FILE RETENTION AND DESTRUCTION GUIDELINES

DETERMINING HOW LONG TO STORE FILES

Generally, we recommend that you store client files for at least 10 years from the date you cease work on a client's matter.[1] This practice will help ensure that the file is available for defense against a legal malpractice claim. Legal malpractice claims based on a theory of negligence are subject to a statute of ultimate repose that bars claims not filed "within 10 years of the act or omission complained of." ORS 12.115(1).

There may be reasons to store client files for longer than 10 years before destroying them, including: (1) the type of cases you handle; (2) fee agreement provisions and whether a client consents to destruction; (3) your relationship with a client; (4) whether a file contains specific documents or originals; and (5) a file's potential utility to you or your client in the future. This is by no means an exhaustive list of factors to consider in determining how long to store files. We encourage you to conduct your own research, consider additional factors particular to your cases and clients, and adopt a file storage approach based on your independent reasoning.

Case Type

The type of cases you handle may provide reasons to store the file for more than 10 years, particularly if the case involves:

- Adoption;
- Contracts or agreements requiring payments for more than 10 years;
- Estate planning for clients who are still alive after 10 years;
- Family law matters that are ongoing and subject to modification (i.e., custody, parenting time, support);
- Intellectual property;
- Judgments that may need to be renewed;
- A minor who is still under the age of 18 after 10 years;[2]
- A tax basis in property; or
- A situation in which a professional instinct or personal intuition urges you to keep the file longer.

Fee Agreement and Client Consent

We recommend that you include a provision in your fee agreement or engagement letter that specifies the length of time that you will store the file before destroying it (e.g., 10 years). Your client's signature provides consent for you to destroy the file after the specified period.

---

[1] *See* OSB Formal Ethics Op No 2017-192 (defining "client file," explaining the obligation to produce it upon request).

[2] If you represent a person entering a settlement agreement on behalf of a minor, you are required to maintain that person's affidavit for two years after the minor reaches age 21. *See* ORS 126.725(2). *See also* Brooks F. Cooper, "Settlements for Minors – 2009 Legislative Changes," *In Brief* (November 2010).

If there is no agreement providing for the file's destruction, consider these options before destroying the file: (1) obtain the client's consent to destroy the file; (2) give the client a complete copy of the file; or (3) continue to store the file instead of destroying it. Choosing one of these options will help avoid the predicament where you have destroyed the file without consent, the client does not have a complete copy of the file, and you are unable to comply with a request for the file.

Relationship with Client

Your relationship with your client may provide reasons to store the file for more than 10 years, particularly in situations involving:

- Ongoing relationships with clients;
- Problem clients, especially when you are concerned about a lawsuit or bar complaint; or
- A professional instinct or personal intuition that urges you to keep the file longer.

Specific Documents and Originals

Depending on the contents of the file, you may have an obligation to keep specific documents and originals for a specified period of time or refrain from destroying them. To prevent problems, we generally recommend that you keep a copy of original documents but avoid storing originals when possible. Be especially mindful about storing and destroying documents if the file contains:

- Affidavits or verified statements of a client entering into a settlement agreement on behalf of a minor (*see* footnote 2);
- Corporate books and records;
- Intrinsically significant or valuable original paper documents (e.g., securities, negotiable instruments, deeds);[3]
- Oregon eCourt filings with an image of a document containing another person's original signature, in which case you must retain the original paper document for 30 days;[4]
- Original client documents (*see* footnote 3);
- Original wills, which you may not be able to dispose of for 40 years if you keep them;[5]
- U.S. Bankruptcy Court documents filed electronically;[6]

Utility

Certain files may have utility to you or your client even after 10 years. Before destroying a file, consider whether it:

[3] *See* OSB Formal Ethics Op No 2016-191.

[4] *See* UTCR 21.120(1).

[5] *See* ORS 112.815.

[6] *See* Oregon LBR 5005-4(e) – Retention of Original Document.

- Contains research, motions, notes, or other materials that are not saved in a separate location and that you may wish to build upon, refer to, or reuse; or
- Could be useful to your client or future counsel because of ongoing matters like appeal, retrial, post-conviction relief, or habeas proceedings.

CLOSING, STORING, AND DESTROYING FILES

Once you cease work on a client's matter, you are ready to: (1) close the file by gathering pertinent materials, addressing consent to destruction, determining whether further action is required, and setting a destruction date; (2) store the file in a secure, organized fashion that lets you easily access and review it before destruction; and (3) destroy the file on the chosen date.

