FILE RETENTION AND DESTRUCTION

Most client files (whether paper or electronic) should be kept for a minimum of 2 years after the client may have suffered some damage as a result of the lawyer's conduct, to ensure the file will be available to defend you against malpractice claims. Files that should be kept longer may include:

1. Cases involving a minor who is still a minor;
2. Estate plans for a client who is still alive after the work is performed;
3. Contracts or other agreements that are active or are still being paid off;
4. Cases in which a judgment should be renewed;
5. Files establishing a tax basis in property;
6. Criminal law – keep for two years after the client is released or exonerated
7. Support and custody files in which the children are minors or the support obligation continues;
8. Corporate books and records;
9. Adoption files;
10. Intellectual property files; and
11. Files of problem clients.

When closing your file, return original documents to clients or transfer them to their new attorneys. Be sure to get a receipt for the property and keep the receipt in your paper or electronic file.

The first step in the file retention process begins when you are retained by the client. Your fee agreement should notify the client that you will be destroying the file and should specify when that will occur. The client's signature on the fee agreement will provide consent to destroy the file. In addition, your engagement letter should remind clients that you will be destroying the file after certain conditions are met.

The second step in the file retention process is when the file is closed. When closing the file, establish a destruction date and calendar that date. If you have not already obtained the client's permission to destroy the file (in the fee agreement or engagement letter), you can get written permission when you close the file or you can make sure that the client has a complete copy of the file. This includes all pleadings, correspondence, and other papers and documents necessary for the client to construct a file for personal use. If you choose the latter alternative, be sure to document that the client has a complete file. This means that the paper or electronic file you have in your office is yours (and can be destroyed without permission) and the file the client has is the client's copy. File closing is also a good time to advise clients of your firm's policy on retrieving and providing file material once a matter is closed.

The final step in the file retention process involves reviewing the firm's electronic records for client-related material. Electronic data may reside on network servers, Web servers, Extranets, Intranets, the Internet, local hard drives of firm PCs, laptops, home computers, zip drives, disks, portable memory sticks and flash drives, PDAs and Smartphones, or other media. Examples include e-mail communications, instant messages, electronic faxes, digitized evidence, word processing, or other documents generated during the course of the case. Review these sources to

ensure that the client file is complete. If these documents exist only in electronic form, you may choose to store them electronically or print them out and place them in the appropriate location in the client's file.

If you possess personal health information of clients or others within the meaning of the Health Insurance Portability and Accountability Act (HIPAA), you are obligated to conduct a risk analysis and take proper steps to secure your records. Failure to do so can result in civil penalties.

The retention policy for electronic data should be consistent with the retention policy for paper files.

Organization and Destruction of Closed Files

Keep a permanent inventory of files you destroy and the destruction dates. Before destroying any client file, review it carefully. Some files need to be kept longer, as noted above. Others may contain conflict information that needs to be added to your conflict database or original documents of the client, which should never be destroyed. Always retain proof of the client's consent to destroy the file. This is easily done by including the client's consent in your fee agreement or engagement letter and retaining the letters with your inventory of destroyed files. Follow the same guidelines when evaluating whether to destroy electronic records.

On June 1, 2005, a new law took effect that regulates the disposal of consumer information. The Fair and Accurate Credit Transaction Act (FACTA) Disposal Rule (the Rule) requires any person who maintains or possesses "consumer information" for a business purpose to properly dispose of such information by taking "reasonable measures" to protect against unauthorized access to or use of the information in connection with its disposal. The Rule defines "consumer information" as any information about an individual that is in or derived from a consumer report. Although the Rule doesn't specifically refer to lawyers, it may be interpreted to apply to lawyers, and the practices specified in the Rule would safeguard clients' confidential information. "Reasonable measures" for disposal under the Rule are (1) burning, pulverizing, or shredding physical documents; (2) erasing or physically destroying electronic media; and (3) entering into a contract with a document disposal service.
Permanent destruction of electronic data requires special expertise.
