File Retention, Destruction and Security Policy

NextChapter BK, Inc.

Last Modified May 17, 2017

This policy is set forth to memorialize the processes and procedures for retention, review and destruction of client files following termination of representation for NextChapter BK, Inc. ("Company"). It is intended to ensure the Company's compliance with applicable legal and ethical obligations to former clients.

File Closing Procedures

Following termination of use for any reason, including withdrawal of the Company, termination at attorney's request, or conclusion of the matter for which the Company was engaged, the attorney's client file shall be closed. Closing of the file shall be performed by the Company's software engineers and entails removal of the information from the database in its entirety.

At the time of file closing, extraneous documents may be discarded at the Company's discretion. Such extraneous documents may include notes, drafts, extra copies of documents, hard copies of electronically-available documents.

Storage of Retained Files

During the file retention period, all electronic files shall be housed on the Company's secure servers as defined below in the Security Policy.

Time Period for Storage of Files

All files shall be maintained for a minimum period of 7 years or until directed to be removed by attorney's request.

Security Policy

ENCRYPTION
NextChapter uses heavy encryption to ensure that data cannot be read if a client uses a public network. All data is transmitted over 256-bit encrypted connections and stored in an encrypted format on physically secured servers with unique session encryption keys.

VULNERABILITY SCANS
NextChapter is audited daily by Symantec SSL and McAfee SECURE to help ensure your data is protected from security vulnerabilities and other online threats. McAfee SECURE thoroughly inspects site for malware, viruses, phishing attacks, and other malicious activities to ensure that it's safe for you and your client's data.

DATA BACKUP
We have multiple backup systems in place to protect your data, governed by the following policies: All backups are replicated to at least 2 physical datacenters. All backup systems are tested biweekly. Backups occur once daily at a minimum. Your practice's data is 100% accessible and protected.

PHYSICAL STORAGE
NextChapter uses Heroku's secure storage facilities for data storage. These facilities are distributed around the globe, making it extremely difficult for an adversary to locate the position of your data. Every storage center is highly secured by military grade perimeter control, state-of-the art electronic surveillance and 24-7 monitoring by trained security personnel.

PROTECTED BILLING INFORMATION
All credit card transactions are processed using secure encryption—the same level of encryption used by leading banks. Card information is transmitted, stored, and processed securely on a PCI-Compliant network. Learn more about Stripe: https://stripe.com/us/features#seamless-security