Model Case Closing & File Retention and Destruction Policy

[ORGANIZATION] will store client files for a period of at least ten years, to be calculated from the date work ceases on the matter. Once [ORGANIZATION] ceases work on a matter, [ORGANIZATION] shall:

1. Close the file:
    a. Send disengagement letter to the client;
    b. Go through the file to identify original documents, remove multiple copies of the same documents, and tie up loose ends (e.g., complete additional work, ensure disengagement letter or notice of termination sent to client, confirm withdrawal motion was filed and granted, if applicable);
    c. Promptly return all original documents to the client;
    d. Ensure the file is complete by gathering all documents in physical and electronic formats stored in different locations (e.g., server, cloud storage provider, email, computer hard drive, mobile device, or other media) and save them to the client file.

2. Store the file:
    a. Determine whether the file contains health information subject to the Health Insurance Portability and Accountability Act and/or consumer information subject to the Oregon Consumer Identity Theft Protection Act, and, if the file contains such information, review the applicable laws and identify a storage method that satisfies them;
    b. Store the file for at least ten years from the date [ORGANIZATION] ceases work on a client's matter in a manner that safeguards client property and maintains confidentiality. [ORGANIZATION] may store client files electronically using a third-party vendor only after evaluating

that vendor to (1) assure that the vendor complies with industry standards relating to confidentiality and security; (2) determine how the vendor stores its data and metadata; and (3) assess whether the vendor's practices comply with [ORGANIZATION's] duties under the Oregon Rules of Professional Conduct (ORPC), including the duty to reliably secure client data and keep information confidential. Should [ORGANIZATION] hire a third-party vendor for the electronic storage of client files, it shall inform the vendor of its duties to safeguard client property and maintain confidentiality under the ORPC and enter a service agreement requiring the vendor to preserve the confidentiality and security of the client file and to notify [ORGANIZATION] of any nonauthorized third-party access to the materials. [ORGANIZATION] shall review the vendor's practices at least annually to assure that those practices continue to sufficiently safeguard client property and confidentiality given advances in technology. Should [ORGANIZATION] determine that it can no longer meet its duties under the ORPC through reliance on the vendor, it shall promptly take corrective action, including, if necessary, ceasing any agreement with the vendor, hiring a new vendor, and/or storing client files in-house.

c. Organize all closed files by the year in which they are closed.

3. Destroy the file:
    a. Securely dispose of all physical documents by shredding;
    b. Permanently erase or destroy all electronic or digital documents;
    c. Keep a permanent inventory of files destroyed and destruction dates.