NJSBA PRACTICEHQ Affinity CONSULTING

TOOLS AND PROTOCOLS TO PROTECT CLIENT DATA

Client confidentiality is not just good practice; it's an ethical obligation. ABA Model Rule 1.6(c) requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[1] Comment 18 to that rule lists the factors that determine what counts as "reasonable": the sensitivity of the information, the likelihood of disclosure if safeguards aren't adopted, the cost and difficulty of implementing safeguards, and how much those safeguards would interfere with the lawyer's ability to represent the client.[2]

Encryption sits at the center of that analysis. This guide covers where encryption matters most for a small or solo firm: the devices your team uses, the cloud services where client files reside, and the email and portals that carry confidential client information.

ENCRYPTION DEFINED

Encryption converts readable information into coded data that can be opened only with the correct key or credential. It can protect files and devices while data is stored and protect information while it travels across a network.

WHY ENCRYPTION MATTERS

Law firms remain attractive ransomware targets because they hold valuable and sensitive client information. One industry report identified 455 publicly named legal-sector victims in 2025, up from 196 in 2024.[3] Professional services accounted for 21 percent of observed ransomware incidents in the first quarter of 2026.[4] Compromised credentials were an initial access vector in 22 percent of the breaches reviewed in Verizon's 2025 Data Breach Investigations Report.[5] Many successful attacks exploit familiar weaknesses, including stolen credentials, unmanaged devices, unpatched software, and inadequate monitoring.

Malpractice carriers have noticed. Insurers increasingly ask about multi-factor authentication, email encryption, and document retention controls before renewing cyber policies. Encryption is no longer a nice-to-have; it's part of the underwriting conversation.

DEVICES: LAWYERS MUST ENCRYPT LAPTOPS, TABLETS, AND PHONES

COMPUTER ENCRYPTION

If you have a laptop, someone may steal it, or you might misplace or otherwise lose it. You must encrypt the machine if you have confidential client information on the computer. When the computer is powered off or properly locked, full-disk encryption makes the information on its drive unreadable without the required key or credential, including when the drive is removed and installed in another computer.

---

[1] American Bar Association, Model Rules of Professional Conduct, Rule 1.6(c).

[2] American Bar Association, Model Rules of Professional Conduct, Rule 1.6, Comment 18.

[3] GuidePoint Security, *2026 Ransomware & Cyber Threat Report* 21 (2026), https://www.guidepointsecurity.com/wp-content/uploads/2026/01/GRIT-2026-Ransomware-and-Cyber-Threat-Report.pdf.

[4] Beazley Security, *Quarterly Threat Report: First Quarter, 2026*, under "Ransomware Impact Analysis by Sector" (2026), https://beazley.security/insights/quarterly-threat-report-first-quarter-2026.

[5] Philippe Langlois, *Additional 2025 DBIR Research on Credential Stuffing*, Verizon Business, https://www.verizon.com/business/resources/articles/credential-stuffing-attacks-2025-dbir-research/ (last visited Sept. 22, 2026).

For laptops and desktops, stick with the encryption built into the operating system:

- BitLocker – included for free with Windows 11 Pro. Some qualifying devices enable Device Encryption automatically, but the firm should verify the encryption status rather than assume it is active. Standardizing on Windows Pro or Enterprise makes encryption and centralized management easier.

- FileVault – included for free with macOS (for use on Apple Macs). FileVault encrypts the startup volume, and a device-management service can require it, store the recovery key, prevent users from turning it off, and rotate the key when necessary.

Because BitLocker and FileVault are integrated with their operating systems, they are usually the simplest options to deploy, update, and manage. They are included with supported editions of Windows and macOS rather than licensed as separate encryption products. Third-party alternatives such as WinMagic SecureDoc remain available for organizations that need centralized policy management across Windows, macOS, and Linux devices. WinMagic currently identifies FIPS 140-3 validated cryptographic modules for those platforms.[6] But if the person managing IT at your firm is also doing legal work, don't add that complexity; BitLocker or FileVault is enough.

EXTERNAL DRIVES AND USB STICKS

Encryption should also cover external drives and USB media that store client information. A simpler policy is often better: prohibit removable storage unless the firm has approved the device, encrypted it, and recorded who is responsible for it. Before a computer, external drive, or USB stick leaves service, confirm that client data has been securely erased under the firm's disposal procedure.

SMARTPHONES

Smartphones and tablets remain the easy part. Current iPhones and iPads enable Data Protection when the user sets a passcode. Android devices launched with Android 10 or later must use file-based encryption, but the firm should still require a strong screen-lock credential. As of this writing, you'd have to go out of your way to turn it off.

