Closed Files – Retention and Disposition

August 2017

DM155602

This article was updated by Barbara Buchanan, QC, Practice Advisor, in August 2017. Previous updates were: Barbara Buchanan and Chris Canning, Summer Law Student, July 1, 2015; Barbara Buchanan, March 2015; Barbara Buchanan, and Michael Choi, Summer Law Student, June 2013. The article is based on a version co-authored by then Law Society staff Felicia Folk, Practice Advisor, Jackie Morris, Staff Lawyer, and Karen Munro, Summer Student, and first published in *The Advocate* 403 (Vol. 54, Part 3 May 1996) under the title, "Closed Files: What Shall We Do With Them?" and was later revised and given its present title. The present article is updated to August 1, 2017.

The Law Society of British Columbia
8th Floor, 845 Cambie Street
Vancouver, B.C. V6B 4Z9
Telephone: 604.669.2533, toll-free 1.800.903.5300
Fax: 604.669.5232
TTY: 604.443.5700
www.lawsociety.bc.ca

Table of contents

Introduction....1

Purposes of file retention....1

1. Statutory requirements – the client....1
2. Regulatory requirements – the lawyer....1
3. Ethical requirements – the lawyer....4
4. Defending against negligence claims....5
    a. The former Limitation Act, R.S.B.C. 1996, c. 266....5
    b. The new Limitation Act, S.B.C. 2012, c. 13....6
5. Defending against complaints....6
6. Future needs of the lawyer or client....7

Reasons for destruction of file documents and files....7

1. The client already has all significant file materials....7
2. Space and cost....8
3. The future of the firm....8
4. Statutory requirements....9

Procedural steps in retention of files....9

1. Maintain appropriate file organization from the start....9
2. Strip the file on closing....9
3. Establish a file destruction date....12
4. Choose a method for numbering and organizing closed files....13
5. Storage considerations....13
    a. On-site storage concerns....13
    b. Off-site storage concerns....14
    c. Security and confidentiality....14
    d. Fire....15
    e. Flooding and other water damage....15
    f. Environmental factors....15
    g. Earthquake....15
    h. Insurance....15

i. Other concerns....16
6. Off-site storage possibilities....16
a. Self-storage....16
b. Records storage providers....17
c. Archives....177
7. Electronic storage....18
a. Local storage and backup....18
b. Document imaging....18
c. Off-site, network, and cloud storage....19
How long to retain files....20
Methods of destruction....20
1. Physical destruction....20
2. Destruction of electronic documents....211
Some resources....22
Appendices....233
Appendix A: Statutory requirements for client records....233
a. Business Corporations Act, sections 42, 44, 196, and 356....233
b. Canada Business Corporations Act, sections 22, 50, 155, 157, 209, 223(5), and 225....244
c. Income Tax Act provisions....255
d. Other legislation....255
Appendix B: Suggested minimum retention and disposition schedule for specific records and files....26
Appendix C: Closed file information form and checklist....32
Appendix D: File ownership....34
1. Document ownership at termination of retainer — accounts paid....34
2. Document ownership — solicitor's liens — accounts unpaid....35

Closed Files – Retention and Disposition

Introduction

What should a law firm do with its closed file records? This paper discusses why a lawyer should retain client files and records, how this can be done, as well as time frames for destruction.

Purposes of file retention

Why should a lawyer keep client file records after the work is finished? There are statutory, regulatory, ethical, and practical reasons to keep client file records for various lengths of time.

1. Statutory requirements – the client

Statutes such as the *Business Corporations Act*, S.B.C. 2002, c. 57, the *Evidence Act,* R.S.B.C. 1996, c. 124, the *Income Tax Act*, R.S.B.C. 1996, c. 215, the *Canada Business Corporations Act*, R.S.C. 1985, c. C-44, the *Income Tax Act,* R.S.C. 1985, c. 1 (5th Supp.), the *Canada Evidence Act*, R.S.C. 1985, c. C-5, the *Personal Information Protection Act*, SBC 2003, c 63 contain records retention provisions, some of which are set out in Appendix A. Lawyers should be aware of the provisions and return to the client any original documents the client is required to retain. Some clients may not be permitted to keep records outside of Canada (e.g. registered charities, municipalities, public bodies). For such clients, records that are kept outside of Canada and accessed electronically within Canada are not considered to be records kept in Canada.

A client may also be subject to the statutory requirements of governments outside of BC or Canada for which the client may require advice from counsel competent to practice in such other jurisdictions.

If the client instructs a lawyer to retain the client's records until certain statutory requirements are fulfilled, and the lawyer chooses to accept that responsibility, the lawyer should establish the terms in writing, including who will bear the costs of such retention and when the obligations will end. These matters can be dealt with in the retainer letter or the final closing letter.

2. Regulatory requirements – the lawyer

The Law Society Rules include mandatory provisions regarding storage, retention, production and security of records. There are requirements related to fiduciary property, general funds, trust funds, valuables, cash transactions, complaint investigations, forensic audits, client identification and verification, leaving a firm, storage providers and the security of records. Lawyers should familiarize themselves with the rules and pay close attention to rule changes.

What are the record retention requirements for Law Society Rule purposes?

The length of time that a lawyer should keep a record depends on the type of record. Is it a trust accounting record, a client verification record, a legal opinion written to the client or something else? Consider what is meant by a "record" in the context of a particular rule. For example, Rule 3-75 only applies to the records referred to in Rules 3-67 to 3-71. In contrast, the records referred to in Rules 10-3 and 10-4 are a broader category of records (more on this later).

Accounting, trust account, general account, cash and billing records. Rule 3-75 applies to the records referred to in Rules 3-67 to 3-71. Rule 3-75(2) requires a lawyer to keep the following records for as long as the records apply to money held as "trust funds" (as defined in Rule 1) or to "valuables" (as defined in Rule 1) held in trust for a client and for at least *10 years* from the final accounting transaction or disposition of valuables:

- accounting records, including supporting documents (Rule 3-67);
- trust account records (Rule 3-68);
- general account records (Rule 3-69);
- records of cash transactions (Rule 3-70);
- billing records (Rule 3-71).

A "record" includes "metadata" associated with an electronic record (as defined in Rule 1). Note that "metadata" includes the following information generated in respect of an electronic record:

- creation date;
- modification dates;
- printing information;
- pre-edit data from earlier drafts;
- identity of an individual responsible for creating, modifying or printing the record.

Except for electronic records, Rule 3-75 requires that the records to which it refers *must be kept at a lawyer's chief place of practice in BC for at least three years* from the final accounting transaction or disposition of valuables. Having regard to the accounting and storage systems employed by a specific lawyer, Rule 3-76 permits the Executive Director to modify the storage requirements of that lawyer under Rules 3-68 to 3-71 or 3-75.

Monthly trust reconciliations and supporting documents. A lawyer must retain monthly trust reconciliations and the detailed listings required to support the reconciliations for at least *10 years* (Rule 3-73).

Fiduciary property. If a lawyer is responsible for "fiduciary property", Rule 3-55 requires that a lawyer must be able to produce on demand, for *10 years* from the final accounting transaction or disposition of "valuables":

- a current list of valuables, with a reasonable estimate of each;
- accounts and other records respecting the fiduciary property;

- all invoices, bank statements, cancelled cheques or images, and other records necessary to create a full accounting of the receipt of disbursement of the fiduciary property and any capital or income associated with the fiduciary property.

Client identification and verification. A lawyer must retain a record of the information and documents obtained for the purposes of client identification and verification for the longer of (a) the duration of the lawyer and client relationship and for as long as is necessary for providing services to the client, and (b) a period of at least *six years* following completion of the work for which the lawyer was retained (Rule 3-107).

