Protecting client data

11 steps to take when using technology

By Peter Roberts

The intersection of lawyer ethics and technology use can be murky, especially given the pace at which technology advances continue. So where's the line on how you should safeguard the client information on your systems?

The Law Society of Upper Canada's Practice Management Technology Guideline (http://rc.lsuc.on.ca/jsp/pmg/technology.jsp) specifically reminds lawyers to address concerns about client confidentiality, security, disaster management and technological obsolescence.

The Guideline stipulates that lawyers who use electronic means of communications must ensure that they comply with the legal requirements of confidentiality or privilege set out in Rule 2.03 of the Rules of Professional Conduct. Accordingly, when using electronic means to communicate in confidence with clients or to transmit confidential messages about a client, lawyers should "use reasonably appropriate technical means" to minimize the risks of disclosure, discovery or interception of such confidential communications. If the information is "extraordinarily sensitive," lawyers should use and advise clients to use encryption software.

The Guideline also says that a lawyer should "develop and maintain law office management practices that offer reasonable protection against inadvertent discovery or disclosure of electronically transmitted confidential messages."

Further, the Guideline says that lawyers "should adopt adequate measures to protect against security threats" such as unauthorized copying, computer viruses, hackers, power failures and hardware theft. Moreover, lawyers should have back-up and disaster recovery plans and "should ensure that information in electronic form will be accessible in the future."

Thus, the Guideline gives a "heads-up" to Ontario practitioners in describing the concept of (changing) lawyer competence for protecting client information when using technology. We know keeping up with the changes in the law is difficult enough. But the Guideline tells us that a certain level of lawyer competence in the security of technology is necessary to comply with the Rules of Professional Conduct.

What does "competence" mean in this context? Here, in order of importance and offered from a practice management advisor's perspective, is a list of the present requirements of competency for protecting client information when using technology.

Data safeguarding checklist

1. Turn off the computers at night. Leaving a computer running after you have left for the day allows access to client information to anyone who comes through your office. If you have a storefront or street-level law office (not an office in a secure tall building), it is all the more important to turn off the computers when you close up shop.

2. Use a password to open your operating system. Whether you use a Macintosh or a Windows computer, be sure to set up the user accounts with a secure password. In Windows, go to Control Panel–User Accounts and follow the prompts. On the Mac, go to System Preferences, then Security.

3. Back up client data. This means making a copy of your electronic client data in case the original data is lost owing to a system failure, accidental deletion, file corruption or otherwise. Your backup system might involve CD-ROMs, DVDs, a flash drive, an external hard drive or an Internet backup vendor. A best practice is to use at least two methods of backup. For example, more lawyers are now using an external hard drive as a "local" (in office) backup as well as an Internet account where the files are also backed up on a regular basis. Disk imaging, which is another method of backup, enables copying the software applications, settings and so forth on your hard drive, too.

4. Run a test-restore on the backup. What a concept – actually finding out if you can retrieve the lost files from a backup! You don't want to find out your backup isn't working properly when you are attempting to recover data after your hard drive has crashed. Show yourself that the backup did its job by following these steps: Create a file, back it up, delete the file, and attempt to retrieve the file from the backup. You'll be glad you did.

5. Secure your wireless network. This prevents unauthorized persons from using your network, although technically it can be tricky. You can use the step-by-step instructions on the practicePRO.ca site or ask your technology vendor to assist you with this important task.

6. Use antivirus software and a firewall. Use anti-virus and anti-spyware and keep both updated on a routine basis. Also, be on your guard if you notice an e-mail that is out of the ordinary. Visit only known and trusted websites because malware is transmitted more often by websites than by e-mail.

7. Remove the metadata before e-mailing files. Metadata is "data about data." Sounds geeky, but it is the common term for the potentially embarrassing data that resides hidden from the eye within your electronic files. Think edits, deletions, author names, date created and the like. (See http://tinyurl.com/yand6f2 for details on the subject.) You do not, for example, want the other side to be able to see the edits to your settlement offer or demand letter. Convert the file to a PDF before e-mailing it. Also, in Word 2007, go to the Office button and choose Prepare–Inspect Document to check for metadata.

8. Use a password to protect sensitive e-mail attachments. Oh no! You were tired and accidentally sent the draft settlement offer file to the other side – not to your client with the similar last name! But not to worry because on the attached file you set a password that is required for the recipient to open the file. In Word 2007, go to the Office button and choose Prepare–Encrypt Document–Set the password. In Adobe Acrobat 9 Professional (not Adobe Reader), go to File–Properties–Security, then Security Method–Choose Password Security. At the outset of a matter, discuss your security policy about electronic data with the client and agree on a password that is easy for the client to remember but difficult for others to guess. Password-protected files are harder (but not impossible) to open if the wrong person comes into possession of them.

9. Be familiar with Adobe Acrobat or PDF Converter 6. I like to think of these products as "environments" and not simply software applications. Why? Because the more you work within these programs, the more comfortable you become. Like visiting a foreign country, the longer you are there, the more familiar you become with the area. Soon, with PDF files and features, you realize there is very little you need to do with paper – and remember, using PDF helps reduce the metadata that could be unknowingly shared outside the office.

10. Move the Reply To All *and* Forward *buttons away from the Reply button in your e-mail program.* Nobody is perfect. We have all sent an e-mail message to an undesired recipient at one point or another. Fortunately, to reduce the odds of it happening again, those little toolbar buttons can be moved around by (in Outlook) going to Tools, then Customize. When you see the dialog box appear, ignore it and simply move the cursor to the button that you wish to move. Left-click the mouse and drag the button away from the *Reply* button. Then let go, and voilà.

11. Use Outlook's practice management features, or even better, practice management software. Okay, this is not exactly a security tip, but it can help you manage client files better. Beyond being simply an e-mail or a calendar program, Outlook and practice management products (e.g., Amicus Attorney, TimeMatters, etc.) have many ways to manage information in your practice. Examples are conflicts checks using the Contacts feature; managing telephone conversation records by caller, topic, date or case; tracking case calendars; and managing access to important documents, PDFs and images by attaching a shortcut to the document with the contact. (See http://tinyurl.com/y9o33ka for tutorials from Microsoft on using Outlook features.)

Implement as many of these tips as possible and rest easier that you are closer to achieving that level of technology competence that is increasingly being expected of lawyers.

This article was adapted from a similar article that originally appeared in the March/April 2010 issue of Law Practice magazine, Volume 38, No. 2 (www.lawpractice.org), published by the American Bar Association's Law Practice Management Section. Sections are reproduced with permission of the author.

Peter Roberts is the practice management advisor in the Law Office Management Assistance Program (LOMAP) of the Washington State Bar Association. Formerly a legal administrator in law firms in Washington, DC, New Hampshire, Boston and Seattle, he is a frequent speaker and writer on practice management topics.