PRACTICE ADVICE

TECHNOLOGY AND DOCUMENTATION

DATE: 2009

TECHNOLOGY AND DOCUMENTATION

FREQUENTLY ASKED QUESTIONS

Q: As part of our new electronic charting system, we are unable to provide a handwritten signature. We have therefore recommended that clinicians type their name and professional designation at the end of each e-chart entry. Is this sufficient to meet College standards?

Most electronic charting systems are designed to track all entries through the use of unique identifiers or passwords. This means that every entry is "coded" to identify its author. If your system is set up this way, typing your name and professional designation is sufficient to identify the entry as yours. Some systems do not provide enough room to enter full designations, such as "M.H.Sc., Reg. CASLPO". In this case, some institutions have written a short policy or statement indicating that the electronic signature in its abbreviated form actually refers to the full designation.

Q: Supervisors have always been required to co-sign any documentation completed by their students. Our electronic documentation system does not allow for two electronic signatures on one entry. Our current practice with electronic documentation is for supervisors to write a separate electronic note indicating that they have read and agreed with what the student documented. Is this sufficient to meet College standards?

Yes, this is sufficient. One issue to be aware of, however, is the modification of chart entries. Ideally, your system should allow corrections or changes to be tracked and attributed to the appropriate author.

Q: I am part of a team of professionals who are at different locations and who work for different agencies. The parents of my client have asked me to disseminate my assessment report and regular progress notes to all team members by e-mail. I am concerned about sending confidential information this way.

You can certainly raise these concerns with the parents, emphasizing the risks inherent in sending *any* information electronically. If they still request or insist that you provide the information in this format, you can build in a few provisions to make the e-mail communications more secure. For instance, you could also documents with a password, which you will share with team members under separate cover or via telephone, or you could encrypt your reports and progress notes.

Q: We are involved in designing our new electronic storage system. Is it sufficient for us to retain scanned copies of our standardized assessment forms?

As agencies look for ways to reduce the amount of paper they are storing, members are under increasing pressure to dispose of as much documentation as possible. The act of scanning and storing file contents is acceptable, as long as the information is retrievable in the future if needed or required. It should also be noted that the actual forms need not be retained in paper or electronic format, as long as the information is available somewhere in the record. For example, an assessment report which contains a list of raw scores, percentile ranks, and/or standard scores is in compliance with CASLPO's proposed Records Regulation, 2011. You may want to retain the forms for future use if you feel it may be needed. Some departments and agencies have set up a separate filing system for raw data because members have felt the need to retain this information.

Q: I've heard people talk about "encryption" as a means of ensuring that information is secure on a computer. What does this mean and how do I do it?

According to the Personal Health Information Protection Act, 2004, members must ensure that records of personal health information in their custody or under their control are retained, transferred or disposed of in a secure manner. Encryption is the process of transforming information to make it unreadable to anyone except those possessing a key or password. The result of the process is encrypted information. Cryptographic software to perform encryption at various levels is widely available. You can also encrypt a word document on your desktop computer by going into FILE, INFO and PERMISSIONS. Consult your Information Technology officer to activate this type of security.

Q: My laptop was stolen and it contained several patient/client reports. What should I do?

The Office of the Privacy Commissioner/Ontario sets guidelines for dealing with this situation, which is considered a privacy breach under the Personal Health Information Protection Act. A series of specific steps should be followed, and are described in the Privacy Commissioner's guide "*What to do When Faced with a Privacy Breach: Guidelines for the Health Sector"*, available at www.ipc.on.ca. The four main steps involve Responding, Containing, Notifying, and Investigating and Remediating. Members are also invited to call CASLPO for advice.

Q: In order to keep my electronic documents secure, I wish to create a back-up system. Does CASLPO have any standards or guidelines?

CASLPO does not recommend any specific methods, however it is common practice to keep electronic documents in a second location in order to prevent loss from theft, fire, or mechanical failure. This is as simple as ensuring that you maintain a back-up of all files on some type of media such as Memory stick or portable hard drive. Online backup services are also available, but check their security settings.