Current iPhones and iPads use hardware-backed encryption. Setting a passcode activates Apple's Data Protection features, and a longer passcode makes the protection stronger. Face ID and Touch ID make a strong passcode easier to use, but biometrics do not by themselves guarantee that a device is secure. The passcode, software version, lock settings, and management configuration all matter.

Modern Android devices also use encryption. Devices launched with Android 10 or later are required to use file-based encryption, but firms should still choose supported models that receive security updates and require a strong screen lock. Avoid allowing old personal devices to become permanent repositories for client email and documents.

For both platforms, configure a short automatic-lock period, hide sensitive notification previews, and require users to report a missing device immediately. Mobile applications should store as little client data locally as practical. When feasible, use managed applications that can remove firm data without erasing the user's personal information.

MANAGE DEVICES AND RECOVERY KEYS

A small firm needs a reliable inventory of every computer, phone, and tablet that can reach client information. Mobile device management, often called MDM, lets the firm apply security settings, verify encryption, install or remove business applications, and act when a device is lost. Microsoft-oriented firms can use Microsoft Intune, which is included with Microsoft 365 Business Premium. Apple-oriented firms can consider Jamf Now together with Apple Business Manager. A technology provider can manage either platform if the firm does not have in-house staff.

Use management tools to distinguish between a full wipe and a selective removal of firm data. A full Intune wipe restores a managed device to factory settings. A retire or selective-wipe action may be more appropriate for a

[6] WinMagic, "SecureDoc Full Disk Encryption" product documentation, 2026.

personal device because it removes managed accounts and data while leaving personal material in place. Test the chosen process before an emergency and document who may authorize it.

Recovery keys deserve the same care as the encrypted data. Store BitLocker keys in Microsoft Entra ID, Active Directory, or the firm's approved management system. Escrow FileVault keys in the firm's MDM service. Do not leave a recovery key in a laptop bag, save it only in an employee's personal account, or rely on one person to remember where it is. Limit access, log retrieval when the system permits it, rotate a key after use, and periodically test that an authorized administrator can recover a device.

ONLINE DATA: CLOUD STORAGE ENCRYPTION

Of course, the truth of most client data today doesn't live on a laptop. It lives in the cloud, and not all cloud encryption is equal.

Mainstream cloud-storage services such as Dropbox, Google Drive, and Microsoft OneDrive encrypt files at rest and in transit. In their standard configurations, the provider manages the encryption keys.[7] Provider-managed encryption is not the same as client-side or end-to-end encryption. Depending on the service and its controls, the provider may retain the technical ability to decrypt content to operate the service or comply with valid legal process. For most routine firm documents, this level of protection, combined with strong access controls, is adequate.

For genuinely sensitive material, some firms adopt zero-knowledge encryption, where files are encrypted on the device before upload and the provider never holds the key. Services offering client-side or zero-knowledge encryption include Tresorit, Proton Drive, and Sync.com. Review each product's account-recovery design carefully because recovery options, administrator capabilities, and responsibility for lost credentials vary.[8] The tradeoff is that if you lose your password, no one, including the provider, can recover your files.

If your firm uses a legal-specific document management system rather than general-purpose cloud storage, check its certifications rather than taking marketing claims at face value. NetDocuments and iManage publish information about independent audits, security certifications, and encryption at rest and in transit. Available key-management and customer-managed encryption options vary by product and subscription, so confirm them in the vendor's current documentation and contract.[9] [10] Ask any vendor holding client data for the same: SOC 2 Type II report, encryption standard used at rest and in transit, and where the data physically resides.

EMAIL AND DATA IN TRANSIT

Email is the most common way privileged information leaves your firm, and it's the piece most often assumed to be "handled" when it isn't. Microsoft 365 and most major email providers encrypt the connection between mail servers using TLS by default.[11] That protects the message in transit between servers, but it is not the same as encrypting the message itself, and it offers no protection once the message lands in an inbox that someone else can access.

ABA Formal Opinion 477R explains that lawyers generally may transmit client information over the internet when they have made reasonable efforts to prevent inadvertent or unauthorized access. The circumstances may require

---

[7] Priviy, "Encrypted Cloud Storage Services in 2026: Complete Guide to Zero-Knowledge vs At-Rest Encryption," 2026.

[8] Ibid.

[9] NetDocuments, *Legal Data Security and Governance*, https://www.netdocuments.com/solutions/security-data-governance/ (last visited Sept. 22, 2026) (describing annual SOC 2 Type II audits, ISO 27001–series controls, and NetDocuments-managed and customer-managed encryption-key options).

[10] iManage, *iManage Cloud Services Agreement* 34, https://support.imanage.com/worksite/iManage_Cloud_Services_Agreement.pdf (last visited Sept. 22, 2026) (describing encryption at rest and in transit and optional customer-managed encryption keys); iManage, *Seven Considerations for a Modern Corporate Document Management System*, https://go.imanage.com/iManage-7-considerations-for-modern-corp-dms.html (last visited Sept. 22, 2026) (identifying SOC 2, SOC 3, CSA STAR, and ISO 27001 certifications).

