work well together. For example, procedural mechanisms such as password administration are an excellent starting point. Configuration management and backup are an integral part as well. When assessing a system the dentists must ask whether a provider whose computer skills and administrative efficiency are less than average can operate it securely. Yes, blasé and careless providers do exist. If it is more convenient for them to run the system insecurely, they will.

A trusted system should also maintain integrity of information, for example, human data entry errors can create incorrect information. Dentists should also take into account human design issues such as the use of integrity checks‡ on manual data entry. Minimizing human error cannot solely be accomplished by integrity checks within the computer application. The quality of user manuals and training is important to help reduce the ‘garbage in-garbage out’ phenomenon. When a system is being installed the dentist must ensure that all relevant training has been completed and any necessary plans, procedures and materials are in place. These must include a disaster recovery plan in the event of a system failure.

Before a patient begins their relationship with the practice, they should be given information on the clinics’ access control policies. Patients are then given an opportunity to object and conceivably they could request their record be restricted to one or more

---

† In 1997, the Atlantic Region Health, part of the Department of National Defense’s healthcare strategy, used independent trust evaluation for the submission of electronic medical and dental information to a third party claims adjudicator. The process, based on EnTrust technology was expensive. While a high level of trust was achieved, this illustrates an example far outside the resources of the individual dental practitioner.

‡ Program integrity is the assurance that the electronic record is identical to the source document.
named providers. For this reason, password-based systems must support restricted access control lists which, in this case, would be a list containing a single clinician. Information brochures for patients and consent forms should be drawn up and tested before any patient information is entered into the system. Exposing information and consent in this way will help limit the residual risk.

Only when these steps towards a trusted computing environment have been completed, should the system be furnished with final components to enable communication with other systems.

**Practice Management Systems**

The most commonly used application is a practice management system. While this forms only one component of the COHR, its pervasiveness in the dental office is so great that these systems are rapidly adapting as the hub for a suite of software required to maintain a COHR system. Therefore, it is important that dentists first address security and confidentiality with the practice management system before integrating additional components into their offices. The security issues discussed below are applicable to all components of the COHR system; however it should be noted that clinical, charting and imaging modules require additional security measures.
As previously mentioned, practice management software is available from a mature product stream and each vendor offers a different approach to “built-in” security. This means that each system has unique security capabilities. The following section describes a form of security policy or principles, which may be applied to dental computing. These suggestions are simply a restatement of the commonsense language of computer security.

Limit Access to Information

In a computer system, each user has access to certain “objects”. This access information may be stored by user or by object. In the user case, the access permissions are called privileges, and might have the form ‘Dr Downing may read the records of John Doe and Jim White’. If the permissions are stored by objects, they are called access control lists, and might have the form ‘This is John Doe’s record and it can be read by Dr. Downing and Dr Smith’. The latter approach leads to simpler engineering, as the number of patients per doctor is much larger than the number of doctors per patient.
Each identifiable patient record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system should prevent anyone not on the access control list from accessing the record in any way. In many current systems, access control lists are commonplace. If a record is present on the practice database, then specific doctors in that practice may read it and append information to it. However, with the introduction of networking, access control lists need to be made explicit. They must be consistent across a range of systems, and must be enforced by mechanisms that are technically effective.

To facilitate this, groups may be used instead of individual names. For example, if Dr. Downing, Dr. Smith and Jean Jones together form the staff of the Downing practice, then the records to which they all have access might simply be marked `Downing'.

**Attribution and Audit Logs**

It is desirable to record all file and record accesses (whether reads, appends or deletions) using attributes. All accesses to clinical records should be marked on the record, with the users name, as well as the date and time. An audit trail must also be kept of all deletions. Systems developed using accreditation and audit logs will typically record all write accesses and even if material is removed from the main record, there remains an audit trail which can help reconstruct the record as it was at any point in time. Changes to a patients record should be write and append-only access and these operations should be tracked by the users name. These requirements help to ensure that breaches of confidence can be traced and punished. In addition, deletions should be logged so that the intentional destruction of material can be recognized.