Records storage, security and production of records. Regardless of whether a lawyer stores records in paper form or electronic form and whether the records are stored at the lawyer's office or off-site, a lawyer must comply with the records storage and security rules. A lawyer may maintain records, including electronic records, with a "storage provider" in compliance with Rule 10-3. A "storage provider" means any entity storing or processing records outside of a lawyer's office, whether or not for payment. If for example a lawyer stores information himself or herself outside of the office, the lawyer is a "storage provider". A lawyer must protect all records and the information contained in them by making reasonable security arrangements against all risks of loss, destruction and unauthorized access, use or disclosure (Rule 10-4).

When required under the *Legal Profession Act* or the Law Society Rules, a lawyer must, on demand, promptly produce records in any or all of the following forms:

- printed in a comprehensible format;
- accessed on a read-only basis;
- exported to an electronic format that allows access to the records in a comprehensible format.

A lawyer must not maintain or process records, including electronic records, with a "storage provider" (as defined in Rule 1) unless the lawyer:

- retains custody and control of the records;
- ensures that ownership of the records does not pass to another party;
- can comply with a demand under the Act or the Law Society Rules to produce the records and provide access to them;
- ensures that the storage provider maintains the records securely without
    - accessing or copying them except as is necessary to provide the service obtained by the lawyer,
    - allowing unauthorized access to or copying or acquisition of the records, or
    - failing to destroy the records completely and permanently on instructions from the lawyer, and
- enters into a written agreement with the storage provider that is consistent with the lawyer's obligations under the Act and the Law Society Rules.

A "record" referred to in Rules 10-3 and 10-4 includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise (see section 29 of the *Interpretation* Act). In other words, a record would generally include the entire client file.

Dealing with closed file records is one of the many things to think about when a lawyer leaves a firm or retires (see *Ethical considerations when a lawyer leaves a firm*, *Practice Advice*, Benchers' Bulletin, Summer 2017 or *Winding Up A Practice: A Checklist* on our website). Rule 3-87(1) requires a lawyer, before leaving a firm in BC, to advise the Executive Director in writing how he or she intends to dispose of all of the following that relate to the lawyer's practice in BC and are in the lawyer's possession or power:

- open and closed files;
- wills and wills indices;
- titles and other important documents and records;
- other valuables ("valuables" defined in Rule 1);
- trust accounts and trust funds;
- fiduciary property.

Rule 3-87(2) requires that within 30 days after withdrawing from practice, a lawyer or former lawyer must confirm with the Executive Director in writing that the documents and property referred to in the preceding paragraph have been disposed of and of any way in which the disposition differs from that reported under subrule (1).

3. Ethical requirements – the lawyer

The *Code of Professional Conduct for British Columbia* (BC Code) provides ethical guidance relevant to file management, storage and disposal procedures in section 3.5 (Preservation of clients' property). "Property" has a broad definition and includes a client's money, securities as defined in the *Securities Act*, original documents such as wills, title deeds, minute books, licences, certificates and the like, and all other papers such as client's correspondence, files, reports, invoices and other such documents, as well as personal property, including precious and semi-precious metals, jewelry, and the like (Code rule 3.5-1).

A lawyer must care for a client's property as a careful and prudent owner would when dealing with like property, and observe all relevant rules and law about the preservation of a client's property entrusted to the lawyer (Code rule 3.5-2). A lawyer is responsible for maintaining the safety and confidentiality of the client's files in the lawyer's possession and should take all reasonable steps to ensure the privacy and safekeeping of the client's information.

Code rule 3.5-2 and the duties in Law Society Rules 10-3 and 10-4 are closely related to the ethical duty of confidentiality set out in the rules under Code section 3.3. The duty of confidentiality survives the professional relationship and continues indefinitely after the lawyer has ceased to act for the client (Code rule 3.3-1, commentary [3]). Subject to any solicitor's lien rights, the lawyer should promptly return a client's property to the client on request or at the conclusion of the retainer. A lawyer must clearly label and identify a client's property and place it in safekeeping distinguishable from the lawyer's own property.

4. Defending against negligence claims

A user friendly document management policy should be established and followed. Appropriately documenting a file in the first place, retaining the file, and retaining the right parts of the file can be crucial in a lawyer's defence against a liability claim. The initial retainer letter, notes of instructions and conversations, telephone records, copies of important papers and correspondence, drafts, and other items are particularly important in the defence of a negligence suit or other claim. If a lawyer turns over a file to a successor lawyer, it is in the original lawyer's interest to note what file materials belong to him or her and need not be provided to the client and, before handing the remaining documents over, to keep a copy at the lawyer's expense of certain of the file contents that belong to the client. See Appendix B: Minimum retention and disposition schedule for specific records and files – Rules and Guidelines, and Appendix D: File Ownership.

In light of the discovery component of limitation periods (see below), negligence actions can be brought many years after the alleged negligence has occurred. However, the risk of a claim does diminish as time passes. The Lawyers Insurance Fund reported that from 1986 through 2016, 81% of reports of claims or potential claims were made within three years of the alleged negligence and 97% were within 10 years. Out of a total of 29,510 reports, 832 or 2.8% were made more than 10 years after the alleged mistake. Nevertheless, the possibility of late claims exists and such claims are more difficult to defend against without documentary evidence to refresh the lawyer's memory or to corroborate events.

a. The former Limitation Act, R.S.B.C. 1996, c. 266

Section 3(5) of the *Limitation Act*, R.S.B.C. 1996, c. 266 ("the former Act") governs professional negligence actions, which must be brought within six years of the date when the right to bring the action arose. It was established in *Central Trust Co. v. Rafuse*, [1986] 2 S.C.R. 147, a case that dealt with professional negligence by a lawyer, that the limitation period begins to run at the date the client discovers or ought to have discovered the material facts upon which the cause of action is based by the exercise of reasonable diligence.

However, under the former Act, several provisions operate to extend the six-year limitation period under certain circumstances. Those which most concern lawyers are section 6, which provides that the running of time is postponed where the plaintiff is not aware of the factual basis

of the claim, and section 7, which provides that the running of time is postponed where the plaintiff is under a legal disability. Lawyers should also be aware of any relevant case law that may affect the interpretation and application of these postponement provisions.

These postponement provisions do not affect the running of the ultimate limitation period under section 8. The plaintiff's claim will be statute-barred 30 years after the claim arose.

b. The new Limitation Act, S.B.C. 2012, c. 13

A new *Limitation Act*, S.B.C. 2012, c. 13 ("the Act") came into force on June 1, 2013. The modernized Act brought BC's limitation period legislation in line with that of some other Canadian provinces that have reformed their legislation. There are significant changes to limitation periods for most claims.

The Act simplifies the time limits for filing civil claims. There is a basic 2-year limitation period that begins at discovery and a 15-year ultimate limitation period that begins at occurrence (with some exceptions). There are special rules to suspend limitation periods for minors and adults under a disability.

Claims that accrued and were discovered or reasonably discoverable prior to June 1, 2013 will continue to be governed by the former Act. The Act's limitation periods applies to claims arising from acts or omissions that occur and are discovered on or after June 1, 2013. If the act or omission occurred before June 1, 2013 and discovery of the claim occurred on or after that date, the new basic two-year limitation period applies from the date of discovery unless the Act specifies otherwise (see the transition rules in the new Act).

Under the new Act, most claims are discovered when a claimant knew or ought to have known that the injury, loss, or damage was caused by the defendant and that a court proceeding would be an appropriate remedy (although discovery is postponed for some claims).

