

Ri\$k Management in the Dental Office

Paul H. Downing DDS

Dartmouth, Nova Scotia, CanadaS

William R. Hiltz DipInst BSc CET

Halifax, Nova Scotia, Canada

Introduction

Risk management in the dental office, from a financial point of view, has changed dramatically in the last few years as more and more practices become dependent on information technology. Hardware, software and personnel disruptions, for even a few days, can cause severe financial loss. Longer disruptions can threaten your ability to provide essential services. The continued operation of a dental practice depends on a keen awareness of potential disasters; the ability to implement a plan to minimize disruption of critical computer functions and, the capability to recover the practice's operations quickly and effectively.

In this article we define the three main components of dental office information systems, discuss some of the risks associated with each of these and offer some practical suggestions and simple tips on how you can plan for, and manage, risk in your own practice. In addition, we discuss the abuse of computer systems by their users and how you can prevent this.

Dental office information systems consist of three essential elements; the **physical elements** (hardware), the **non-physical elements** (software) and the **operational elements** (humans). All three elements must operate together at a high degree of reliability, integrity and accuracy; otherwise system performance can be compromised. The degree of information system compromise will depend, in part, on the level of internal control and effectiveness of management.

Without proper risk management of dental office information technology, financial losses can be considerable. Production loss from failed equipment, cost of recovery of lost data, revenue loss from errors in treatment billing, appointment scheduling and account collections are all areas of concern. Mismanagement of your dental computing resources may also encourage fraudulent activity by dishonest employees. Finally, a compromised information system can result in erosion of your patients' confidence in the practice.

The Physical Elements, Hardware:

Consider these consequences of a recent dental office's computer hardware failure. Because of time needed to restore lost data, a patient who owed money on account does not receive any statements for three months. When a statement finally arrives, it contains incorrect and overstated charges. In the same practice, another patient pre-confirmed their appointment two months earlier and then arrived on time. The office had lost their records for this patient's appointments, so the patient was forced to wait 45 minutes, as they were now double booked. These are concrete examples of events that have happened due to hardware failure. In this example, the most recent backup of critical data was several months old. Aside from the patients' frustration, the staff was overloaded, as they coped with re-entering several months of transactions using patient charts, old reports and notes. A sense of tension flowed through the practice, as everyone operated in crisis mode. One could never estimate exactly how much money was lost due to the damage of patient accounts and erosion of patients' confidence in the practice. Planning ahead could have prevented these examples.

Hard disks fail, monitors accidentally unplug, but the ultimate hardware failure occurs when the dentist opens the office on Monday morning, only to find that someone else visited on Sunday night. Now the computers are missing, and so is all the data. Accounts receivables, treatment histories, account histories, appointment schedules, insurance information are now all gone.

If the office followed a regular and reliable backup procedure, this would not have happened. Therefore, regular backups really are a must.

There are many ways and systems available for backups. Make use of a few of them. Automatically scheduled backups are very convenient, and can be done by tapes, disks, Zip drives, by copying the file to another part of the hard drive, or in networks to another computer. Take advantage of local computer experts, and have them set up a system that suits your needs. Automatic backups should be scheduled at night or during office down time, and should be set up to record every business day. Backup recording mediums, such as disks or tape drives, should be labeled for each day of the week, taken from the office each night, and returned in the morning. Monitor the backups, to be sure that they are working, and regularly restore the data to another computer. We recommend keeping an archive of month end backups so that little glitches that have occurred over time can be traced back to their origin.

Printed daily reports can help restore lost data, and should always be taken home each evening. At the end of the day, also print out a day sheet of the next day's appointments, so that you will know what patients to expect if the system fails. As we move to a paperless society sometimes it is still necessary to "chop down a few trees".

If the dental software application copyright will allow you to maintain an off-site copy on your system at home, you should restore your office data on your home system at least once a week. Check with your dental software supplier to determine if they will allow you to maintain two copies of your dental system; one in the office, and one at home. If the office computer has a catastrophic failure, the home computer can be quickly brought in as a temporary measure. ZipTM drives are an economical and fast way to transfer data from office to home. While not all dental software licence agreements will allow you use the product on systems outside the practice, we feel that dental software vendors should consider allowing their clients the right to maintain a duplicate "live" copy of the dental application on their home computer. This solves the problem of verifying data backup integrity and, for dentists who live close to their practice, provides a quick and expedient way to recover in the event of an office system failure.