Whenever groups are used, a record must always be kept of which individuals read a record or add anything to it. This takes the form of an audit log, which cannot be created, written to nor deleted by users. The audit log contains all the necessary information to determine who had access to the record, what changes were made, what was printed to hardcopy and unauthorized access attempts. There are a select few practice management systems in Canada that have this type of robust security built into the application. Many
of these systems rely solely on the networking software to control user access. This will prevent unauthorized use of the system but falls short of creating a reconstruction of events when a challenge arises. Challenges may be a suspicion of fraud or embezzlement by staff members or a legal challenge by a patient or other provider. Since an efficient audit log can track all changes by groups and users, the clinic’s risk is minimized.

The process by which an audit log can track user access to records and the changes that are made is called: attribution. Because attribution tracks users based on group access and password controls, it is not acceptable for a group to be implemented by a password shared by all the staff, or leaving a terminal permanently logged on to an administrator account. Such actions mean abuses could not be attributed to an individual.

Monitor and Control Outside Requests for Access to Information

Apart from the patient himself, only clinicians should have access to personal information. The reasons for placing the trust at the professional boundary are traditional and practical. The recent appeals by the CDA regarding Bill C-6 show that dentists do not consider the mechanisms of the civil and criminal law to give adequate protection. If a dentist gave a record to an insurance carrier or social worker who then passed it along to another party without consent, or kept it in an insecure place, then the dentist may still be liable and have no recourse.

Therefore, only clinicians (dentists, hygienists and other healthcare members) are trusted to enforce the principle of informed consent and the control of clinical records lies with the individual clinician who is responsible. Since more than one provider usually practices in a clinic, one of the providers in the access control list must be marked as being responsible. Only they may alter the access control list, and add other health care professionals to it.

When information is sought by a lawful third, such as a social worker, a lawyer, police, insurance company or employer, then the information must be provided on paper – not by electronic exchange or on computer disk.
Dentists should be aware that computer records might not be usable as evidence unless they come with a justification - on paper - that during the normal day-to-day activity of the dental office, proper security and authentication procedures are enforced. A signed statement on paper will best satisfy a legitimate requirement for evidence.

Cipher and Limit Information on the Screen

The use of discrete ‘flags’ that indicate the presence of hidden information is desirable. For example, patient medic alerts, financial status and other sensitive information can be displayed as an icon or short mnemonic. These flags can alert the provider to important information without it being displayed on the computer screen in a generic, readily understood, format.

Computer screens remain a curiosity with patients. Keep them turned away. If possible, choose a narrow viewing angle screen (e.g.: flat panel LCD) to keep on-screen information less evident. Clinics that choose to have workstations in the operatory must use discretion when working with them. Workstations in the operatory are valuable as patient education tools. They can be used to support treatment by visually displaying treatment options using charts, digital radiographs and images, however the focus should be on the proposed treatment. Administrative functions, treatment fees and the records of other patients must not viewable by the patient. Discretion can be achieved by using a swivel monitor that can be turned away from the patient’s line of sight, or by using a switching device that allows for remote on/off control of the display screen.

Persistence of Information

There are rules on how long records must be kept. In Nova Scotia, the Provincial Dental Board recommends patient records be maintained for ten years. Thus, no one should be able to delete clinical information until the appropriate time period has expired.

However, preserving records is not entirely straightforward. In some cases, it is desirable to allow deletion of information that has been identified as incorrect, such as simple data entry errors and their subsequent revised entries. Yet, a system should not allow the
traceless deletion of mistakes, as this would destroy the record's value as evidence in a legal challenge. Accordingly, information should be updated by appending rather than by deleting, and the most recent changes brought first to the provider’s attention. Deletion should be reserved for records that are time expired.

**Graphical and Imaging Systems in the Dental Office**

**Clinical Charting**

Clinic charting is a direct replacement for paper-based charts. Charting modules use a graphical interface that mimic a conventional paper chart. This module of the COHR is an area where only providers should have permission to enter and modify information. Electronic charting systems contain providers’ notes, patient medical information, treatment plans, past treatment history and other sensitive information. While a division exists between the practice management modules of the COHR, certain parts of the charting database are used in the practice management system. For example: while in the operatory, a provider will enter treatment into the charting module, this information is then relayed to the front desk for insurance and patient account processing.