Closing the File

One important aspect of closing the file is gathering all materials that belong in it and putting them together. OSB Formal Ethics Op No 2017-192 defines "client file" broadly to include correspondence, records, electronic documents, email, text messages, and more. Because of its broad definition, assembling the client file may require you to gather information from paper documents as well as electronic data from servers, the Internet, desktop hard drives, laptop hard drives, external hard drives, mobile devices, cloud storage providers, or other media.[7]

Next, if you wish to avoid the predicament described under "Fee Agreement and Client Consent" (above), you could take the following steps if you haven't taken them already: (1) provide a complete copy of the file to your client (rather than awaiting a request, which may come at a much later and less convenient time); or (2) obtain the client's consent to destroy the file at a future date. If you take these steps, be sure to document the fact.

Finally, closing is an ideal time to: (1) return or segregate specific documents and originals that you do not wish to destroy (*see* "Specific Documents and Originals," above); (2) review the file for loose ends (e.g., additional work, conflict system update, final billing, withdrawal motion or notice of termination);[8] and (3) establish and calendar a destruction date.

Storing the File

Security is a key consideration for your file storage system whether you decide to store files in paper format, electronic format, or a blend of both. You have a duty to store files in a manner that safeguards client property and maintains confidentiality (*see* footnote 3). These considerations underlie your duty to evaluate a third party if you plan to store files on its server (i.e., in "the cloud").[9] Depending on file content and your storage method, laws may require you to employ heightened security measures and provide notice of unauthorized access. For

---

[7] *See* "Checklist for Scanning Client Files" at https://www.osbplf.org/ > Practice Management > Forms > View Forms by Category > Paperless Office and Cloud Computing.

[8] *See* "File Closing Checklist" at https://www.osbplf.org/ > Practice Management > Forms > View Forms by Category > File Management.

[9] *See* OSB Formal Ethics Op No 2011-188.

example, files containing health information may subject you to HIPAA,[10] while files containing consumer information may subject you to the Oregon Consumer Identity Theft Protection Act (OCITPA).[11] It is incumbent upon you to determine applicable law and use a storage method that satisfies your security obligations. You may need to consult with an information technology expert or specialist within the applicable area of law.

In terms of organization, you may wish to store closed files in a way that makes them easy to access and review prior to destruction. A simple method is to store files by the year in which you ceased work on the case and then review them at the end of your established retention period (e.g., 10 years). For example, label a physical box or digital folder with "2019," fill it with files closed in 2019, and begin a final review in 2029.

A final review consists of checking files for anything you would rather keep or return than destroy. For anything you wish to store on a long-term or permanent basis, you could use a "long-term storage" or "do not destroy" label. You are not required to destroy files, but file destruction relieves you of costs and logistical issues related to long-term storage.

Destroying the File

After you make a final review of the file and decide to destroy it, you are ready to select the means of disposal. Your duty to maintain confidentiality applies to the disposal process.[12] Like the file storage process, file destruction may implicate laws requiring specific methodology. Under OCITPA, the obligation to protect information during disposal could be satisfied by "burning, pulverizing, shredding, or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed" (or by contracting with a party who can).[13] ORS 646A.622(2)(d)(C)(iv) to 646A.622(3).

Note that destroying an electronic file is more complicated than destroying a paper file. This is due not only to the difficulty of deleting electronic data but also to the number of locations that may house your client's electronic data. Keep in mind that: (1) if you store a file on your own hardware, you may need to use specialized software or physical obliteration to destroy the electronic data; and (2) if you store a file in the cloud, you may or may not be able to destroy electronic data on your storage provider's server.[14] The difficulty of destroying electronic data is a factor to consider in devising your file storage system, especially if you plan to use the cloud.

An inventory is a simple means of recording which files were destroyed, the dates of destruction, and whether clients consented to destruction. You may wish to keep proof of consent along with the inventory in case there is a dispute as to whether consent was provided.

---

[10] *See* Kelly T. Hagan, "Business Associate, Esq.: HIPAA's New Normal," *In Brief* (September 2013), *and* Kelly T. Hagan, "The HIPAA Compliance Process," *In Brief* (May 2014).

[11] *See* ORS 646A.622 to 646A.628 *and* Kimi Nam, "Protect Client Information from Identity Theft," *In Brief* (August 2008).

[12] *See* OSB Formal Ethics Op No 2005-141.

[13] Visit http://www.naidonline.org/ for more information.

[14] *See* Hong Dao, "Unwanted Data: How to Properly Destroy Data in Hardware," *In Brief* (April 2017).

FILE RETENTION AND DESTRUCTION GUIDELINES

IMPORTANT NOTICES

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund, except that permission is granted for Oregon lawyers to use and modify these materials for use in their own practices.