A few years ago, one of the first dentists in our area to computerize his office suffered an extensive fire. He had tape backups home for four of the five working days of the week. When he tried to restore them, none of them worked. All his financial data appeared to be lost. In desperation he checked the fifth tape, which had gone though the fire, been submerged in water and then covered in corrosive ash. Amazingly, it worked. You can never have too many backup copies of your critical data both on and offsite.

Dental office hardware problems can be complex, with interesting complications, so unless someone in the office has a special interest, repairs are usually best left to local professionals. We strongly recommend that each dental office develop a relationship with a local computer technician or company to handle any problems.

The non-physical elements (software)

Most dental software today is quite good. Before buying into any dental software program, do your homework, and be sure the company is selling you something that will satisfy your present and future needs. Assign someone in the office who has an interest in the program as the contact

person for the software vendor, and have them call frequently when there are any problems or suggestions. Vendors should encourage this, as it gives them valuable client feedback towards improving their software.

Your local computer technician can provide a significant role in risk reduction during the finger-pointing process that almost always happens when things go wrong after new software is installed in the dental office. If software problems become complicated, let your technician represent you as a “hired gun” to straighten out the usual quirks that can happen, especially when the software vendor is miles away in another province.

Operational elements (humans).

Proper employee selection and training is essential risk management for today’s information systems. Data input and analysis is useless if it is not accurate and understood. Be sure your employees understand how the systems work.

The most common “risk” is that created caused by the human element. Data entry errors occur in all computer systems. Even banks, with their strict auditing controls, make mistakes from time to time. The majority of dental offices do not have the resources of a bank auditor to ensure that all data entry is correct. Common errors are missing or incorrect addresses, postal codes and telephone numbers. The dentist may never be aware of these, since they do not usually show on the management reports. Nonetheless, a high incidence of these simple errors may indicate that other “sloppy” data entry behaviour is present. Most dental software will allow you to print, or view, a list of patient names, addresses and phone numbers. Look for obvious mistakes and then request they be corrected. An easy way to do this is to direct your staff to update the patient record as each patient arrives. Be specific about how much information is needed. As you probably know, most dental software have places to store “non-essential” items like patient email addresses, preferred appointment times, referrals, short notices and more. The software folks do not put these things in their program just to fill space. Chances are, this information links to a report or other function that is intended to provide enhanced facility. The need for this information may not be immediately apparent however, in time, you may come to appreciate your effort. If you request your staff to enter these items on a patient-by-patient basis as they arrive, the task becomes much easier.

Other, more dangerous, errors include those with patient financial transactions. These include patients not being charged or over-under charged or deletion of charges. Missing charges can be detected by comparing the appointment list against the detailed production summary report at the day end. Some systems will automatically check each day’s appointment scheduler for scheduled patients who have not been charged any fees. While this provides a convenient and quick verification at the end of the day, it still does not check for under or overcharged patients. A quick review each day of service charges (by treatment code) for each provider will usually spot these errors. Your staff must be fully aware of the treatment fees and any variances from the provincial fee guide that you may use.

Most dental software suppliers will provide an annual update of the provincial fee guide. In one office, the recently updated 1999 fee guide contained several fees from the 1998 fee guide. For many months, the staff continued using the 1998 fees to process insurance claims and calculate co-payments. The fee differential was only a few dollars but over time, it amounted to a significant amount of unrecoverable revenue. Therefore, it is prudent to request a printed copy of your fee guide from the computer system and review the fees to make sure they match with the current guide. When you receive an annual fee guide update from your software vendor, repeat the process. You do not need to check every fee, just the ones that are most common.

A number of dental programs will allow complete deletion of individual patient charges in order to correct inappropriately billed accounts. Other systems will only permit adjustment entries to balance the account and some permit you to decide which method to use. If your software will permit deletion of patients' charges (or payments) make sure that you have some way to track this. In our office, each user must log on to the computer system using a unique user name and password. As deletions, adjustments or transfers are done on any account, the system maintains an audit log that reports the action, time of day and user. This way, uncertain deletions can be questioned.