While the front desk staff does not require a patient’s chart to perform billing and insurance claim processing, most front desk workstations can access this information. Dentists must ensure that adequate security is enforced. The front desk is a busy place and patient charts should only be retrieved and displayed on an ‘as-needed’ basis. Unfortunately, the practice management module and charting module often do not share the same database and patient charts have often become repositories for non-clinical information related to insurance plans. As a result, the patient chart is accessed from the front desk to review these notes and in the process, exposing the chart on the computer screen. When considering a charting module, the same types of security control are required as with the practice management system with the proviso that non-clinical information must not be part of the patient’s electronic chart. This information should be

---

5 This occurs when “Vendor A” supplies a Practice Management System and “Vendor B” supplies a Charting System. In both systems you will find areas to store patient notes and comments. Since these systems come from different suppliers, these fields represent two separate databases to store the same information.
stored in the practice management system and charting should be accessible only by the clinicians working in the treatment rooms.

Many charting systems integrate with intra-oral cameras (photos) and digital radiography (x-rays) and display these images directly on the computer screen with the patient’s chart. These systems work by capturing images and then storing them on a hard drive. These images are different in format than typical database files and attribution is difficult to achieve. Unlike a database where each field can have integrity checks and access control, an image can be accessed and altered without leaving any evidence or an audit trail. As previously mentioned in the Standards section, the new DICOM V3.0 standard has been released. The medical profession is adopting this standard for digital images; however the adoption of DICOM by suppliers of dental digital imaging equipment has not happened. DICOM has robust methods to authenticate, control access and detect alterations of medical images. Since, in a dental practice, these images form part of the COHR, some discussion is dedicated to the security issues related to digital radiography.

(intentionally left blank)
Figure 2: A screenshot of a typical charting image application. Patient dental charts (restorative and periodontal) can be displayed. (Courtesy T-DOCS)

Digital Radiography

Digital radiography is a direct replacement of conventional film based radiography with an electronic image gathered from a sensor connected to the computer. Images are entered into the computer using three common methods. (i) direct radiography, (ii) indirect radiography or (iii) computed radiography. Regardless of which method is used, the result is a grey-scaled pixel-by-pixel image. These are typically stored as JPEG files. Since these images are stored using popular graphic formats, they are able to be manipulated using personal computer software. This increases the potential for fraud resulting from falsification of insurance claims. A recent study determined that electronically altered dental radiographs, depicting patients requiring expensive treatment, such as root-canal therapy and full-coverage crowns, could be submitted to an insurance carrier for approval. (9)
A separate study determined that digital images stored on the hard drive of a computer dental radiography system could be exported, altered, and subsequently restored to the system without any visible signs of alteration. (10) This study demonstrated the ease that was accomplished using commercial software and limited technical ability. Computed radiographic images are also susceptible to alterations. (11)

![Figure 3: Screenshot of a typical digital radiograph image. Current software enables dentists to manipulate these images, which may improve clinical decisions. Courtesy Xamine-It](image)

This ability to manipulate digital radiographic images illustrates the potential legal problems of image manipulation and calls for manufacturers of digital radiography equipment to be pressed towards exploring methods of preventing such abuse. Dentistry should also be aware of the implications potential abuse and should develop measures both to prevent it from occurring and to facilitate its detection. The author is unaware of any dental digital radiography supplier that is currently offered DICOM compliance however, several manufacturers are promising DICOM compliant products sometime in 2000.
Setting Office Policies

Security Policy Manual

It is generally agreed that the security of the COHR must meet or exceed the standards presently applied to paper records, yet an absence of clarity on the proper goals of protection has led to confusion.

While systems security policies lay out the details of who may access the information in and at what level. The main threat to the confidentiality of clinical records is carelessness. Following some common-sense rules that practices have been using for years can reduce this threat. (See Appendix C)

Controlling access to information includes restrictions on reading, writing, appending, and deleting data. A threat model often drives security policies and the details of your policy should reflect the nature of the threat. For a security policy to meet the needs of a particular setting, it must be written in the proper context. It should not burden the reader with unnecessary technical details and focus on the important problems while ignoring distractions.

Every dental office, regardless of the level of computerization, should have a written security policy in force. This policy will protect those patients whose records are on file in the computer system, but also deal with the issue of a patient who does not want their record kept on a computer system at all. Dentists cannot discriminate against a patient who demands that their record be kept on paper instead. This may sound illogical, but there are reasons for it. The patient’s fears may well be justified if they are a celebrity, or a target for assassination. These events are rare but should not be unanticipated.

