ALPS
Practice Management Pointers

Don't Overlook File Storage Concerns

Mark Bassingthwaighte, Esq.
mbass@alpsnet.com

Firm administrators and attorneys alike often seek risk management advice regarding the various and sometimes convoluted issues that arise when trying to establish a file retention policy. While I applaud the effort of those who successfully implement such a policy, don't overlook the related issue of proper storage practices. This is because even the best laid plans may all be for naught if once you go to retrieve a file from storage you end up finding the paper file partially destroyed or the digital file inaccessible due to a long-term storage misstep.

Allow me to share a few examples that highlight the concerns. I have visited a number of smaller firms over the years that have had paper and digital files stored in an unlocked out-building or a business basement with unmonitored outside access and/or common access for all building tenants. One firm even had files stored in a central room literally in a massive pile on the floor that was over my head in height. Imagine trying to find a file that is eight to ten years old in that mess! I have seen files sitting on wet damp concrete floors already in an early state of decay and files stored so densely in attics that floors were literally beginning to buckle under the weight. (That can't be good.) Then there are the firms who have placed files in storage facilities located in a flood plain right beside a river or placed files in personal storage facilities otherwise known as an attorney's garage, home basement, or family cabin where anyone and everyone in the family has access.

Lawyers have ethical duties to act competently to safeguard information relating to the representation of a client from inadvertent and unauthorized disclosure. At a minimum, paper files should be stored under lock and key and digital files password protected and encrypted. Employees of other businesses in the building, non-employee family members, the night cleaning crew, a passerby, or the unscrupulous non-client who wants to dig into old records should never have an opportunity to view a client file. As an aside, once the time for file destruction comes, keep the same rule in mind and follow through with proper file destruction. Don't leave old files in a dumpster until trash day comes or try to recycle or give away computers of any type without having the drives wiped, and yes, both missteps happen.

Files should be catalogued and stored in a manner that will allow you to readily find an old file if and when the need arises because time wasted on trying to find old client files whose whereabouts are unknown is money down the drain. Also, don't overlook the necessity and value of creating an inventory of all original documents or other client property that is to be held long-term and remember to keep a copy of this inventory at a separate and secure location in the event of a disaster. If one hundred original client wills

were to eventually end up destroyed in a fire, the ability to determine whose wills were destroyed will prove extremely valuable as you seek to remedy the situation.

Proper storage would also dictate that files be stored in a fashion that minimizes the risk of decay or destruction. If file boxes must be kept on a concrete floor, place them on shelving of some sort in order to keep the boxes at least an inch or two off the floor. If the storage space is within a flood plain, store the files on the upper floors of the building if this is an option. Additional steps should be taken to protect original documents such as wills, deeds, or abstracts if they are going to be stored for extended periods of time. Because these types of materials are client property, they should be kept in a fireproof safe, a safety deposit box, or even a firm vault. Depending upon the number of documents stored long-term, an additional thought is to store these documents in Tupperware if flooding is a concern because safes are not waterproof.

Finally, make certain that you address the somewhat unique storage issues that arise with digital files. As with paper files, these files should be stored in a manner that will allow any specific file to be easily found and readily accessed years later. Heaven forbid over the years a firm goes through several hardware and software upgrades and their practice over the years was to periodically dump files in native format to CDs, tape, or disk without a record of what went where. The eventual search for a file and the effort to actually access the data could prove to be a costly undertaking. Try finding a 3 ½ inch floppy drive, a copy of Word 5.0, and a computer that can run this stuff today. I can assure you, that wouldn't be fun. A better alternative would be to develop standardized file naming and storage protocols coupled with defined long term storage format that is likely to be accessible years from now such as PDF.

As with paper files, electronic storage media should be maintained under conditions that seek to prevent unintentional damage and unauthorized access. Throwing unencrypted disks that are not password protected into a box in a closet at home doesn't cut it. Once again, Tupperware and a fireproof safe rated for the storage of electronic media or even a secure cloud-based storage process can do wonders in this regard. Just remember to password protect and encrypt all digital data that will be stored in the cloud or on hardware that will travel off site.

Truth be told, the advice shared here is nothing more than a little common sense. The real problem is that it is too easy to overlook these issues in a desire to get to the next active matter. Once matters close, files can quickly move to the out-of-sight, out-of-mind category and the few final administrative/storage steps can too easily move into that "we'll get to it when we can" to-do list. I am just gently trying to suggest that a little effort up front truly can prevent a major headache down the road. I have personally lived through a flood, a hurricane, and a data breach. Trust me; it's worth the effort.

Risk Management Questions?

Mark Bassingthwaighte, Esq. is the Risk Manager for ALPS Property & Casualty Insurance Company. He is available to answer risk management questions and can be reached at 1-800-367-2577 or mbass@alpsnet.com.

Disclaimer:

ALPS presents this publication or document as general information only. While ALPS strives to provide accurate information, ALPS expressly disclaims any guarantee or assurance that this publication or document is complete or accurate. Therefore, in providing this publication or document, ALPS expressly disclaims any warranty of any kind, whether express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Further, by making this publication or document available, ALPS is not rendering legal or other professional advice or services and this publication or document should not be relied upon as a substitute for such legal or other professional advice or services. ALPS warns that this publication or document should not be used or relied upon as a basis for any decision or action that may affect your professional practice, business or personal affairs. Instead, ALPS highly recommend that you consult an attorney or other professional before making any decisions regarding the subject matter of this publication or document. ALPS Corporation, as well as any of its subsidiaries, affiliates and related entities shall not be responsible for any loss or damage sustained by any person who uses or relies upon the publication or document presented herein.