PLF *in*BRIEF

ISSUE 136 | JANUARY 2019

Malpractice Prevention Education for Oregon Lawyers

LAW PRACTICE

File Retention and Destruction Procedures: Additional Safeguards to Protect Your Firm from Lost or Exposed Client Data

By Rachel Edwards, PLF Practice Management Advisor

File retention and destruction procedures are one potential safeguard to help reduce your firm's risk of data loss or exposure from a cyberattack. They can also protect your firm from non-cyber incidents, such as a natural disaster or loss due to stolen or misplaced files. So whether you have all paper files, all electronic files, or a combination, creating file retention and destruction procedures is an important step towards protecting your firm from lost or exposed client data.

The procedures should encompass not only retention and destruction of client files after closure of the matter, but also retention procedures while the matter is open, such as handling and storage of incoming documents. This allows for improved file organization and consistency, increasing your firm's efficiency when handling files while open and when preparing files for storage upon closure of the matter.

Before creating file retention and destruction procedures, it is important to understand your obligations and the reasoning behind our recommendations for handling client files. Lawyers have a right to retain a copy of their client files. Generally, the PLF recommends that you keep client files for a minimum of 10 years after closure of the matter to ensure the file will be available to defend you against a malpractice claim. This is based on statute of ultimate repose. ORS 12.115(1). You may need to keep some files longer than 10 years. You may also be required to retain certain original documents. See our "File Retention and Destruction Guidelines" for additional information, available at *www.osbplf.org > Practice Management > Forms > Category > File Management*.

Lawyers must also take reasonable steps to prevent the inadvertent disclosure of, or unauthorized access to, client information. This is both while the file is open and after closure of the matter. ORPC 1.6(c). As for storage of client data electronically, lawyers may use electronic systems to store client files as long as they take reasonable steps to ensure the security and availability of electronic documents during appropriate time periods, including following the completion of the matter or termination of the representation. OSB Formal Ethics Opinion 2016-191.

Each firm has different needs and circumstances when it comes to file retention and destruction. Listed below are general tips for developing procedures that fit your firm's needs:

- **Create a written procedures manual** – A

written procedures manual encompassing all of the firm's policies regarding file retention and destruction allows for inclusion of all procedures in one location. The manual should comply with your ethical and legal obligations and set forth the procedures for retention and destruction of both electronic and paper data. See our practice aid titled "Creating an Office Procedures Manual" for helpful information and sample language, available at *www.osbplf.org > Practice Management > Forms > Category > Office Manuals*.

Below are factors to consider when drafting your procedures manual:

- *Client file defined* – In accordance with OSB Formal Ethics Opinion 2017-192, a client file is the "sum total of all documents, records or information (either in paper or electronic form) that the lawyer maintained in the exercise of professional judgment for use in representing the client." Include language in the manual specifically addressing what types of documents must be stored as part of the client file, and in what format. Remember this includes emails and text messages, with limited exceptions. Include procedures for how these types of electronic documents will be stored as part of the client file.

- *Client consent* – It is also recommended that attorneys enter into reasonable agreements with clients regarding how the lawyer will maintain the file both during and after representation. This includes client consent to retain, destroy, and return files as part of the written fee agreement. See our sample engagement letters and fee agreements for specific language at *www.osbplf.org > Practice Management > Forms > Engagement Letters and Fee Agreements*.

- *File organization* – Develop a procedure for how files will be organized in both paper and electronic form. For example, consider setting up a template for each type of file upon opening, specifying the name of the file, file subfolders, and naming conventions for each type of document.

- *Handling of incoming documents* – Include procedures regarding how to handle incoming documents. For example, who opens and processes incoming mail? Are paper documents scanned and shredded? If so, by whom and where will the scanned documents be stored? Are emails stored electronically? If so, what is the procedure for storage of the emails while the case is open and after closure of the file?

- *File storage* – Develop procedures regarding where the files are being stored while open and after closure. For example, do you want to maintain the file electronically from the start, utilize a combination of paper and electronic, paper both while open and after closure, or paper while open and then scan into electronic form for storage after closure? There are a multitude of options. Find what works best for your firm. Before drafting file storage procedures, first consider what steps it will take to accomplish these goals. If you want to maintain electronic files, develop and implement procedures making it easier to do so, such as requesting that clients provide documents to you in electronic form if possible. Also consider whether maintaining a file in electronic form may be difficult for particular clients if they request a copy of their file. For example, if a client has no access to a computer, an electronic file may create a hardship for the client.

- *File backup* – Be sure to include procedures for properly backing up your data. Backup is the process of creating and keeping a copy of your files in a location different from where they are stored. See our practice aid titled "How to Backup Your Computer" for additional information, available at *www.osbplf.org > Practice Management > Forms > Category > Hardware and Software*.

- *File security* – You must take reasonable steps to ensure the security and availability of client files during the representation and after closure of the matter. OSB Formal Opinion 2016-191. Determine appropriate methods for storage of files, paper and electronic, in

accordance with your duties to maintain client confidentiality. For example, consider the use of password protection, encryption, or some other type of security for protecting electronic documents. Paper files need to be stored in a locked cabinet or storage facility, protected from environmental hazards such as fire and water. See our practice aid titled "Protecting Yourself and Your Law Firm from Data Breach Checklist" for additional information, available at *www.osbplf.org > Practice Management > Forms > Category > Cybersecurity and Data Breach*.

- *File closure* – When you close the file, return all original client documents and property to clients after making copies for storage. If you want to store files electronically, establish and document your storage method. Harddrives or servers are preferred over CDs, DVDs, or USB drives, which are easily misplaced and can become damaged over time. See our practice aid titled "Checklist for Scanning Client Files" for additional information, available at *www.osbplf.org > Practice Management > Forms > Category > Paperless Office and Cloud Computing*. Also develop a tracking system to determine the proper date of destruction for each closed file. It is recommended that you organize closed files by the year in which they were closed. And if you choose to convert paper files to electronic-only after closure of a matter, confirm that doing so will not violate the terms of the retention agreement with the client, and be careful not to destroy paper documents that have intrinsic significance or are valuable originals, such as securities, negotiable instruments, deeds, and wills. OSB Formal Ethics Opinion 2016-191.

- *File destruction* – Be sure files are properly destroyed after being stored for the requisite period of time. If you have paper files, reasonable measures for destruction include shredding, pulverizing, or burning. Proper destruction of electronic data can require special expertise. For more information, see our inPractice article titled "Unwanted Data: How to Properly Destroy Data in Hardware." Retain a permanent inventory of files destroyed showing the matter and the destruction date. Also retain proof of the client's consent to destroy the file. This can easily be done by including the client's consent in your fee agreement or engagement letter and retaining those documents with your inventory of destroyed files. Allow your staff to assist in retention and destruction, but a managing attorney should review and approve before any files are destroyed.

- **Mandate employee training and cooperation** – Disseminate the procedures manual to all firm members and require everyone to sign an affirmation of understanding and agreement of compliance.

- **Review the procedures manual on a regular basis** – Review your file retention and destruction procedures manual on a regular basis, at least annually.

Even if you don't necessarily have the time or resources to create a formal procedures manual, the act of simply writing down your basic file retention and destruction procedures can increase efficiency and reduce the risk of loss or exposure of your clients' data.