

# Softwords

A&L Computer Software Limited

June 2004



A&L's Head Office: (905) 886-8066  
 Oak/Miss/Bramp/Ajax: (416) 520-3238  
 Ottawa Office: (613) 737-0677  
 Timmins Office: (705) 268-4922  
 Windsor Office: (519) 977-6050  
 Web Link Address: www.anl.com

## ...Contents...



### The Future Is Now

Increasing Document Security, Accessibility & Productivity

...Page 1



### Inefficiencies In Medical Offices

Don Price

...Page 2



### User's Corner:

System Transfers  
FHG Billing

...Page 3



### PIPED Act

...Page 3

Softwords is a quarterly newsletter published by A&L Computer Software Limited, 175 W. Beaver Creek Road, #6, Richmond Hill, ON, Canada, L4B 3M1. Reproduction of Softwords without written permission is strictly prohibited. For information, questions or suggestions concerning the publication please contact the editor, David Haisell, at the above address, or e-mail at dahais@aol.com.

A&L Web site: www.anl.com

## The Future Is Now

### Increasing Document Security, Accessibility & Productivity Wishful Thinking or Reality?

Many of us have heard the various media reports detailing instances of identity theft or of personal information being misappropriated in some fashion. While we may focus in on the after effects of information theft, we often don't give much thought to the sequence of events that allowed it to occur in the first place; most often, a culture of complacency surrounding traditional paper or electronic media handling.

Reviewing *PIPEDA*, the federal government's new Personal Information Protection and Electronic Documents Act, one becomes aware of how much this law will change the way many practices manage personal information in their care. Among a host of other requirements, safeguards must be in place to protect personal data against loss or theft, unauthorized access, disclosure, copying, use or modification, regardless of the format in which it is held.

If you need to find an alternative to insecure bulky paper files or a method of controlling access to and sharing electronic documents, A&L's document management application, **Document Console**, might be something to take a closer look at.

#### A&L Document Console & Security

Like many robust applications, Document Console has the ability to manage simultaneous users and also control what functions each user has the ability to perform on the retrieved documents. This would be analogous to having a security officer assigned to each staff member who accesses paper files. The security officer would not only check to see if the person were allowed to have the document, they would also accompany and protect it based on a pre-defined set of permissions.

It is important to note that documents

are stored *inside* the Document Console databases in an encrypted format. Your information is completely protected; even if an unauthorized person gained access to the raw databases, they still wouldn't be able to view or retrieve any of the stored documents.

#### A&L Document Console & Accessibility

Document Console has been designed to work with both Local Area Networks (LAN's) and Wide Area Networks (WAN's). Simply stated, this means that documents can be accessed from any computer in the world that has a high-speed Internet connection and of course, Document Console. When the document has been retrieved, and as long as the user has the proper permissions, it can immediately be edited, printed, faxed, e-mailed or exported out of Document Console for use with another application.

#### A&L Document Console & Productivity

Think of the steps and time required to create, retrieve or re-file documents, especially if they have been misplaced or misfiled. How many man-hours per day are consumed maintaining your paper based filing system? There is just no getting around the fact that the greatest time component involved with traditional paper files is document handling. With Document Console, any saved document is only a few keystrokes away and misfiled documents are a thing of the past since a search on the actual text contained within a document can even be performed.

In many traditional filing systems, paper is the medium used for information storage, and as noted above, considerable

(Continued on Page 2)

## The Ten Most Inefficiencies Seen In Medical Offices

By Don Price, B.Sc., M.B.A.

This is one of a series of articles by Don Price on Practice Management which have been appearing in recent issues of **Softwords**. Don Price, B.Sc., M.B.A., is a Practice Management Consultant based in Ottawa, Ontario. He travels extensively throughout Canada helping physicians and their staff tune up and revitalize their offices through consultations and seminars. In addition, Mr. Price publishes workbooks and two bi-monthly newsletters for physicians and medical office staff. He can be reached at 1-800-458-1900 or fax (888) 339-5975.



**T**here's a common misconception that because medical practices are dealing with life and death situations on a regular basis, it's hard to maintain efficiency consistently.

"No two days are alike," says one doctor. "We can't anticipate where the next crisis is going to land us."

"It's all well and good planning a schedule," a staff member says, "but patients don't plan to be sick on the day we've set aside for their particular problem."

Both are right. This makes running a medical practice more challenging than running almost any other sort of business.

There are ten mistakes that the majority of practices have in common, but reducing the negative impact of any of these will enhance efficiency and reduce crisis management.