The BC Government developed detailed resources on the new Act and the effect of the transition rules, available at ag.gov.bc.ca/legislation/limitation-act/2012.htm. Also see the resources for managing limitations under Limitations and Deadlines on our website.

5. Defending against complaints

A related reason for file retention is to enable a lawyer to defend against a complaint investigation or forensic audit. An investigation or audit may not only occur during the active work on a file or when a client has decided to change lawyers, but also after a file is closed. The Law Society's Professional Conduct Department has advised that complaints usually arise within five years after the file is closed, but they can arise later.

A possible complaint is one of the many reasons why a lawyer should properly document a file in the first place. The same sort of file documentation and document retention described above

for the defence of a negligence claim is useful for replying to a complaint. When investigating a complaint, the Executive Director may require production of files, documents and other records for examination or copying, even if such material is privileged or confidential. If a lawyer who is required to produce and permit the copying of files, documents and records, does not comply, steps may be taken against the lawyer (Rule 3-6).

6. Future needs of the lawyer or client

When creating a closed file records policy, a law firm should consider the types of files the lawyers handle. For example, wills files should typically not be destroyed for a minimum of 100 years after the will was executed, unless 10 years have passed since the deceased's will was probated. Family, commercial, estate administration and trust files may be needed again long after the lawyer's work is finished. These needs do not relate to negligence or complaint problems, but to new instructions from the client as to the interpretation, enforcement, or variation of agreements, or in the case of wills, the upholding the will. Therefore, what is retained in these files and the length of time for retention should reflect these needs. Different types of files can and should be retained for different periods of time. See the suggested retention and disposition schedule for specific documents and files set out in Appendix B of this article.

Reasons for destruction of file documents and files

Why not simply play it safe and keep every file forever? Indeed, this has been a solution for some law firms. However, not every paper in a file, nor indeed every file, needs to be retained.

There are four main reasons why a lawyer might properly decide to destroy a file or part of one:

1. The client already has all significant file materials

Many file documents belong to the client. A lawyer will have provided the client, as part of the reporting process during the course of a file, with copies of documents and significant letters prepared or received. At the file's conclusion, the lawyer should also provide the client with originals (if possible) or copies of all other documents of importance or interest to the client. From the lawyer's point of view, it is better for the client to be responsible for important documents and valuables, since this can help prevent claims for negligent loss of these items. The lawyer should note in the part of the file retained by the firm (whether in paper or electronic form), what documents and valuables were provided and returned to the client. The easiest way to do this is by keeping a copy of the closing letter to the client, which lists the documents and valuables and advises the client of the file destruction date. Also use a closed file information form and checklist. See Appendix C for a sample.

By providing a client with file material on an ongoing basis, and by finishing the file by returning the client's original documents and valuables with a closing letter, the client's needs

for file material in the future are significantly reduced and a file destruction date can be set. For further information, see Appendix D and *Ownership of Documents in a Client's File*, July 2015, a practice resource on the Law Society website.

2. Space and cost

Closed files can be expensive to store. Paper files take up a considerable amount of space to store securely within the office or off-site, which may be costly. Even "stripped" paper files eventually consume a great deal of space. The costs of maintaining and storing records electronically may be more economical than physical storage; however, a lawyer must maintain electronic records, in compliance with the Law Society Rules as previously discussed (see in particular Rules 3-55, 3-73, 3-75, 3-107, 10-3 and 10-4).

3. The future of the firm

What happens when a law firm dissolves, or a lawyer dies, retires, or quits practice? This issue may be of less concern where there are many lawyers in the firm, but it is vitally important for sole practitioners and small firms. Some questions to consider are: Who will have responsibility for the files, who will want them, who will store them, and who will pay for storage? When lawyers leave existing firms, they rarely take closed files, but there should be some discussion about responsibility for the files. A partner continuing in practice elsewhere might depart with his or her closed files, but if that is not possible, a firm may want to know that its responsibility and costs for storage will end at some point. This is another reason that a destruction date should be set by the responsible lawyer for any file that goes into storage.

Any lawyer leaving a firm should have a clear understanding of the firm's intentions with respect to closed files for which the lawyer was responsible. Although it is recommended that files be stored for lengthy periods, a lawyer leaving should confirm with the firm its intentions, especially if the lawyer has concerns that a client may make a complaint or claim which the lawyer can best answer with the file.

From the day a lawyer opens a practice, the lawyer should reduce in size as many files as possible, and set file destruction dates on closing files to make winding up the practice as easy as possible. Before retiring, a lawyer should make arrangements with another lawyer to take custody over closed files which cannot yet be destroyed. These actions may prevent the lawyer's representative from the chore of having to deal with client files and possibly having access to confidential information. Rule 3-87 sets out the requirements for reporting to the Law Society about whatever arrangements are made.

The Law Society does not act as a repository for closed files for lawyers or their estates. In limited circumstances an exception may be made to this practice (for example, where a sole practitioner has died and proper arrangements have not been made in advance for secure document storage). Sole practitioners and lawyers in small firms are especially encouraged to

have a plan in place for unexpected emergencies and for retirement. See the Law Society website resources on Succession Planning and Practice Coverage in this regard.

4. Statutory requirements

Section 35(2) of the *Personal Information Protection Act*, S.B.C. 2003, c. 63 states that an organization must destroy its documents containing "personal information" (as defined in section 1) or remove the means by which the personal information can be associated with particular individuals as soon as it is reasonable to assume that (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and (b) retention is no longer necessary for legal or business purposes. However, despite subsection (2), if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it (section 35(1)).

Lawyers should consider this legislation in terms of how it affects law firm records (including employee records) and client records but the legislation does not decrease the Law Society's record retention requirements as they pertain to lawyers.

Procedural steps in retention of files

1. Maintain appropriate file organization from the start

A user friendly policy for the organization, retention, disposition, and destruction of client files should include a system for managing paper documents, electronic documents, and any non-document items. Designate a person with the skills and authority to implement and oversee the policy. Lawyers and support staff should be trained to understand and adhere to the policy. Not only will it make it easy to find relevant information, but having a policy may assist in responding to a claim or complaint as well as save on storage costs. The policy should take into account the Law Society's regulatory requirements and BC Code obligations set out previously in this article.

2. Strip the file on closing

While a file is open, lawyers and staff can make the eventual job of stripping and closing the file easier. Before a file is closed, it should be stripped. Consider the following:

1. Check the file to ensure that a closing letter was delivered to the client that listed the documents and valuables that were provided or returned to the client and that advised when the balance of the file will be destroyed.

2. Generally, any document that can be obtained from the court, land title office, or other government registry may be stripped from the file and destroyed, including pleadings,

affidavits, transfers, mortgages, and similar documents (see page 24, How long to retain files, for information on the court's file destruction policy). On the other hand, although copies of pleadings may usually be obtained from the court registries, there will be a delay and a cost to obtain them if a lawyer ever needs to do so. The likelihood of needing copies should also be considered prior to establishing a policy to strip all pleadings and other registered documents. Electronic copies may also be sufficient for some purposes.

If the nature of the file suggests that the lawyer will be called upon to provide information or copies to or on behalf of the client, the cost of retaining these documents and retrieving the file from storage and who should bear the cost of that service should be considered.

3. For real estate documents that have been e-filed, section 168.6(1) of the *Land Title Act*, R.S.B.C. 1996, c. 250 provides that an electronic instrument that has been received by the registrar under section 153 is conclusively deemed to be the original of the instrument. For example, an electronically filed Form A is deemed to be the original, not the paper Form A with the actual signature. However, the registrar may require production of the paper versions of the documents for inspection after application but before registration pursuant to section 168.51 of the *Land Title Act*. Lawyers should be in a position to comply with inspection requests from the registrar before final registration of the electronic instrument.