In addition to the security of dental information, an emphasis must be placed towards its integrity and availability is required. For example, if information is corrupted, providers may make inaccurate diagnosis, which may harm the patient. If information is unreliable, then its value as a basis for clinical decisions is diminished. There is also the legal
concern that oral healthcare professionals, called to justify their actions, may be unable to rely on computer records as evidence. As previously mentioned, setting your security policy on paper is a required step. Your policy should focus in internal security first, then external. Recall that most errors and breaches of security occur by insiders. A study by the US government's Office of Technology and Assessment confirmed that the main threats to privacy in computerized clinical record systems come from insiders rather than outsiders, and that they are increased when these systems are networked to outside sources. (12)

Other Security Threats: Equipment Failure, Theft, Loss or Damage.

A serious security threat to the continued availability of computerized patient information is theft of the computer. At a minimum, the main server should be bolted to the floor or desk, preferably within a locked office. Data can also be ruined in by fire, flood, equipment failure, and computer viruses. Along with physical security, measures to control the risk of computer virus infection are essential. Current virus detection software is not an option.**

However, even if theft or viral infections never happen, the risk of equipment failure still requires that the dental office have a tested disaster recovery plan. Regrettably, most clinics do not perform a realistic test of their procedures until it is too late. When a real disaster strikes, recovery is usually held up for lack of manuals, suppliers' phone numbers and other things. Given that this is an unforeseen, yet very critical threat, it is advisable to have an annual test based on a realistic scenario, such as the complete destruction of a computer by fire or theft. This should contain a ways and means to perform a full system recovery on another machine from offsite backups.

The importance of data backups cannot be overstated. It is essential to keep several generations of backup sets onsite and at least one set offsite. Some viruses can cause a complete data loss but it may take some time to notice that thing have gone wrong. A typical schedule should maintain daily, weekly and monthly backups.

** Popular virus detection software is available from Symantec Inc (Norton AntiVirus) and McAfee VirusScan.
A computer security plan must also consider the possibility that viruses may appear innocuous and their only effect is to make alterations to records. This is harder to detect and may only be realized weeks after an infection. The risk of internal viral infections will increase as user privileges - such as writing to the disk - are increased. The risk of external virus infections will increase when allowing connections to outside networks, like the Internet.

Storage Requirements for System Backups

When performing backups, it is wise to consider the amount of storage (measured in megabytes) that will be required. For a simple practice management system, the backup requirements may be only a few 1.44 Mb floppy disks (at the low end) and a single 250 Mb ZIP disk (at the high end). However, using floppy or ZIP disks will fall short when archiving digital radiography and imaging systems. These files are stored as images and impose great demands on the backup system. Tape backup devices capable of storage in multiple gigabytes are required. The benefit of using a tape backup is that they can be erased and used multiple times. This allows an alternating backup schedule using a series of tapes, which are cycled through the schedule. While tapes offer the convenience of multiple backups and erasures, this design feature has an inherent security threat. Tapes are magnetically sensitive and can be erased in the presence of a magnetic field. This may occur intentionally or unintentionally with the end result being the destruction or alteration of data.

From a security perspective, a preferred backup method is to use a write-once, read-many CDROM. These devices can backup 650 megabytes of data on a single disk. A major advantage to write-once technology is that, unlike magnetic tape backup, write once CDROMs cannot be erased. If a CDROM backup were performed automatically each week, the clinic would have an unalterable trail of sequential backups. The cost of this technology has dropped dramatically in recent years and it is certainly within the limits of most dental office budgets. The disadvantage of write-once CDROM
technology is its limited capacity. A CDROM can hold 650mb of data and in a dental office that uses a complete COHR system, the amount of data will eventually outgrow the capacity of the CDROM. In this instance, streaming tape drives with 10 or more gigabytes of storage space are required. Interestingly, recent developments in DVD technology promise multiple gigabytes of storage on a single DVD disk. When this technology is available, it should provide a more secure alternative to tape backups. It should be noted however that both CDROM and DVD technology are not replacements for tape backup units. They are meant to be adjuncts that can provide non-erasable, time stamped archives of clinical information.