[11] Microsoft Learn, "Email Encryption in Microsoft 365," Microsoft, 2026.

additional precautions when the information is especially sensitive or when an agreement or law requires greater protection.[12]

For Microsoft 365 users, two common paths get you there:

- Microsoft Purview Message Encryption, which wraps the message, so the recipient opens it through a portal and authenticates with a Microsoft or Google account or a one-time passcode

- S/MIME, which uses a certificate pair, but requires both sender and recipient to have certificates installed — a heavier lift for solo and small-firm use

Third-party services (Virtru, Zix, Proton Mail Business, among others) offer similar wrapped-message encryption without requiring certificate management, and are worth a look if you send sensitive attachments regularly.

USE CLIENT PORTALS FOR SENSITIVE DOCUMENTS

For highly sensitive documents, a secure client portal is often the better choice because the firm can control access, keep the document out of multiple inboxes, and sometimes revoke or expire a link. Use the portal built into a vetted law practice management or document-sharing platform when it meets the firm's requirements. Confirm the recipient before granting access, use the narrowest permissions available, and remove access when it is no longer needed.

AI AND PROTECTING CLIENT DATA

A prompt, uploaded pleading, transcript, or connected document repository may contain client information. Before staff use an AI system with that information, review it as a data vendor. The firm should know whether prompts and outputs are used to train models, how long the provider keeps them, whether humans may review them, which subprocessors are involved, how deletion works, and what administrative and audit controls are available. Review connectors and plug-ins separately because they can expand what the system can read or where information can go.

OpenAI states that it does not use inputs or outputs from ChatGPT Business, ChatGPT Enterprise, or its API to train models by default. Microsoft states that Microsoft 365 Copilot prompts and responses receive enterprise data protection and are not used to train foundation models. These assurances can support a firm's review, but they do not replace it. The firm still must choose the correct account type, configure retention and sharing, limit access to authorized users, and understand any feature that sends data to another service.

Create a short approved-tools policy. Prohibit client information in consumer AI accounts unless the firm has expressly approved the service and the use. Require users to minimize the information submitted, remove unnecessary identifiers when practical, and check every output before relying on it or sending it to a client, court, or opposing counsel. AI output can be inaccurate or incomplete and must receive appropriate human review. Human review, however, cannot cure an improper disclosure of client information made when the prompt or document was submitted.[13]

VETTING VENDORS

Every cloud tool your firm adopts (*e.g.*, practice management, e-discovery, e-signature, billing) is another place client data sits at rest and moves in transit. Before signing on with a new vendor, ask for the same three things every

---

[12] ABA Standing Comm. on Ethics & Pro. Resp., Formal Op. 477R, *Securing Communication of Protected Client Information* 1, 5–6 (May 22, 2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf.

[13] ABA Standing Comm. on Ethics & Pro. Resp., Formal Op. 512, *Generative Artificial Intelligence Tools* 4, 6–7 (July 29, 2024), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf.

time: their encryption standard at rest (AES-256 is the current baseline), their encryption standard in transit (TLS 1.2 or higher), and a current SOC 2 Type II report or equivalent independent audit.

EVALUATION QUESTIONS

Before approving cloud storage, practice-management software, e-signature tools, or another software-as-a-service product, determine:

- whether data is encrypted at rest and in transit, and which party controls the encryption keys;
- how the service separates customer accounts and controls employee or support access;
- where data is stored, which subprocessors receive it, and what security reports or independent audits are available;
- how the firm can export and delete data, including copies retained after the contract ends;
- what logs, administrative controls, incident notices, and customer-managed key options are available.

Record the decision and review important vendors at renewal or after a material service change. A written review is especially useful when a product holds complete client files or integrates with the firm's email and document systems.

A PRACTICAL MINIMUM STANDARD

- Verify full-disk encryption on every firm computer and require current, encrypted mobile devices.
- Enroll devices in a management system that can enforce settings and support remote lock, wipe, or removal of firm data.
- Store recovery keys in a controlled firm system and test the recovery procedure.
- Approve cloud and software vendors through a written security and data-handling review.
- Use a secure portal or approved message encryption when the information or circumstances require more than ordinary email.
- Allow client information only in approved AI accounts and require human review of every material output.
- Encryption does not stop ransomware or malicious software after an authorized user signs in. Firm computers should therefore use centrally managed endpoint protection that can detect suspicious activity, isolate an affected device, and alert someone responsible for responding. The firm should also document whom to contact and what immediate steps to take when a device or account may be compromised.