   In most cases, the lawyer can return the paper originals to the client by enclosing them with the final reporting letter. The lawyer will want to keep a copy in the client's electronic or paper file for the normal retention period.

   For more information on this subject, see "Practice Watch: E-filing and retention of documents – What to do?" in *Benchers' Bulletin* (2006) No. 5 November-December.

4. The Law Society Rules set out retention periods and other requirements with respect to specific types of records. See "Regulatory requirements – the lawyer" at page one in this paper for discussion of these requirements.

5. Dispose of or retain other file contents as suggested by this list of sub-files:

Sub-File	Suggested Disposition
Notes, correspondence and emails (communications)	Keep
Pleadings	Put in the firm precedent file or destroy

Client documents (see Appendix D)	Give to the client
Opposing party documents	Give to the client
Case law	List and destroy
Valuables, assets (estates, family, commercial)	Give to the client
Liabilities (estates, family, commercial)	Give to the client
Drafts of agreements (commercial, family)	Keep as evidence of client instructions along with the final version
Medical evidence	Give to the client
Wage loss evidence	Give to the client
Research (non-legal information referred to at trials or hearings)	Put in the firm research files

6. Ensure that electronic data or records are considered when making decisions about the retention and destruction of files. If the file is composed of both physical and electronic parts, ensure that all components are properly indexed and accounted for. Comply with the Law Society Rules regarding the retention and storage of electronic records (see "Regulatory requirements – the lawyer" in this paper).

7. Consider whether additional material should be kept or may be removed or destroyed, depending on the area of law:

    a. **Will files:** Long-term storage of original wills can become a major problem for sole practitioners and small firms, particularly when the lawyers want to retire. For this reason, it is suggested that lawyers return original wills to clients for safekeeping after execution.

Retain copies of everything else in the file: a copy of the original will, successive drafts, notes, copies of previous wills, and correspondence. Will files must be treated differently from other files, since they contain evidence of matters such as testamentary capacity and intention and document the lawyer's work.

Once a will has been probated, it is suggested that the file should be retained for 10 years after final distribution of the estate and any trusts are fully administered.

b. **Corporate files and record books:** For provincially incorporated companies dissolved under the *Company Act*, R.S.B.C. 1996, c. 62, corporate record books must be kept at the registered and records office for at least 10 years after dissolution because a corporation has 10 years within which to reinstate itself. For provincially incorporated companies dissolved under the *Business Corporations Act*, S.B.C. 2002, c. 57, section 351(2) of the Act and section 25 of the Business Corporations Regulation, B.C. Reg. 65/2004 require retention of corporate record books for at least two years or a period designated by the court or other legislation.

   For federally incorporated companies, section 225(1) of the *Canada Business Corporations Act*, R.S.C. 1985, c. C-44 requires the holder of the dissolved company's records to retain them for a period of six years or a period designated by the court or other legislation.

   The lawyer should also keep the corporate file for dissolved companies in case negligence is alleged in the dissolution of the company.

c. **Family files:** Difficulties may arise long after a family file closes. In particular, lawyers are reporting potential negligence problems involving pensions 20 years and more after separation agreements were executed. While permanent retention of family files is onerous, family lawyers should be hesitant to destroy files, and a minimum 10-year retention period is recommended with a potentially much longer time frame where pensions and minors are involved.

3. Establish a file destruction date

After considering the statutory, regulatory, and ethical requirements, the areas of law, and the other issues previously raised in this article, determine a destruction date for each file at closing. While some documents in the file will have been disposed of or destroyed upon closing the file, the destruction date is the ultimate date upon which the balance of the file will be destroyed. See more information about how long to retain files in Appendix A and B.

4. Choose a method for numbering and organizing closed files

Some firms attempt to organize their closed files by the original file number. This is only efficient for storage purposes if all files close at a uniform rate or if, for instance, closed family files are stored in a different area from closed criminal files. Otherwise, fairly bulky files, even after stripping, have to be filed between long-closed files, forcing office staff to shift large numbers of files to fit them in (or give up and store them in a location which may make their future retrieval difficult).

An effective and simple method for organizing closed files is to assign a new sequential number to them as they are closed. Options include:

- using sequential numbers: C-1, C-2, etc. (the C designates closed status);
- numbering each file according to its year of closing (e.g. 15-1, 16-2, 17-5);
- segregating closed files by area of law and numbering sequentially within that area: e.g. RE-16-1 for the first real estate file closed in 2016. While more complex, this system makes destruction easier in that most files in a particular area of law and closed in the same year can often be destroyed at the same time.

Regardless of how the firm organizes closed files, it should also maintain a database (and some lawyers may additionally maintain a hard copy file closing book) that lists sequentially the file name, original file number, closed file number, storage box or carton number and storage location, and the file destruction date. The firm's file database should also be updated with the closed file number and file destruction date.

5. Storage considerations

The following are examples of some factors that a lawyer might consider when choosing where and how to store files in addition to what has been previously said about the requirements under the Law Society Rules 10-3 and 10-4 and the BC Code rules under section 3.3 and 3.5.

a. On-site storage concerns

Closed files should be stored separately from open files. Unused office space is usually the first storage option for closed files. Files can be stored in filing cabinets or in boxes. If shelving is used, steel shelving units are preferable because they are not flammable. Since client security of records is a concern, the firm should ensure that only lawyers and staff will have access to office files. It is advisable to store closed files at the office for at least two years after closing, because this is the most likely time when access may be needed. However, a lawyer must keep some records at his or her chief place of practice in BC (see "Regulatory Requirements – the lawyer" at page 1).

b. Off-site storage concerns

What happens when a firm runs out of office space? For some lawyers, off-site storage locations have included basements, attics, barns, warehouses, and other empty spaces belonging to members of the firm. Most of these, however, may be unsatisfactory choices and may not meet the Law Society Rule and Code requirements previously discussed. Security may be compromised by unauthorized access. Also flooding, fire, vermin, temperature, humidity, and other problems may result. One alternative solution is to rent space and set up a records storage centre. For some firms this will not be an affordable option, and a commercial storage provider should be considered. In any event, in Rule 10-3, a "storage provider" means any entity storing or processing records outside of a lawyer's office, whether or not for payment. A lawyer must not maintain records, including electronic records, with a storage provider unless it can be done in compliance with Rules 10-3 and 10-4.

c. Security and confidentiality

A lawyer must protect his or her records and the information contained in them by making reasonable security arrangements against all risks of loss, destruction and unauthorized access, use or disclosure (Rule 10-4(1)). Any storage area to which unauthorized persons have access should be rejected. If files are stored at the law firm, ensure that clients and other visitors do not have access to the space.

If a lawyer intends to rent space from a storage provider, the lawyer should carefully review the proposed storage agreement and ask a lot of questions before committing. For example, does the storage provider have a privacy officer? Is the privacy officer a member of the International Association of Privacy Professionals? What kind of certification does the privacy officer have? Can the Rule 10-3 requirements be met if the lawyer uses this provider? If lockers are used, are they sufficiently durable? What types of locks are used? How many sets of keys are there for the locker? Will the lawyer be the only individual with access to the locker? Will the storage company's staff have access and for what purposes? What are the insurance needs? Will the storage provider notify the lawyer if there is a Rule 10-4 breach? Rule 10-4(2) outlines the circumstances in which a lawyer must notify the Executive Director of the Law Society in writing of all of the relevant circumstances if the lawyer has reason to believe that:

- he or she has lost custody or control of any of the lawyer's records for any reason;
- anyone has improperly accessed or copied any of the lawyer's records for any reason; or
- a third party has failed to destroy records completely and permanently despite instructions to do so.