Compression algorithm software is often used in backup and archival storage of information however these algorithms should not be used for digital radiographs. Depending on the type of compression used, reduction in image file size can result in a loss of detail (lossy compression) and this is unacceptable for diagnostic images. However, photographs of patients (either intra or extra-oral) are not subject to the same diagnostic criteria and these images can often be compressed without severe image degradation.

**Assigning Protection Priorities**

A common theme that is delivered by the media concerning computer security is to focus on the sensational and ignore the fact that these are low probability threats. For example, consider the huge amount of publicity given to the occasional hacking attacks on the Internet. While there can be no doubt that a capable hacker can manipulate Internet traffic in various ways and may succeed in logging on to a system by password sniffing and address snooping techniques, one must always consider the low incidence of these attacks. Furthermore, most - if not all - Internet service providers provide firewalls to make intrusion very difficult. Capable and motivated adversaries will usually find cheaper and more reliable means to breach your computer security. Most often, this is physical removal of the computer system by breaking and entering.

---

*†† A file size of a digital radiograph image (periapical or bitewing) is approximately 182kb. If a dentist takes the equivalent of*
Therefore, it is essential to draw a distinction between vulnerabilities and threats. Vulnerability is a weakness in your security plan. A threat is countered by security. Therefore, as security decreases, vulnerability increases and the threats ability to cause a security breach will increase.

**Summary**

We have described the threats to the confidentiality, integrity and availability of patient dental records. We have also proposed various security measures which can help to form a foundation on which the confidentiality of a computer based record can exist.

The security of a COHR system should be such that a dental provider, with limited computer skills, can maintain patient confidentiality. The continuing and rapid evolution of technology, coupled with the benefits it brings, raise concerns that privacy is being overlooked. It is not so much the application of technology that causes the most concern but the fact that privacy may simply be overlooked as we become overwhelmed by technology. In addition, privacy protection is often not an integral part of many existing COHR systems but is added later and perhaps not as effective. However, the industry is responding by creating stronger vendor alliances and single source providers of COHR systems. These new systems remain unproven since there are so few installations and to the author’s knowledge, not one COHR system in Canada has faced a legal challenge regarding computer based oral health records. Interestingly, the dental profession subjects the computer based dental records to a much higher security standard than the traditional paper chart even though a well planned computer system can provide a much higher level of security than paper based systems.

In general, as a society, we trust computers. We have become dependant on computer systems to conduct our financial transactions, track our investments and guide our airliners safely home. We trust computer systems each time we pay for a purchase using a debit card. In fact, we are inconvenienced when a place of business does not accept

---

1 full mouth series per day, for 250 days per year, the total will reach 1 gigabyte. Now, consider that these records should be
electronic cash. This level of trust has been achieved through public confidence in the security of these systems.

Does the future hold the same for a dental office? Certainly patients will expect the same level of trust and security from their own dentist. As the number of dental practices using COHR systems increases, dentists must assure themselves and the public, that they are capable of providing a ‘trusted’ computer based record keeping system.

One only needs to consider the alternative. The recent media attention to computer hacking would only be further aggravated by a story whereby a patient suffered grave consequences as a result of a single breach of confidence in the dental office. This could cause an erosion of public trust in dental computing and dentistry. Moreover, patients may feel threatened and suppress sensitive facts, which would degrade the quality of record keeping and treatment. Patients would prefer to hide embarrassing facts.

For dentists considering the installation of a computer system and for those who already use computers in the practice, the message about computer security is clear. You either: Do, or do not. There is no try.
References

1 Rhodes, P.R., The Computer-based Oral Health Record, Journal of Dental Education, 1996, Volume 60, Number 1


3 Department of Justice, Canada, URL: http://canada.justice.gc.ca/atip/Provte_en.html

4 Bill C-6, First Reading to Senate, Department of Justice, Canada

5 Canadian Dental Association, 1999, Position Brief on Bill C-6, Personal Information Protection and Electronic Documents Act URL: http://www.cda-adc.ca/public/frames/eng_index.html

6 Supreme Court of Canada, 1992, McInerney vs. MacDonald

7 Consumer Reports, Oct 94, Who's reading your medical records?, pp 628--632


9 Tsang A.; Sweet D; Wood, Potential for fraudulent use of digital radiography, Journal of the American Dental Association, 1999 Sep; 130(9): 1325-9