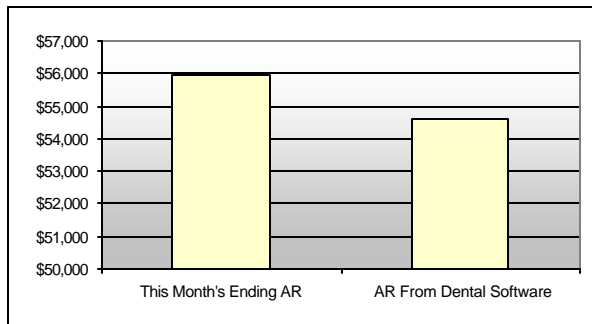
While most dental software today is quite good in terms of reporting and auditing, additional systems should be used to ensure the data is accurate. One method is to go back to old-fashioned paper. We always print a report of production and payment by provider, at the end of each day. A quick review before going home can disclose errors or omissions in billing, while everything is still fresh in your mind (we only billed this much?!). The report is filed, at home, for future reference at the month end, and as a backup.

Take the time every week to randomly audit one day's production. Once you become accustomed to reading the reports, this process will only take a few minutes. Review in detail, the transactions from the previous day. Compare the day sheet to the production report, to be sure that all patients were charged properly.

At the end of the month, a report showing daily totals is printed. The totals are compared to the printed daily report totals that have been kept on file. We reconcile our bank statements at the end of each month, so why not do the same for our daily printed reports. If everything is in order, the month is closed off or "locked", so that no further changes (hopefully) can be made.

At the end of each yearly quarter, the printed monthly totals are compared to the computer totals, to be sure again, that no changes are occurring.

Computer spreadsheets are another tool in checking office data. It is relatively easy to create a spreadsheet from Lotus or Excel, where monthly total charges and payments by provider can be entered, and a year to date running total produced. This should be the same as the yearly running total in the dental software. More importantly, the monthly accounts receivables can be monitored. (Previous AR + charges - payments = current AR.) Have the spreadsheet calculate this, and then compare the AR to the dental programs AR. If these two totals are not the same there are serious problems.



<i>Previous Month's AR</i>	\$46,213.00
<i>This Month's Charges</i>	\$48,977.00
<i>This Month's Payments</i>	\$39,256.00
This Month's Ending AR	<u>\$55,934.00</u>

AR From Dental Software	\$54,633.00
Difference	\$ 1,301.00

Checking your computer account receivable from month to month is a simple 3-step process.

Risk management is just one component of a practice's overall management program. In general, if an office has poorly developed general management skills, employees will have an inadequate understanding of the goals, objectives and priorities of the practice. As a result, staff may often operate in crisis management mode and become involved in too many activities. A by-product of this is that some staff may equate increased activity with productivity. This transcends to the dentist who notices increased activity and reduced productivity and then questions; "Why did we ever buy a computer in the first place?" While there is no doubt that the issues surrounding proper risk management require a sense of urgency, they are often undermined in practices that lack effective planning and organization in other areas. Therefore, in some practices, simply having a risk management plan may not protect solvency in all disaster situations.

Putting it all together.

We have discussed the three most important risks in dental office computing: computer unavailability, software development and inconsistencies in data. To mitigate the effects of computer hardware failure, a disaster recovery plan should be created. Develop an ongoing relationship with a local computer "hired gun" to manage hardware/software glitches. To detect inconsistencies in data, implement a formal report policy. Finally, backup your data backup, backup your data, backup your data!

We're reminded of a verse from a Joni Mitchell song where she sang: "Don't it always seem to go that you don't know what you've got till it's gone". Do everything you can to ensure your computer systems are available, replaceable in a hurry and contain accurate data. Lost computers and lost patients are big holes to fill in your practice.

About the Authors

Dr. Paul Downing has worked in private practice in Dartmouth, Nova Scotia since graduating from Dalhousie University in 1979. He has been active in organized dentistry in Nova Scotia, where he has served as president of the Halifax County Dental Society, Chairs of Public Relations, and Professional Development Committees for the Nova Scotia Dental Association, is co-founder and frequent guest speaker of the Chebucto Dental Implant Study Club, and is currently vice president of the NSDA. His dental office has been computerized since 1989, and has helped as beta test sites for two different aspiring dental software programs.

William Hiltz has been providing computer and management consulting services to dentists since 1992. He holds a Diploma in Industrial Instrumentation from the Marine Institute, an advanced B.Sc. from Dalhousie University and is a Certified Engineering Technologist. Presently he is completing MBA studies at Dalhousie and is an adjunct faculty member of the Nova Scotia Community College where he delivers courses in Programmable Logic Controllers and Dental Informatics. He may be reached at by email at: wrhiltz@is2.dal.ca or by Internet at www.wrhiltz.cjb.net