In addition to the Law Society's regulatory requirements, section 34 of the *Personal Information Protection Act* places a duty on organizations to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks.

d. Fire

Any storage facility should have adequate safeguards against fire. It may be better to have sprinklers in a storage facility than to worry that the documents may be subject to water damage. In one incident, an entire floor of an American records centre was destroyed by fire, and an investigation showed that sprinklers would have prevented the fire from moving beyond a very limited area (see W.O. Maedke et al., *Information and Records Management*, 2nd ed. (Encino: Glencoe Publishing Co., 1981 at 296).

e. Flooding and other water damage

A potential storage facility should be examined for possible water problems. Basements, in particular, may be subject to dampness and flooding, and overhead pipes and leaky roofs can also be a problem. If files are stored in basements or other areas prone to flooding, file boxes should be placed on shelves that keep them above the flood level.

f. Environmental factors

Temperature and humidity will affect the durability of paper. The more stable the environment, the better the storage conditions. Paper files may need humidity levels between 30% and 60%, and temperature between 18º and 24ºC (W.O. Maedke, *supra* at 295–96). Ensure that other environmental factors are not a concern, such as mold or pests.

Microfilm and computer media require a different environmental standard. Ideally, they should be kept at 18º–22ºC, with relative humidity between 30% and 50%. Remember that many types of electronic storage mediums will decay over time. CDs and DVDs may become unreadable, and prolonged exposure to sunlight or other environmental influences can destroy electronic storage devices as well.

g. Earthquake

If the office is located in an earthquake-prone region, consider any extra precautions that a storage facility takes with regard to earthquake damage protection.

h. Insurance

On-site storage of closed files may be covered by the firm's basic office insurance policy. However, the firm may also want to obtain "valuable papers" coverage. For off-site storage, insurance, including disaster coverage, is particularly advisable since insurance may not be available from a commercial storage business. When files are insured, it is especially important for the firm to keep an accurate index of files and documents stored.

If the firm stores files electronically, consider whether the firm is adequately insured to protect against cyber risks such as viruses, computer fraud, and the theft or manipulation of data. Note

that the professional liability policy obtained through the Law Society does not cover cyber risks or other data breaches: see My Insurance Policy: Questions and Answers on our website.

i. Other concerns

Lawyers who opt to store files in homes or outbuildings should consider floor strength and may need to consult a professional to ensure the structure is suitable for storage. Also consider physical access to files or file boxes. If it is necessary to store boxes in stacks several boxes deep, some boxes will be extremely difficult to retrieve.

When storing information electronically, it is advisable to be aware of the possibilities of future obsolescence and to have a backup storage system and recovery plan.

6. Off-site storage possibilities

a. Self-storage

Where a firm expects that infrequent access will be needed to its physical closed files (or where a small number of files are stored), a self-storage facility may be an acceptable solution; if the storage can be maintained in compliance with Rules 10-3 and 10-4. Self-storage facilities are those which store mostly household and personal items such as furniture and boxes, but will allow a party to store almost anything. In these facilities, it is usually only the party storing the items who has access. The employees at the storage facility will not and should not help to retrieve files. Thus, in situations where files are required frequently and on short notice, accessing files in self-storage may not be a practical use of either a lawyer's time.

Items in self-storage are usually stored in lockers of varying sizes, and the renting party usually supplies the lock and retains the keys. Some facilities have lockers suspended off the ground, which may be more appropriate for files than floor lockers because they would be safer from flood damage. As well, some facilities can supply shelving units inside lockers. Self-storage facilities usually charge for locker rental by the month, and the prices may significantly vary. Self-storage is available in most suburban centres.

Some storage centres may offer business or commercial customer-oriented packages that include heightened security, better access conditions and facilities, and other services.

Self-storage may not be a safe option, however. A law firm has no way to control what types of substances are stored in lockers or areas near its closed file locker. As well, anyone who is renting a locker may have complete access to the storage warehouse. The facility also may not have particular safeguards against fire or water damage.

In short, while a firm must carefully review self-storage conditions, self-storage may be the least expensive option.

b. Records storage providers

Where a firm will need access to closed files frequently, or where it has large numbers of files to be stored, it may wish to consider a professional records storage provider.

Records storage providers offer many services not available with the self-storage option, although there are extra costs for each service. Some will supply software and train law firm staff to index files and boxes. The index is then used by both the storage company and the firm. Some businesses use bar-code indexing to know the location of each box and file, whether stored on its shelves or temporarily delivered to the firm. The records storage provider's employees will search and retrieve specific boxes or files upon request.

Apart from storage, searches and retrievals, other services offered can include the following:

- interfile (adding a file to an existing box);
- courier pick-up and delivery;
- sale of storage boxes;
- confidential file destruction;
- a "destruction date" system which allows a party to request that boxes of files be destroyed on certain dates;
- a climate-controlled vault for computer media and microfilm;
- digitization and electronic information storage and retrieval.

For safe off-site storage, a professional records storage provider may be the best solution. Providers often offer a number of safety features. For example, files may be stored in warehoused boxes to which only trained employees have access. Many have 24-hour surveillance of all entry points. Requests for files are accepted only from designated individuals within a law firm or business. In addition, some facilities are earthquake-proof and fire-resistant, with metal shelving units bolted to a thick concrete floor, with concrete construction throughout, and an extensive sprinkler system.

Services, safety features, and prices vary between the different storage companies. The law firm may be able to negotiate its own contract and basic rates with a storage business, depending on the amount of material stored.

c. Archives

Finally, the lawyer and the client could consider archival donation. This option will be appropriate only for very specific files which contain documents of historical value because of the subject matter or the parties involved. The lawyer could arrange to have any such files examined by the BC Archives in Victoria, BC but only if the lawyer is released from his or her duty to maintain confidentiality and solicitor-client privilege (Code rule 3.3-1). Ownership rights transfers may also be required and file deposits are subject to acceptance policies established by the Archives. Consequently, this option will generally not be a feasible one for nearly all files.

7. Electronic storage

Take into account the requirements of Law Society Rules 3-73, 3-75, 3-107, 10-3 and 10-4 with respect to the information below regarding electronic storage.

a. Local storage and backup

Storing files on computers at the lawyer's place of practice is likely the most convenient way to store information, both for putting files into storage and for retrieval. For computers and electronic storage devices at the office, ensure that proper security measures have been taken at both the software and the physical level. Computers should be password-protected and the appropriate encryption and security measures should be installed to prevent unauthorized access to the system. Lawyers will likely need to consult a professional to ensure that protection and security measures are adequate, as well as for an appropriate system for backing up data and a disaster recovery plan. Data could be lost due to accidental deletion, a virus, power outage, a natural disaster, etc., so a backup data system that duplicates the data should be kept in a safe, secure and fireproof location.

Physical security is also crucial to maintaining proper records storage. In many cases, issues stem from the physical loss of a storage device, which then exposes the law firm to liability for loss of the information contained within it. Controlling access, taking steps to prevent theft or loss of hardware, locking away storage devices properly, and maintaining general office security are important steps to take to protect information.

