MAINTAINING APPROPRIATE FILE AND RECORDS MANAGEMENT SYSTEMS

PMBR Committee Working Group #5

Client Files	Yes	No
Do you have a standardized filing system for all client files?		
Do you have a file-naming convention for paper and electronic files? • Do you have a policy to ensure electronic and paper copies of files are consistent? • Do you have policy to ensure all email or text communication with your client is copied to your paper/electronic files?		
Do you have a policy for handling originals received from clients? • Do you log or document receipt? • Do you scan and return originals or retain them?		
Do you have a file retention policy that complies with Colo. RPC 1.16A? • Does your policy also account for your obligations under other rules (e.g., Colo. RPC 1.15D; C.R.C.P. 121 § 1-26(7))?		

FILE MANAGEMENT, SECURITY, AND RETENTION

File Security	Yes	No
Are your client files secure? • Do you have a system in place for tracking or limiting access to the files by members of your staff? • Is your office secure? ▪ Is your office locked? ▪ Are your paper files kept in a secured cabinet or are a within your office? ▪ Are your files protected from flood/fire/vermin? ▪ Do you share office space with other attorneys or professionals not in your firm? ▪ Do other third parties have access to your work area, e.g. landlords, maintenance staff, cleaning staff?		

FILE MANAGEMENT, SECURITY, AND RETENTION

Cyber Security	Yes	No
Do you maintain electronic copies of files on a cloud-based system? • Have you ensured that your system meets the requisite encryption standards to ensure security of client information?		
Do you backup copies of your electronic files? • How often are files backed up? • Are back-ups maintained onsite? • Do you routinely test your back-ups to ensure files can be restored?		
Can you access client files remotely?		
Do you have password strength policies for all users who have access to electronic files?		
Do you have a firewall in place for your office system?		
Do you have anti-virus software for your office system?		
Do you process, store or transmit client credit card information? • If so, are you in compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirements?		
Do you have a plan in place in the event your electronic file security is breeched? • Is there a system in place for notice to clients in the event of a breech? • Is there a plan for remediation?		

FILE MANAGEMENT, SECURITY, AND RETENTION

Email	Yes	No
Do you have email use policies for employees and staff?		
Do you have encryption policies in place to address transmission via email of medical records, financial records, or other highly confidential materials?		

FILE MANAGEMENT, SECURITY, AND RETENTION

Training	Yes	No
Do you have a training system in place for employees and staff with respect to file systems, computer usage, and email usage? Is the training for new hires only? Do you require long-term employees to go through training according to any regular schedule?		

FILE MANAGEMENT, SECURITY, AND RETENTION

Disaster Recovery	Yes	No
Do you have a disaster recovery plan in place for paper files?		
Do you have a disaster recovery plan in place for electronic files?		

FILE MANAGEMENT, SECURITY, AND RETENTION