

How Long Should I Keep Closed Client Files?

Disclaimer: This material is intended as only an example which you may use in developing your own form. It is not considered legal advice and as always, you will need to do your own research to make your own conclusions regarding the laws and ethical opinions of your jurisdiction. In no event will ALPS be liable for any direct, indirect, or consequential damages resulting from the use of this material.



Meet Mark:

Mark Bassingthwaighte, Esq., serves as Risk Manager at [ALPS](#), a leading provider of insurance and risk management solutions for law firms. Since joining ALPS in 1998, Mark has worked with more than 1200 law firms nationwide, helping attorneys identify vulnerabilities, strengthen firm operations, and reduce professional liability risks.

He has presented over 700 continuing legal education (CLE) seminars across the United States and written extensively on the topics of risk management, legal ethics, and cyber security.

A trusted voice in the legal community, Mark is a member of the State Bar of Montana and the American Bar Association and holds a J.D. from Drake University Law School. His mission is to help attorneys build safer, more resilient practices in a rapidly evolving legal environment.



Contact Information:

Mark Bassingthwaighte, Esq.
ALPS Insurance Agency
111 N. Higgins Ave, Suite 600
Missoula, MT 59802

(T) 800.367.2577 | (D) 406.523.3859

mbass@alpsinsurance.com

www.alpsinsurance.com



As a risk manager for a national legal malpractice insurance company, this is the one question I have been asked more than any other. Often the reason why is because an attorney or law firm is tired of paying the costs associated with storing all their closed files, and they're hoping to hear it's okay to get rid of most of them.

Unfortunately, the answer isn't as straightforward as one might hope because the answer is it depends. Start with a baseline assumption of seven years and go from there. Of course, once any destruction date arrives, make sure you follow through with a proper file destruction process.

File Retention:

General Retention Guidelines: Why Seven Years Is a Reasonable Baseline:

Because guidelines and ethical opinions differ across jurisdictions, you should always check with the authorities where you practice. That said, most recommendations fall in the seven-to-ten-year range. Speaking as a risk manager, I lean toward the shorter end of that window. My reason is this. The statute of limitations on malpractice under contract law is often five or six years, and I add one more year just to play it safe. Thus, seven years is generally sufficient for most matters. If seven years have not yet passed, the safest answer is simple: keep the file.

I can share that over the years I have encountered a few firms that take a far more aggressive approach. Some of these firms went so far as to destroy all files well within the first-year post closure. I strongly advise you against this. If a malpractice claim ever arises, you will have no file to defend yourself with, which is a position you never want to be in. Trust me on that one.

Why Some Files Must Be Kept Longer Than Your Standard Retention Period:

Even after your seven-year (or up to ten-year) retention period has passed, you may still be unable to destroy certain files. As with most rules, there are exceptions that require additional storage time. These include, but are not limited to:

- Files where the malpractice statute of limitations has not yet run (and remember the doctrine of continuous representation can toll these statutes).



- Files involving a client who was, and still is, a minor.
- Estate planning files for clients who are still alive.
- Files containing agreements that have not yet been executed or fully paid off.
- Files establishing the tax basis of client assets.
- Adoption files.
- Support or custody files with continuing obligations.
- Files with renewable judgments.
- Corporate books and records for active client entities.
- Files for clients convicted of a capital crime.
- Files involving certain “problem clients.”

In a perfect world, every file would have been assigned a destruction date, or at least a review date, when it was first closed. If that didn't happen, use these exceptions to guide your decisions now.

File Destruction:

Always Conduct a Final Review Before Destroying Any File:

Before destroying any given file, conduct one final review. This step prevents premature destruction and ensures that documents that should not be destroyed are preserved.

When the file was originally closed, you should have separated and returned all original documents belonging to the client. If that didn't happen, now is the time to correct it.

During this final review, identify and preserve:

- Documents that clearly or probably belong to the client.
- All original documents.
- Any documents the client may need or reasonably expect you to preserve.
- The file's closure letter.

That closure letter is more important than many lawyers realize because it can help clarify whether a conflict of interest exists later. If closure letters are destroyed, you lose the ability to provide documentation that an inactive client is actually a past client under Rule 1.9, the “Former Client” Rule.



Why You Shouldn't Unilaterally Decide to Destroy Client Files:

To varying degrees in many jurisdictions, the file is considered client property. This means clients should be made aware of and give their permission to have their property destroyed. If clients were never informed of your file retention and destruction policy when their file was closed, try to contact them now to see if they want their file. Some lawyers try sending letters to the last known address, but with older files this effort often yields little success. To avoid having to deal with this problem, many firms now include file-retention language in their engagement letters and closure letters, at least on a going forward basis. If you wish to adopt a similar approach, consider including the following sample language in your closure letters.

"I have enclosed your original documents as I no longer need to keep them, and I thought you would want them for your records. It is our firm's practice to destroy files [number of] years after we close them. If you would like us to return your file to you [number of] years from now instead of destroying it, please send me a note to that effect within the next thirty days so that we can segregate your file from all our other files and accommodate your request. You will need to be responsible for keeping us informed as to how to reach you should your contact information ever change."

If you find yourself needing to send past clients a letter years after closing their files, you might consider designing a letter based upon this sample language.

Our policy is to destroy files [number of] years after they are closed. We have retained your file for that period of time and are now preparing to have it destroyed. If your desire is to have our firm continue to store it or see that it is returned to you, you must send me a letter telling us of your desire and this must be done no later than ten days after the date you receive this letter.

Protect Confidentiality to the Very End:

Once you determine which files can be destroyed, make sure you follow through and see that they are properly destroyed. Never just toss boxes upon boxes of files in a dumpster behind the office or drop them off at the local landfill! Client files must be incinerated or shredded because your obligation to preserve and maintain client confidences doesn't end even though your file retention period has.



Document the Final Disposition of Every File:

And finally, create and maintain an inventory of the final disposition of all files. At a minimum, track:

- Client name
- File matter
- Method of disposition (destroyed or returned)
- Date of disposition

This record will prove useful should any questions arise years later.

Why You Don't Get a Pass Just Because Digital Storage is Inexpensive:

One final thought. I have found that some firms try to avoid the headache of having to work through much of the above by choosing to keep digital copies of client files indefinitely because virtual storage is inexpensive. They scan the file, destroy the hard copy, and keep the digital version.

On the surface, this may seem like a problem has been solved, but it really hasn't. Again, your ethical obligations remain the same regardless. For example, as you replace or upgrade hardware and storage devices, all client data on those devices should still be reviewed to ensure nothing is prematurely lost. Similarly, you can't simply abandon a cloud storage account or recycle or donate old devices without destroying all digital client files that were stored there. In other words, the issues remain the same whether your files are paper or digital because there is no digital storage exception in the Rules of Professional Conduct.