There are many publications on the topic of digital security and best practices in this area. One free source of information is the Canada Revenue Agency's Information Circular IC05-1R1 "Electronic Record Keeping" available online. Another is the Government of Canada's Anti-Spam Legislation website regarding spam and electronic threats. The Law Society website also has some resources listed under fraud prevention and "Other scams and risks".

b. Document imaging

A firm may consider document imaging, the conversion of paper documents through scanning devices into digital images that can be viewed on a computer. Lawyers can arrange for all incoming documents to be scanned and named according to a document management plan. Scanners can range in price from a few hundred dollars for a personal scanner to thousands of dollars for a high-speed scanner. In addition, money will need to be allocated to imaging software. Whatever technology is used, lawyers should appreciate the evidentiary benefits in defending a malpractice claim if the scanned material provides not just an exact picture of the original document but an exact replicate of the original file. This will help ensure that information probative of events that might have been gleaned from, for instance, the order of documents in the file, different colours of ink used, notes on the file folder itself or pasted onto file documents, is not lost.

The advantage of document imaging is conservation of space; however, there are disadvantages as well. First, staff time is necessary to carry out the scanning. Second, consider future readability of the imaged documents. To help ensure that files are readable, specifications for document imaging technology should require that the files be stored in a non-proprietary format. The computer industry changes so quickly that storing images or text in a proprietary format may result in the documents becoming unreadable. Lawyers should also consider storage conditions, since computer media should be stored where there are special environmental controls.

Consider any relevant implications or concerns about the admission of evidence in electronic form. For example, see the *Canada Evidence Act*, R.S.C. 1985, c. C-5, sections 30, 31, and 31.1-31.8; the *Electronic Transactions Act*, S.B.C. 2001, c. 10; and the *Evidence Act*, R.S.B.C. 1996, c. 124, section 35.

c. Off-site, network, and cloud storage

Some electronic files can be stored at an off-site location, either through physical storage of data devices at an off-site storage facility or over the internet or other network connection. If the firm chooses to store data on a remote network, there are many factors to consider. Basic concerns such as security, costs, and access must be addressed. More complex issues such as the geographical location of the data servers must also be examined carefully due to the possibility of jurisdictional issues and statutory or regulatory requirements.

If a client's file will be stored electronically outside of BC through the services of a third party, the client should be informed of this at the outset of the professional relationship so that the client can assess whether or not the client wants to use the lawyer. Confirm any consent in writing.

Implementation of cloud computing systems further requires that the lawyer be aware of the risks associated with remote storage options and comply with Law Society Rules 10-3 and 10-4. Although the Law Society does not currently specify which storage provider to use or not use, if the Executive Committee declares, by resolution, that a specific entity is not a permitted storage provider for the purpose of compliance with Law Society Rule 10-3, lawyers will not be permitted to maintain records of any kind with that entity. Lawyers must ensure that they meet statutory, regulatory, and ethical requirements, be diligent in assessing which technologies they use and any legal or jurisdictional issues that may apply to them, and establish clear procedures for access to any sensitive information.

For more information on this subject, see the Law Society's Practice Resource, "Cloud computing checklist v. 2.0" (May 2017). For background see the "Cloud Computing Due Diligence Guidelines," (January 2012) on our website (note that Law Society Rules 10-3 and 10-4 came into effect in 2014). Also see the feature article *Cloud Computing* in the Winter 2014 Benchers' Bulletin and the *Practice Tips* article.

How long to retain files

There is no universal agreement on how long to retain client file records. To decide on a file retention policy, take into consideration the statutory, ethical, and regulatory requirements, the areas of law practised by firm's lawyers, and the potential needs of the lawyers and clients. Suggested minimum retention guidelines for BC practice are set out in Appendix B.

Government and public bodies manage their physical and digital records according to legislative requirements. Their records retention schedules may assist lawyers in determining a policy. BC courts retain their records in accordance with the *Document Disposal Act*, R.S.B.C. 1996, c. 99 and three different records schedules. These schedules are the *Administrative Records Classification System* (ARCS), program-specific *Operational Records Classification Systems* (ORCS), and *Ongoing Records Schedules* (ORS). There may also be Special Schedules attached to specific types of records. General information on government records retention policies and the Court Services ORCS can be accessed on the British Columbia government website. See Information Management & Technology.

Methods of destruction

When a law firm decides to dispose of a file, confidentiality should be a major concern. It is not acceptable to throw file documents in the trash or into a dumpster and have them end up at a public landfill. Moreover, as one law firm found out with some criminal defence files, a firm cannot merely place such records in a "recycling bin" without first receiving assurances of confidentiality and destruction (In that instance, a "sorter" found confidential documents in non-recyclable plastic binders, some of which had police stamps, and turned the documents and files over to the RCMP, who then called the Law Society). Confidential documents must be physically destroyed in a secure manner.

1. Physical destruction

If the firm is in a rural area, burning confidential papers may be an option. Some lawyers used to take files to a nearby sawmill and throw them in the cone burner. Unfortunately (for file destruction, but perhaps not for pollution) many sawmills no longer use cone burners. The Law Society has received complaints about lawyers burning files on the beach, as well as of lawyers throwing files into public garbage bins. If Professional Conduct staff see evidence that the method of file destruction is not adequate to maintain client confidentiality at all points during the process, including handling, transportation, and final destruction, a lawyer may be disciplined.

The predominant destruction method is paper shredding. A firm may choose to purchase or lease a paper shredder. The advantages are versatility and immediate access, but the disadvantages

include paper dust (dangerous to computers) and the need to recycle or dispose of the shredded material. A mid-size office shredder can cost up to $2,000 or more.

Shredders are available in a wide range of sizes, from the personal shredder to the "central plant" shredder, and will shred paper into strips or bits of various sizes. Some of the more inexpensive shredders shred in strips that can be re-assembled into a document. "Cross-cut" and "micro-cut" shredders are more secure because they reduce materials into smaller pieces that are more difficult or impossible to reassemble. A firm should weigh the possibility of reconstruction against the cost of more sophisticated shredders.

Alternatively, a firm may hire a paper shredding company. Many such companies will travel throughout BC to shred and then recycle the material. Companies charge by the weight or the volume of the material to be shredded, with some variation depending on location in the province and whether shredding is done at the office or at an off-site location.

Document shredding is also available from some of the off-site file storage businesses. A law firm should require a document or certificate of destruction indicating that the files were destroyed and then recycled. However, a certificate of destruction may not be enough. In BC, a shredding firm was investigated by the police for selling material it had received to a foreign government.

Shredding should ideally be done on-site under the supervision of a trusted member or employee of the firm in order to ensure the security of the documents. The hired shredding company should not have an opportunity to examine the materials marked for destruction. If shredding must be done off-site, ensure that the company has taken sufficient steps in order to guarantee the security and confidentiality of materials during the handling, transit, and destruction of the materials, in addition to providing confirmation of destruction.

When deciding on purchasing an office shredder or hiring a shredding service, a firm should inquire about the preparation required. Most machines, if not all, take staples. Some will even take fasteners and binders. Others may jam with some materials or the company will sort through to eliminate materials which cannot be recycled. Because of the need for client confidentiality, the law firm should sort the materials itself, if necessary, or use a machine or company that will destroy everything while maintaining confidentiality and security.

2. Destruction of electronic documents

Electronic documents must also be destroyed in a secure and complete manner. Simply deleting files from a hard drive or removable storage device is not sufficient since they may remain recoverable. Many different commercial solutions exist; select one that ensures that erased files are not recoverable by any means through guaranteed data destruction and sanitization processes.

If disposing of old computer systems or storage devices, ensure that any sensitive materials are properly transferred to the new system and correctly erased from the old one. For additional

security, remove all storage devices from the old computers and have them physically destroyed with an appropriate shredder or by a commercial shredding service. The BC Government has extensive information about secure electronic media destruction services on its website.

