Alberta College of
Speech-Language Pathologists
and Audiologists

Hear. Speak. Connect.

Electronics and Personal Information

Clinical Documentation and Record Keeping Guidelines, Release Date September 2011

The world of computers and technology continues to progress at an overwhelming pace! These developments can have significant implications with respect to how health care professionals handle and protect client information.

ACSLPA's Clinical Documentation and Record Keeping Guideline provides SLPs and audiologists with information regarding the Protection of Personal Information on Personal Computers, Laptops, or other Mobile Devices.

As stated by Alberta's Privacy Commissioner, "reasonable measures" to guard against unauthorized access to information on a personal computer would include the following:

- Password protection using complex passwords; and
- Anti-virus and anti-malware software.

There are several comprehensive anti-virus and anti-malware software products available. In the context of storage of personal information on mobile devices (including, for example, laptop computers, USB flash drives, smartphones, and tablets), encryption is required in order to meet the standard of "reasonable measures".

What is encryption anyway?

Encryption is the process of transforming information (referred to as "plain text") using an algorithm (called "cipher") to make it unreadable to anyone except those having a "key" that enables one to convert the document into a readable form. Encrypted information is also known as "ciphertext". Encryption also refers to the reverse process, "decryption", which makes the encrypted information readable again (Wikipedia, 2011).

Some commercially available software comes with encryption capabilities (e.g., Windows 7 is capable of encrypting the entire hard drive of a computer); typically home versions of software do not have this capability, whereas business versions do. Rather than encrypting an entire hard drive, it is also possible to encrypt specific files on the hard drive of a computer (e.g., files containing client information). Various versions of encryption software are available for purchase.

It's important to note that encryption does not necessarily "follow the data" when moving it from one storage device (i.e. laptop) to another (i.e., USB flash drive). Hence, if you are moving data from one location to another, you will need to ensure that each device has encryption capabilities. Once you e-mail information, it is typically no longer in an encrypted format, so again, you would have to take alternative precautions to ensure the confidentiality of the information while it is in transit (e.g., removing identifying information from the message or password protecting the information in situations where you have control over both the “sending” and “receiving” ends of the system). Of note, Alberta Health Services does have an “e-mail encryption service” which prevents e-mails from being intercepted and read while in transit. There are also third party services available that provide this type of e-mail encryption service.

Take a few moments to consider your computer. Do you have password protection when accessing your account and client information? Do you have any client information on unprotected USB flash drives or lap top computers? If devices are unprotected or if you are sending reports via email, have you removed identifying information from documents or attachments? The time it takes to review whether you are in compliance with privacy requirements will be well worth it down the road!

References

Wikipedia. (2011). Encryption. Retrieved from: http://en.wikipedia.org/wiki/Encryption