1. Falling behind schedule. Everyone needs to focus on helping the doctor keep on time by implementing strategies we've often discussed in *The Practice Manager*.
2. Making decisions based on emotion, not fact. Meetings should be held regularly so that problem solving and decision making skills can be utilized properly.
3. Not running the practice as a business. Ensuring that the practice runs efficiently with proper guidance and leadership from the top is imperative, and to achieve this, the doctor(s) must be involved on a daily basis.
4. Lack of communication. Ensure that clear communication methods are initiated and followed at all times. Constantly assess how well ideas, problems, and suggestions are communicated.
5. Poor motivation of staff. Never focus only on staff errors. Instead, each doctor must make a habit of acknowledging the good things staff does each day to make their job easier.
6. Lack of consistent staff training. Train new staff properly from day one. Evaluate staff on an annual basis and help them improve on areas of weakness.
7. Not investing in new technology. Don't force staff to work

with technology that is prone to breakdown or out-of-date. It is generally quite easy to cost justify the purchase of new equipment to enhance efficiency and speed.

8. Doctors can't say "no" to patients. Don't let your patients control your practice. Set policies and enforce them so that patients understand your guidelines.

9. Not charging for uninsured services. Most patients can afford to pay for uninsured services, so develop a formal Uninsured Services Policy, and educate your patients.

10. Poor billing habits. Thousands of dollars are lost each year in most practice through poor billing practices. Doctors need to gain a stronger understanding of their Fee Schedules and use their Day Sheet for billing purposes immediately following each patient visit. ☒

(This article first appeared in *The Practice Manager*, a newsletter published by Don Price & Associates.)

### The Future Is Now

(Continued from Page 1)

time is spent accessing this material in order to retrieve relevant information. With electronic based systems, the medium is typically a legacy type computer system consisting of a display monitor, floor-standing CPU, mouse and keyboard. This is ideal for environments where users have a static location from which to access Document Console, but it is not efficient or practical for those who require a high degree of mobility in their day-to-day routine.

Notebook computers, while capable of providing limited mobility, are still somewhat unwieldy, especially when compared to the portability of the new generation of Tablet PC's. These devices have now matured well past the point of being an expensive novelty and are quite capable of withstanding the rigours of day-to-day use while providing the computing power and storage capabilities required by today's applications. Perhaps most importantly, they are folio sized, pen-based systems, allowing users to interact with them in a manner as familiar as ... well ... paper and pen. Combining a Tablet PC, Wi-Fi or wireless technology and Document Console can allow immediate, yet secure access to all of your files from wherever you happen to be in your office. ☒

## Users Corner


### A&L HERO\*: Where Does Your Mail Go?

Before identifying where it goes, you must understand how it gets to you. After each transmission, the program goes through a procedure of downloading all files from MOH and our network site. That includes batch acknowledgements, error reports, remittance advices, as well as messages advising you of remittance advices, fee and program updates, cut-off dates, and the odd reminder of MOH procedures. Rejected batches, batch acknowledgments and claims error reports are identified during transmission. After transmitting, you can go into your Unread Mail and check to see if you've received anything. To check your Unread Mail immediately, click on the icon illustrated by the arrow pointing up.

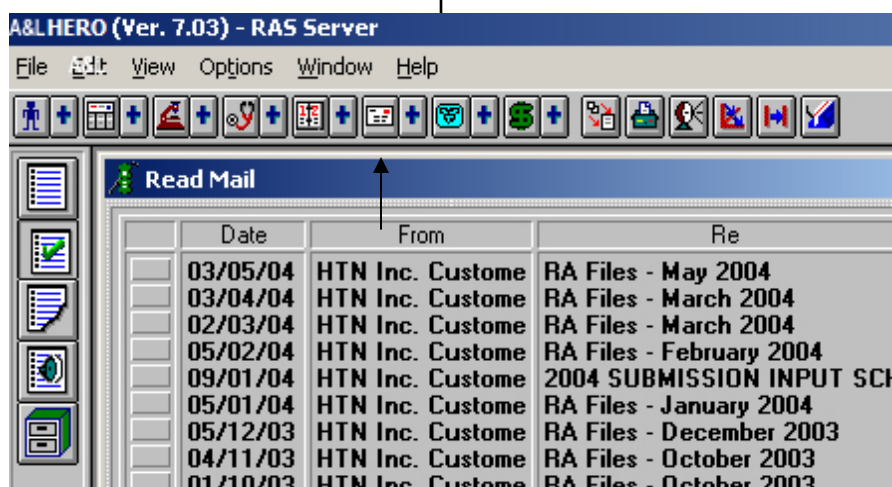
If you do not check it immediately, that's OK. After exiting the application, the first time you launch the A&L HERO\* program and log the doctor in, the Unread Mail will appear. The summary of the internal e-mail will identify the nature of the message. Double clicking on the summary will allow you to see the entire message. At this point, we assume that you have read the message. Upon closing the message the status changes from Unread Mail to Read Mail. Clicking on the Read Mail (arrow on the left side) will show you a list of all

files that have been read or assumed read. If you wish, you can keep the files for reference. However, we do suggest you delete the files once they have been processed. To delete, double click on the line you wish to retrieve and then click on delete.

