

THE ATTORNEY'S GUIDE TO AI & DATA SECURITY: AN ACTIONABLE COMPLIANCE CHECKLIST



As law firms increasingly adopt Artificial Intelligence (AI) to streamline workflows, protecting client confidentiality and firm data is more critical than ever. Passing sensitive legal information through the wrong digital channels can lead to severe ethical and security breaches.

This comprehensive checklist simplifies data management and AI safety into clear, everyday steps to keep your firm secure, compliant, and ahead of the curve.

1



GOLDEN RULES FOR EVERYDAY DATA MANAGEMENT

Before looking at AI, a firm's foundational habits must be locked down. Treat all non-public information as locked files.

- ▶ **Ban Personal Accounts for Work Tasks:** Never use personal emails, personal cloud storage (like personal Google Drive or Dropbox), or unapproved messaging apps to store or send firm or client data.
- ▶ **Enforce "Need-to-Know" Access:** Limit folder and file access only to team members who actively need it to do their jobs.
- ▶ **Use a VPN on Public Wi-Fi:** If working from a coffee shop, airport, or hotel, always turn on a Virtual Private Network (VPN) before accessing or sending any firm data.
- ▶ **Stop Emailing Attachments Directly:** For sensitive documents, do not attach the file directly to an email. Instead, send a secure link to an encrypted folder that requires **Two-Factor Authentication (2FA)** to open.
- ▶ **Password-Protect Critical Files:** If you absolutely must attach a file, encrypt it with a password. Share the password via a separate channel (e.g., a phone call or text), never in the same email.

2

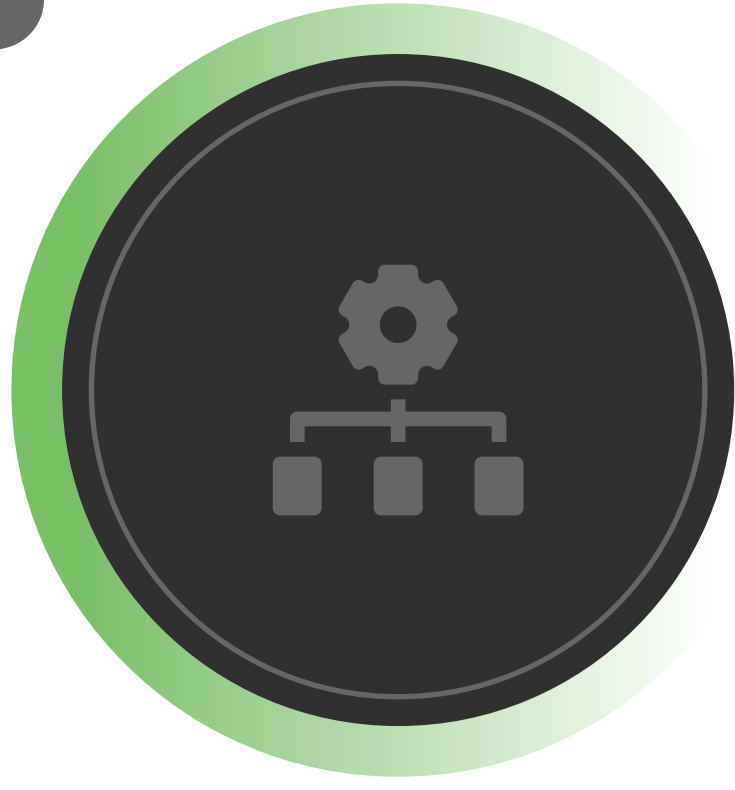


SAFE AI USAGE PRACTICES

AI tools can spark great ideas and speed up drafting, but they can also permanently ingest the data you feed them if they are not configured correctly.

- ▶ **Use Firm-Approved AI Accounts Only:** Never use free, public versions of AI tools (like the free version of ChatGPT or Claude) for work. Only use enterprise accounts provided and managed directly by your law firm.
- ▶ **Turn Off AI "Learning" (Model Training):** Ensure that the privacy settings on all firm AI tools are set to the maximum restriction. Explicitly disable the vendor's ability to use your prompts and data to "train" their AI.
- ▶ **Never Feed Personal or Client Data to AI:** Social security numbers, medical records, financial statements, and highly confidential case strategies should never be typed into a standard AI prompt.
- ▶ **Strip Out Identifying Information:** If you are using AI to analyze a document or help draft a brief, remove all names, addresses, case numbers, and specific identifiers first.
- ▶ **Fact-Check Every Single AI Output:** AI tools are assistants, not digital lawyers. They can hallucinate or confidently invent incorrect case law. Always verify the accuracy of AI-generated insights before using them in practice.

3



DATA CLASSIFICATION: KNOW WHAT TO PROTECT (AND HOW)

Not all data requires the same level of lockdown. Use this simple breakdown to train your team on how to handle different types of information.

- **Sensitive Data**
 - ▶ **What it includes:** Social security numbers, driver's licenses, bank account numbers, medical records, firm financial data, and proprietary software code.
 - ▶ **How to handle it:** Maximize security. Access must require 2FA. Never share it with third parties unless it is a verified, secure vendor (like your firm's primary payroll software). **Never use this data with AI tools.**
- **Private Data**
 - ▶ **What it includes:** Client case files, marketing strategies, internal firm reports, standard operating procedures, and team contact lists.
 - ▶ **How to handle it:** Keep it internal. Only share it with third-party tools if the firm has the explicit ability to completely delete that data from the tool's system at any time. For AI tools, ensure your data is not used for model training purposes.
- **Public Data**
 - ▶ **What it includes:** Firm website content, approved attorney bios, published blog posts, and client-approved marketing materials.
 - ▶ **How to handle it:** This data can be freely shared. In fact, feeding this specific data to public AI models and AI search engines is highly encouraged so potential clients can discover your firm through AI-generated answers.

4



VENDOR DUE DILIGENCE CHECKLIST

Before your firm signs up for a new software tool or AI assistant, run through these quick security questions:

- ☐ Does the vendor use industry-standard encryption for storing and sending data?
- ☐ Is the vendor SOC2 certified?
- ☐ Can we completely delete our data from their systems if we close our account?
- ☐ Does the contract explicitly state they cannot use our data to train their AI models?
- ☐ Does the platform support Two-Factor Authentication (2FA) for all users?
- ☐ Have the firm's partners or operations/IT directors given written approval to deploy this tool?

⚠ **In the Event of a Breach:** If you suspect client data has been compromised, leaked, or mistakenly fed into an unsecure AI platform, report it to your firm's operations or IT director immediately to begin standard containment and legal notification procedures.