Regardless of the document's form and the method selected, it is the lawyer's responsibility to ensure that the documents in the lawyer's possession are handled and disposed of safely, securely, and completely.

Some resources

1. Risk Management, Limitations and Deadlines, Law Society of British Columbia.
2. Barbara Buchanan QC and Chris Canning, *Ownership of Documents in a Client's File*, July 2015, Law Society of British Columbia.
3. Office of the Privacy Commissioner of Canada, *PIPEDA and Your Practice: A Privacy Handbook for Lawyers* (Ottawa: Office of the Privacy Commissioner of Canada, 2011),
4. Office of the Information and Privacy Commissioner for British Columbia.
5. Practice Resource: Cloud computing checklist v. 2.0, May 2017, Law Society of British Columbia.
6. Practice Resource: Cloud computing due diligence guidelines, January 2012, Law Society of British Columbia.
7. Winter 2014 Benchers' Bulletin, Cloud Computing feature, Practice Tips and Practice Watch.
8. Winding Up a Practice: A Checklist, June 2017, Law Society of British Columbia.
9. Ethical considerations when a lawyer leaves a firm, Barbara Buchanan QC, Summer 2017, Benchers' Bulletin, Law Society of British Columbia.
10. Trust Accounting Handbook, Law Society of British Columbia.
11. Disposal Information Checklist, Law Society of British Columbia
12. D.J. Guth, "Retention and Disposition of Client Files: Guidelines for Lawyers" (1988) 46 *The Advocate* 229.

Appendices

Appendix A: Statutory requirements for client records

The statutes listed below contain retention requirements for certain records. All original documents listed below are best returned to the client when closing the file.

a. Business Corporations Act, sections 42, 44, 196, and 356

Under section 356 of the *Company Act*, R.S.B.C. 1996, c. 62, a corporation can be restored up to 10 years after dissolution. Federally incorporated corporations and provincial corporations dissolved under the *Business Corporations Act*, S.B.C. 2002, c. 57 do not have a limitation date on restoration and have mandatory retention periods established under legislation or regulation. Therefore, the entire record book should be retained in accordance with the guidelines for corporate records provided in Appendix B depending on the type of corporation. These records should include:

1. a certificate of incorporation;
2. a copy of its memorandum, including every amendment;
3. a copy of its articles, including every amendment;
4. register of members;
5. register of transfers;
6. register of directors;
7. register of debenture holders;
8. register of debentures;
9. register of indebtedness;
10. register of allotments;
11. minutes of every general meeting and class meeting of the company;
12. minutes of every meeting of its directors;
13. a copy of every document filed with the register;
14. a copy of every certificate issued to it by the register;
15. a copy of every order of the Minister or the registrar relating to the company;

16. a copy of every written contract under which the company has allotted any shares for a consideration other than cash;

17. a copy of every other document and instrument approved in the preceding 10 years by the directors;

18. a copy of every mortgage created or assumed by the company, whether or not required to be registered;

19. a copy of every audited financial statement of the company and its subsidiaries, whether or not consolidated with the financial statement of the company, including the auditor's reports;

20. where the company is an amalgamated company, all of the above types of records for each of the amalgamating companies;

21. where the company is being wound up, the minutes of every meeting of its creditors;

22. a copy of every prospectus and takeover bid circular issued in the preceding 10 years by the company or by any subsidiary;

23. a copy of every information circular issued in the preceding 10 years by the company or any subsidiary;

24. a copy of the instrument of continuation; and

25. where a receiver-manager is appointed under an instrument registered in the office of the registrar, the name and address of that person, the date of appointment and either the date he or she ceases to act or the date of the completion of his or her duties.

b. Canada Business Corporations Act, sections 22, 50, 155, 157, 209, 223(5), and 225

Under the *Canada Business Corporations Act*, R.S.C. 1985, c. C-44, the following records must be kept for six years after dissolution:

- the articles and by-laws and all amendments
- a copy of shareholders' agreements
- minutes of meetings and resolutions of shareholders
- minutes of meetings and resolutions of directors
- copies of all notices naming the directors of the corporation
- a securities register
- financial statements
- the certificate of dissolution.

c. Income Tax Act provisions

Under the *Income Tax Act*, R.S.C. 1985, c. 1 (5th Supp.), sections 230 and 230.1, the Income Tax Regulations, C.R.C. c. 945, Regulation 5800, and Canada Revenue Agency Information Circular No. 78-10R5 "Books and Records Retention/Destruction," the following records and books must be kept in Canada or another place designated by the Minister by anyone carrying on a business or who is paying or collecting taxes for a minimum of six years after the end of the last taxation year to which they relate or from the date the return is filed:

- records and books of account, together with every account, voucher, invoice and agreement necessary to verify the information;
- annual inventories;
- for a registered charity or registered Canadian amateur athletic association, duplicates of each receipt for a donation;
- any records or books of account that permit the taxes payable or the amounts collected, withheld, or deducted to be calculated, including supporting vouchers and cheques, except for those with different retention periods as enumerated in section 5800 of the Income Tax Regulations. (Note, however, the Law Society Rule 3-75 requirement that lawyers keep their own records for at least 10 years.)

Also see IC05-1R1 "Electronic Record Keeping".

d. Other legislation

Other legislation may be applicable. See, for example:

- *Evidence Act*, R.S.B.C. 1996, c. 124;
- *Income Tax Act*, R.S.B.C. 1996, c. 215;
- *Freedom of Information and Protection of Privacy Act*, R.S.B.C., c. 165;
- *Document Disposal Act*, R.S.B.C. 1996, c. 99;
- *Electronic Transactions Act*, S.B.C. 2001, c. 10;
- *Personal Information Protection Act*, S.B.C. 2003, c. 63;
- *Personal Information Protection and Electronic Documents Act*, SC 2000, c %
- *Employment Standards Act*, R.S.B.C. 1996, c. 113;
- *Provincial Sales Tax Act*, S.B.C. 2013, c. 35, and the Provincial Sales Tax Regulation, B.C. Reg. 96/2013;
- *Excise Tax Act*, RSC 1985, c E-15

Appendix B: Minimum retention and disposition schedule for specific records and files – Rules and Guidelines

The following schedule is a revised and updated version of schedules previously published in D.J. Guth's 1988 article, "Retention and Disposition of Client Files: Guidelines for Lawyers" (46 *The Advocate* 229), and in the original version of this paper published in *The Advocate* in May of 1996. Some lawyers may consider the retention periods too long, and others, too short. Factors such as a matter's complexity may require a longer retention period than this schedule suggests so lawyers will need to apply their judgment on any given file. Records retention policies should account for both the applicable limitation periods as well as an appropriate period to allow for discoverability. A lawyer should use his or her judgment based on the lawyer's needs and the needs of the firm and the clients.

When consulting the guidelines, keep in mind the postponement of the limitation period which is available to a plaintiff who is not aware of the factual basis of the claim or is under a disability, as well as the ultimate limitation period, as described in section 4, "Defending against negligence claims." Determine whether a claim falls under the former *Limitation Act* or the new *Limitation Act* and if any transition rules apply and proceed accordingly.

LAWYER'S PERSONAL RECORDS	
Diaries and time records	Retain at least as long as the files to which they refer are kept
Accounting records and supporting documents, trust account records, general account records, records of cash transactions and billing records	As long as the records apply to money held as trust funds or to valuables held in trust for a client and at least 10 years from the final accounting transaction or disposition of valuables (Law Society Rule 3-75)
Monthly trust reconciliations and supporting documents and detailed listings, including a listing of valuables received and delivered	Retain for at least 10 years (Law Society Rule 3-73)
List of fiduciary property; list of valuables, accounts and records respecting fiduciary property; invoices, bank statements, cancelled cheques or images.	Retain for 10 years from the final accounting transaction or disposition of valuables (Rule 3-55(5).