### OFHG

The Ontario Family Health Group had recently suspended the **group identifier** for submissions. In an OFHG communiqué it had stated that commencing April 1/04, all physicians participating in the Family Health Group model would be required to use their four letter FHG identifier in their claims. This requirement has been put on hold until further review by the Ministry of Health and Longer Term Care, and the Ontario Medical Association. Submitting under the FHG identifier prior to official implementation will result in the entire batch being rejected. If MOHLTC has identified a file being submitted as such, please take immediate action by discontinuing the use of the FHG billing number. You are still being paid for "Q" under your conventional billing number. Your FHG Site-Coordinator will keep you up to date on any future changes. If you require further information, please contact your FHG Site-coordinator. 

\*HERO is a registered trademark of HTN Inc



## Your Practice And The New Federal Personal Information Protection Act (PIPEDA)

The **PIPED Act** sets out ground rules for how private sector organizations can collect use or disclose personal information in the course of commercial activities. It balances an individual's right to privacy with the need of organizations to collect, use or disclose personal information for legitimate business purposes. The *Act* has been law since January 1, 2004 and covers all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations..

The basic outline of **PIPEDA** can be summarized thusly:

If your business wants to collect, use or disclose personal information about people, you need their consent, except in a

few specific and limited circumstances.

You can use or disclose people's personal information only for the purpose for which they gave consent.

Even with consent, you have to limit collection, use and disclosure to purposes that a reasonable person would consider appropriate under the circumstances.

Individuals have a right to see the personal information that your business holds about them, and to correct any inaccuracies.

There's oversight, through the Privacy Commissioner of Canada, to ensure that the law is respected, and there's redress if people's rights are violated.

(Continued on Page 4)

**PIPEDA** (continued from Page 3)

Health-care providers have access to and maintain incredibly sensitive personal information about their patients and under *PIPEDA*, there must be safeguards in place to protect this data against loss or theft, unauthorized access, disclosure, copying, use or modification, regardless of the format in which it is held.

Take an objective walk around your office. How well are you protecting your patient's rights to privacy? In other words, how secure is the information in your care? Are paper files accessible by cleaning service staff, couriers, staff family-members or other members of the general public? Can patient or employee files be easily copied or "walked" out of the office? What about all those little sticky-notes? Is there personal information on these and can others access them? What about disposal? Are documents containing personal information destroyed by shredding when they are no longer required - or are they merely placed in the garbage where someone can retrieve them for potentially nefarious purposes?

How secure are the computer systems installed at your practice - are you updating your virus signatures on a frequent basis? Are you installing the updated service patches for the operating systems? If you have email and Internet access - are there firewalls in place to protect your patient's data from malicious acts? Are the systems protected by secure passwords - and are they located in areas that prevent unauthorized access? Are you performing backups on a regular basis and if so, is the backup medium stored in a protected area or left lying about?

From time to time, your software or hardware vendors may need to have direct access to your data files or hard-copy information in order to resolve technical or procedural problems. Have you made your patients aware of this - and most importantly - have they given consent to have their information potentially made available in this manner? Has the vendor requested your authorization to access this information?

If you provide patient information to the drug companies or others for marketing or research purposes - have you informed your patients of this practice? Have your patients given their consent to have their personal information given to a specific third-party? Have they been advised as to how this information will be used? What has the third-party company done to ensure *PIPEDA* compliance; do they have clearly defined published policies and procedures? If it is a foreign-based company with offices in Canada, do they operate under *PIPEDA* or have they chosen not to for purposes of data trafficking? Have you informed your patients of this?

As you can well imagine, ensuring compliancy with *PIPEDA* will affect many aspects of your practice. Both you and your staff must define and implement policies and procedures that will ensure the ongoing protection of the personal information both in your care and divulged to third parties for other purposes.

**What Is Personal Information?**

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This might include:

- ◆ Age, name, ID numbers, income, ethnic origin, blood type, medical records and history.
- ◆ Opinions, evaluations, comments, social status, disciplinary actions.
- ◆ Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example—to acquire goods or services, or to change jobs).

Personal information does not include name, title, business address or telephone number of an employee of an organization.

**What Is Not Covered By The Act?**

- ◆ The collection, use or disclosure of personal information by federal government organizations listed under the Privacy Act.
- ◆ Provincial or territorial governments and agents of the crown in right of a province.
- ◆ "Business card information" such as an employee's name, title, business address or telephone number.
- ◆ An individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list).
- ◆ An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes.

Further information on *PIPEDA* can be obtained from:

The Privacy Commissioner of Canada - <http://www.privcom.gc.ca>

Ontario Medical Association - <http://www.oma.org>

Canadian Medical Association - <http://www.cma.ca>

Royal College of Physicians and Surgeons of Canada - <http://rpspc.medical.org>

College of Physicians and Surgeons of Ontario - <http://www.cpsso.on.ca/>