



WHAT IS PERSONAL INFORMATION?

“Personal information means information that can identify an individual (for example, a person’s name, home address, home phone number, or ID number). It also means information about an identifiable individual (for example, physical description, educational qualifications, or blood type). Personal information includes employee personal information but does not include business contact information or work product information.”

SOURCE: A Guide to B.C.’s Personal Information Act. October 2015. 5th Publication. Office of the Information and Privacy Commissioner for British Columbia. p. 4. Retrieved March 17, 2018. <http://www.oipc.bc.ca/guidance-documents/1438>

records, which are at a higher risk for accidental loss or damage, should be duplicated and stored in a separate secure location.² Original works (including drawings, art work, etc.) belong to the client and should be returned as soon as they are no longer needed.

If you are using an app to manage your private practice, make sure you are familiar with the security and storage methods and that they meet the standards set out by PIPA. You may also want to consider using a Canadian company for cloud storage. Historically, we have had a limited number of Canadian companies to choose from, but that is changing. A good review and comparison article — “Canadian cloud providers: Which providers comply with Canadian regulations?” by Davis Porter (February 16, 2017) — is available at www.cloudwards.net/canadian-cloud-storage-providers/.

It is a recommended best practice that you retain closed clinical files for seven years, starting at the date of the last client contact. If an inactive file concerns a client who was under 19 years of age (B.C. age of majority), the start of the recommended seven-year retention period would commence on that child’s 19th birthday.³

We may be tempted to destroy

LET’S TALK RECORDS RETENTION

BY CORAL PAYNE, RCC

Let’s talk about clinical records. How we store them. How long we need to keep them. Would someone know what to do with our clinical files if something happened to us?

As mental health professionals, we are legally obligated to protect client privacy, which includes information we keep in our clinical records. Under the Personal Information Protection Act (PIPA),¹ it’s our job to make sure we protect our clients’ personal information by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.

Did you know that, under PIPA, we are also legally required to have in place a privacy policy, which should include a records retention and destruction policy? This is not only best practice but can be particularly important if we become incapacitated or pass away unexpectedly.

Your privacy policy will be instrumental in helping the person you have appointed to manage or wrap up your practice know where your files are located, how to access those files, how to contact clients to determine what they want done with their files, how long to keep them, and how to dispose of them safely.

Clinical records (hard copies/electronic/scanned) should be stored in a locked filing cabinet in a locked office. Electronic

client files as soon as possible so they cannot be used by third parties. This is not advised. Some offences — for example, sexual assault committed against someone who was a minor at the time of the incident — do not have a period of limitation, and clinical records may help to bolster a client's testimony (McEvoy, 2013; see first note). In some instances, it may be helpful to keep a summary of the original clinical records (frequency of sessions, treatment plan, progress, referrals, etc.) until you are sure they are no longer needed.

Keeping our clients' personal information safe is of great concern to us all. Are you using new technologies? Have you updated your privacy policy lately? Can someone step in and secure clinical records if you become incapacitated? This would be a great topic to explore at your next peer supervision or clinical supervision session. Find out what others are doing, and look for areas of improvement to your own systems.

BCACC members have access to many helpful

documents located in the "Members Only" section of the BCACC website (bc-counsellors.org) under the "legal" tab, including:

- ▶ A Counsellor's Guide for Developing Client Personal Information Policies and Procedures
- ▶ Standard for the Content of Clinical Records
- ▶ Standard for the Use of Technology in Counselling
- ▶ Standard for Informed Consent to Clinical Counselling and the Collection, Use, and Disclosure of Personal Information
- ▶ Standard of Practice Clinical Counselling Reports
- ▶ When the Coroner Comes Calling
- ▶ Planning for the Unexpected: How Counsellors Can Prepare their Practice In Case they Become Incapacitated or Die Before they Retire

Another outstanding resource is *Balancing conflicting interests: A counsellor's guide to the legal process* by Maureen McEvoy (2013, 3rd ed. Justice Institute of British Columbia).

RESOURCES

- 1 Personal Information Protection Act. http://www.bclaws.ca/Recon/document/ID/freeside/00_03063_01
- 2 McEvoy, M. (2013). *Balancing conflicting interests: A counsellor's guide to the legal process*. 3rd ed. Justice Institute of British Columbia.
- 3 Bryce, G. (2nd ed.) *Planning for the unexpected: How counsellors can prepare their practices in case they become incapacitated or die before they retire*. BCACC: Victoria, B.C.

THE RULE OF TWO

BY CONSTANCE LYNN HUMMEL, RCC



As counsellors, we need to find ways to practise due diligence in protecting client information, while also accounting for the unique needs of our practice in an ever-changing world. A simple rule I recommend is the "Rule of Two" when it comes to security and storage of clinical files. What is the Rule of Two? No matter which method you use to secure and store files, make sure there are always two layers of security someone would have to get through to access information and always store client files (or summaries of files) in two different locations.

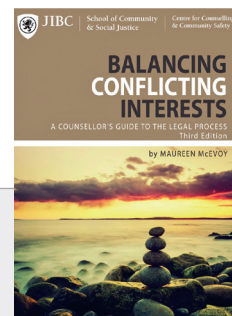
TWO LAYERS OF SECURITY ▶ If you use paper files, this could mean files are placed in a locked cabinet inside a locked office. If you use digital storage, this could mean your files are stored on a password-protected and encrypted external hard drive, and that hard drive is stored

in a locked drawer. If you use an online client-management system or cloud storage, this would mean two-factor authentication and encryption enabling so someone would have to break two passwords instead of just one to access your files.

TWO LOCATIONS ▶ I recommend, at minimum, having a physical or digital backup of client intake information stored in a secondary location (protected by two layers of security). Having full case files (or client intakes/file summaries) backed up in a secondary location means if one of your systems fails (fire in your office, power goes out, hard-drive crashes, etc), you still have either a full backup of all files in a secondary location or at least the intake/summary, so you know exactly who you are currently seeing, can get in touch with past and current clients as needed, and have a quick overview of presenting concerns.

Remember: no system is fail-proof. Over a long career, even with careful planning, things can happen. The Rule of Two helps mitigate the worst-case scenarios and shows you did your best to protect your client data.

Constance Lynn Hummel, MA, RCC, is a psychotherapist, leadership coach, and business strategist for therapists. TheBusinessOfHelping.com



FOR YOUR BOOKSHELF

Balancing conflicting interests: A counsellor's guide to the legal process by Maureen McEvoy, RCC, is a must-have manual for those employed in mental health as counsellors and educators. It includes updates related to changes to the Family Law Act and insights into the legal implications surrounding client interaction and social media.

To get your own copy, follow the link to the order form at: www.jibc.ca/news/balancing-conflicting-interests-counsellors-guide-legal-process.