Client identification and verification records	Retain for the longer of the duration of the lawyer and client relationship and a period of at least 6 years following completion of the work (Law Society Rule 3-107)

CORPORATE, COMMERCIAL & TAX	
Corporate records	For provincial companies dissolved under the *Company Act*: until March 2015 For provincial companies dissolved under the *Business Corporations Act*: 6 years, unless longer retention for a type of record is specified under a different act or regulation For federal companies: 6 years, unless longer retention for a type of record is specified under a different act or regulation
Securities	6 years after financing is completed
Sale of assets and shares	6 years after sale is completed
Private shares issue	6 years after issuance is completed
Share restructuring	6 years after transaction is completed
Amalgamations	6 years after amalgamation is completed
Bankruptcy	6 years after bankruptcy proceedings are completed, or payment
Ordinary Commercial Agreements (not loans)	6 years after the transaction or franchise is completed
Commercial Loans	6 years after the loan's due date

Receivership	6 years after receiver is discharged or payment, unless receiver has entered into another agreement
Indemnity Agreement	6 years after end of term or agreement or termination
Partnership	6 years after partnership agreement is executed
Joint Venture/Syndication	6 years after end of term or early termination
Tax	7 years after the advice is given, if retained for the purpose of giving tax advice (not to abridge any other time periods set out in this schedule)

CRIMINAL	
Prosecution	6 years after completion of sentence
Defence	6 years after completion of sentencing and appeal proceedings (unless strong possibility client has been "wrongfully convicted")

LABOUR	
Collective bargaining	6 years after agreement made
Hearings (labour relations board and arbitration)	6 years after final decision

LITIGATION

Contract action	6 years after dismissal or payment of judgment or settlement, or 6 years after last court activity if matters do not proceed
Tort claim (plaintiff)	6 years after final judgment, dismissal, or settlement, except in cases involving minors*
Tort claim (defence)	6 years after final judgment, dismissal, or settlement
*In cases involving minors, the period commences after the child reaches the age of majority unless a notice to proceed has been filed and accepted (section 20 of the *Limitation Act*).	

MATRIMONIAL	
Litigation	6 years after final judgment or settlement, except when a minor or pension is involved*
Separation Agreements	6 years after pension payments begin; otherwise 10 years after agreement, except where minors are involved*
* In cases involving minors, the period commences after the child reaches the age of majority unless a notice to proceed has been filed and accepted (section 20 of the *Limitation Act*).	

REAL PROPERTY	
Residential conveyance	10 years after state of title certificate received
Commercial conveyance	10 years after closing (there may be transactions of such complexity that a longer retention period is advisable)
Lease/Sub-lease/Licence to occupy	6 years after lease has expired, including any renewal

Foreclosure	6 years after order absolute, property sold, judgment satisfied or instruction received from client to stop proceedings
Receivership	6 years after receiver is discharged or payment unless receiver has entered into another agreement
Option to purchase/Right of first refusal	6 years after the options expire or are exercised
Easement/right-of-way/ restrictive covenant	10 years after registration
Review of title and opinion	6 years from giving an opinion, unless opinion leads to an action
Mortgage/debenture	6 years after expiry of mortgage term
Subdivision/single plan strata development	6 years after completion of the sale of all the property
Phased strata development	6 years after completion of the sale of all of the property in the final phase
Real estate prospectus	6 years after sale of all property covered by prospectus
Building contract	6 years after substantial completion
Encroachment settlement	6 years after settlement

WILLS, ESTATES AND TRUSTS	
Original wills and all wills files	100 years, or, if a will of the client has been probated, 10 years after final distribution of the estate

Estate administration and trust files	10 years after all trusts are fully administered
Committeeships	6 years after committeeship has ended

Appendix C: Closed file information form and checklist

FILE NO. _____ CLOSED FILE NO. _____

DATE FILE CLOSED _____ RETAIN FOREVER ___ YES / NO _____

DESTRUCTION DATE _____

SUPERVISING LAWYER _____

ADMINISTRATIVE ASSISTANT _____

1. Client(s) name _____

   _____

2. Last known addresses, email addresses, and phone numbers

   Business _____ Telephone _____

   _____

   Home _____ Telephone _____

   _____

3. Nature of matter _____

   _____

4. Reason closed _____

5. Judgment entered? Yes ___ Date _____ Not applicable _____

6. Is any client a minor? Yes _____ No _____ If yes, date of birth _____

   Activity required upon majority _____

   _____

7. Client advised as to what must be done upon majority by letter dated

   _____

8. Any limitation dates outstanding? Yes ___ No ___ Limitation date _____

9. Anything requiring us to notify client in the future? Yes _____ No _____

   What? _____When? _____

10. Has this been entered into our reminder system? Yes _____ No _____

11. At time of closing file, any unpaid disbursements, fees, or costs due? Yes _____ No _____ Amount $ _____

12. Were these written off? Yes _____ No _____

13. Trust involved? Yes _____ No _____

    If yes, do we need to notify client when trust terminates or for any other reason? Yes _____ No _____ Date _____

14. Has file been checked to ensure that all important documents or letters have been removed? Yes _____ No _____

15. All **original** documents of client returned to client? Yes _____ No _____

16. Closing letter sent to client and all materials returned? Date _____

17. All returned materials listed in the closing letter? Yes _____ No _____

18. Client and opposing party cards/databases moved to "Closed" and closed file number and destruction date noted? Yes _____ No _____

RETAIN ONE COPY OF THIS FORM AT FRONT OF CLOSED FILE

RETAIN ONE COPY IN "CLOSED FILES" FILE

Appendix D: File ownership

If documents are delivered to the client following termination of the retainer, or if the file is delivered to another party subject to a solicitor's lien, it is important for the lawyer giving up possession to retain a copy, made at his or her expense, of all relevant documents and correspondence.

1. Document ownership at termination of retainer — accounts paid

Which documents should be handed over to a client is a matter of law (*Aggio v. Rosenberg* (1981), 24 C.P.C. 7 at 12 (Ont. S.C. Master)). The lawyer must maintain appropriate security and confidentiality of the client's property at all times (Law Society Rules 10-3 to 10-4 and BC Code section 3.5. See "Ethical requirements – the lawyer" and "Regulatory Requirements – the lawyer" in this article for more information as well as *Ownership of Documents in a Client's File*, July 2015, in the practice resource section of our website.

The following is a non-exhaustive list summarizing document ownership:

The client owns:

- documents created existence before the retainer;
- correspondence from the lawyer or third parties;
- expert reports;
- client's medical records;
- examination for discovery transcripts;
- trial transcripts;
- notes or recordings of conversations with witnesses or officers of the court;
- documents for use in court (case law, briefs, pleadings, factums);
- memoranda of law;
- originals, copies and drafts of wills, powers of attorney, representation agreements, contracts;
- receipts for disbursements;
- corporate seals.

The lawyer owns:

- correspondence from client;
- time entry records;
- inter-office memoranda and other internal communications (including conflicts checks);
- internal requisition forms;
- calendar entries;
- accounting records;
- cash receipt book of duplicate receipts;
- notes prepared for lawyer's benefit or protection at the lawyer's expense;
- ethics consultation notes.

2. Document ownership — solicitor's liens — accounts unpaid

Solicitors' liens are discussed in the practice resource article on our website, *Solicitors' Liens and Charging Orders – Your Fees and Your Clients*.