PRACTICE ADVICE

PRACTICING SECURELY IN AN INSECURE WORLD

DATE: 2012

PRACTICING SECURELY IN AN INSECURE WORLD

Alexandra Rowland-Carling Ph.D., Director of Professional Practice and Quality Assurance

Without doubt, the changes in technology and the Internet have allowed healthcare practioners more efficient ways to communicate, write reports and chart notes, transfer data and store documents. We can access our schedules on our smart phones, write a report on our laptop and send it to the office via e-mail. Patients, clients and families are asking us to communicate via e-mail and we access those e-mails on phones, tablets and laptops.

As we practice, we must never lose sight of issues regarding patient/client confidentially and rights to privacy, and our obligation to practice under the legal tenets of *Personal Health Information Protection Act* (PHIPA). Unfortunately, here at CASLPO, we receive distraught phone calls from members who have had their phones, brief cases, laptops and purses stolen. Also, as USB memory keys get smaller they are easier to lose. Here is some advice both from the College and from the Information and Privacy Commission (IPC) to help you practice securely in an insecure world.

TELEPHONES:

HOME PHONES: If you are running a private practice from your home, make sure that you have either a separate phone line or a separate voicemail box or 'Call Answer' box for your clients to leave a message.

"You have reached the Rowland's house and Private Speech Services. To leave a message for the Rowlands press one and for Private Speech Services press two."

This preserves your private clients' confidentiality when leaving a message as there is no risk that someone else in your home will hear any details.

SMART PHONES: If you have a smart phone from which you can access voicemail messages and work e-mail make sure that you use all security settings. All phones should be protected by at least a 4 digit password. Many phones now allow for up to a 7 digit password – you can never be too safe.

To add a password to access an e-mail account, try the following:

- Go to your SETTINGS
- Go to GENERAL

- Go to RESTRICTIONS
- Select ENABLE RESTRICTIONS
- Enter your 4 digit password
- Select the e-mail account you want to be locked
- Deselect everything else

If your smartphone does not allow you to do this, try downloading an APP from your App store. You are looking for a Lock application.

BLUETOOTH TECHNOLOGY: Different systems allow you to use your telephone in a "hands free" mode while driving your car. Make sure that you do not take a work phone call when you have anyone else in the car who will hear the conversation. Tell the caller that you will call them back; you can always pull over and go to phone mode for your conversation.

USB FLASH DRIVES:

These are small portable data storage devices also known as memory sticks or keys. CASLPO recommends that you use encrypted USB memory sticks. Encryption is the process of transforming information or data into symbols that are indecipherable thus rendering it unreadable. By putting in your password the information is magically decrypted into text.

It is important that you or your employer write up your use of encrypted USB memory sticks in a policy document so should the memory stick be lost or stolen, you have evidence that you used a secure method of data transfer when you make your report to your Privacy Officer or the IPC.

LAPTOPS:

All laptops you use for your work should be password protected. Do not share your password with anyone and remember to change the password every few months. If you have a home laptop used by other people, make sure that there is NO access to either your work documents or work e-mail.

Laptops and desktops can also be encrypted to further safeguard private health information. By using encryption and pass words, should the worst case scenario occur and a computer is lost or stolen, your patient's and client's information is protected, as are you. Again, we recommend that the use of encryption be documented at your place of work as evidence of due diligence when making a 'breach of privacy' report.

E-MAIL:

E-mail systems can now utilize encryption. In a system that uses Symmetric Cryptography both the recipient and the sender share a common key or password that is used to decrypt and encrypt the message. This is a good method to use with families; you would tell them the password to decrypt the message. Most e-mail encryption software uses this system as it is easy, fast and lower cost. Although some systems allow the sender to decide what is encrypted and what is not, we do not recommend this approach. It is much safer to know that everything is encrypted.

ENCRYPTING WORD ATTACHMENTS:

When you have finished writing the Word document, go to **File.** Click on **Info,** you should see a heading **Permissions.** Click on **Protect Document,** and then select **Encrypt with Password.** You will then be asked to provide a **password** and repeat the password. Send the document via e-mail. In a separate e-mail send the password.

The Information and Privacy Commission have developed 7 Principles (outlined below) regarding the use of e-mails with patients/clients.

IPC PRINCIPLES FOR THE USE OF E-MAILS

1. The privacy of e-mail users should be respected and protected.
2. Each organization should create an explicit policy which addresses the privacy of e-mail users.
3. Each organization should make its e-mail policy known to users and inform users of their rights and obligations in regard to the confidentiality of messages on the system.
4. Users should receive proper training in regard to e-mail and the security/privacy issues surrounding its use.
5. E-mail systems should not be used for the purposes of collecting, using and disclosing personal information, without adequate safeguards to protect privacy.
6. Providers of e-mail systems should explore technical means to protect privacy.
7. Organizations should develop appropriate security procedures to protect e-mail messages.

THE TOP TEN TIPS FOR PRACTISING SECURELY

1. Take an inventory of every piece of technology you use which has private health information.
2. Think how a patient's or client's privacy might be breached with every piece of technology and what you can do to guard against a breach.
3. Assume the worst!
4. When travelling, keep all client files in a locked box and laptops in the locked trunk of your car. Take them into your house/office at the end of your day.
5. When you use the phone think who else could be listening to the voicemail or conversation.
6. Learn about and use encryption.
7. Document EVERY method you are using to preserve confidentiality and privacy.
8. Keep up to date with privacy legislation and recommendations from CASLPO and the IPC www.caslpo.com and www.ipc.on.ca
9. Know what to do if there is a breach of privacy.
10. Call us here at CASLPO about ANY question you have regarding privacy.