FLYGHT

MANAGED IT SERVICES | TOLEDO, OHIO

The Law Firm's Guide to IT Security & Ethical Compliance

Protecting Client Confidentiality in the Digital Age

A practical guide for managing partners and office administrators at small and mid-sized law firms — covering ABA ethical obligations, cybersecurity threats, and the technology decisions that protect your clients and your practice.

flyght.support | (419) 670-7100 | support@flyght.support

What's Inside

Why IT Compliance Matters for Law Firms

If you're a managing partner or office administrator at a law firm, here's the uncomfortable truth: your ethical obligations now extend to your technology. It's not optional. It's not a "nice to have." The ABA has made it clear — lawyers have a duty to understand the technology they use to protect client data.

And yet, most small and mid-sized law firms are running on a patchwork of aging systems, consumer-grade email, and an IT provider who "keeps things running" without any real understanding of the legal industry's unique requirements.

> *A data breach at a law firm isn't just an IT problem — it's an ethical violation, a malpractice liability, and a reputation killer, all rolled into one.*

This guide cuts through the noise. We'll cover exactly what you need to know about your ethical obligations, the threats targeting law firms specifically, and the practical steps you can take to protect your clients and your practice.

The Stakes Are Higher for Law Firms

- Client confidentiality isn't just good practice — it's an ethical mandate under ABA Model Rules.
- Law firms are disproportionately targeted by cybercriminals because of the sensitive data they hold and the money they move.
- Malpractice insurance carriers are increasingly requiring specific cybersecurity measures — and denying claims when they're missing.
- A single breach can trigger bar complaints, regulatory investigations, and client lawsuits simultaneously.

ABA Model Rule 1.6: Your Ethical Obligations

ABA Model Rule 1.6 requires lawyers to make "reasonable efforts" to prevent unauthorized access to, or disclosure of, information relating to the representation of a client. That sounds straightforward until you realize what "reasonable efforts" actually means in today's threat landscape.

> *"A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." — ABA Model Rule 1.6(c)*

What "Reasonable Efforts" Means in Practice

The ABA's Formal Opinion 477R clarifies that lawyers must stay current on technology risks and implement safeguards appropriate to the sensitivity of the information. This includes:

- Understanding how your email, file storage, and communication tools handle client data.
- Implementing encryption for sensitive communications — especially when transmitting confidential information electronically.
- Using multi-factor authentication (MFA) on all systems that access client information.
- Having a documented incident response plan so you know exactly what to do when (not if) something goes wrong.
- Regularly training staff on cybersecurity awareness — because your weakest link is usually a person, not a firewall.
- Conducting periodic risk assessments to identify vulnerabilities before attackers do.

The "I Didn't Know" Defense Doesn't Work

Ignorance of technology is not a defense. The ABA has made it clear that lawyers have a duty of competence that includes understanding the technology they use. If your firm is breached because you were running Windows 7, using "password123," or storing client files in an unencrypted cloud folder — "I didn't know" won't protect you from a bar complaint.

This doesn't mean you need to become a cybersecurity expert. But it does mean you need to work with an IT partner who understands the legal industry's requirements and can implement appropriate safeguards on your behalf.

Business Email Compromise: The #1 Threat to Law Firms

Business Email Compromise (BEC) is the single biggest cybersecurity threat facing law firms today. It's not ransomware. It's not some exotic zero-day exploit. It's a carefully crafted email that looks like it came from someone you trust — a partner, a client, a title company — asking you to do something that seems perfectly reasonable.

How BEC Attacks Target Law Firms

Law firms are prime targets for BEC because they routinely handle large financial transactions, wire transfers, and sensitive client communications. Here's how a typical BEC attack works:

Step 1: Reconnaissance

The attacker researches your firm — staff names, practice areas, active cases, recent closings. LinkedIn, court records, and your own website give them everything they need.

Step 2: Account Compromise or Spoofing

They either hack into a real email account (yours, a client's, or a title company's) or create a convincing lookalike domain (e.g., "smithlaw.co" instead of "smithlaw.com").

Step 3: The Ask

They send an email that looks legitimate — often requesting a wire transfer to a new account, asking for sensitive case documents, or changing payment instructions for a closing.

Step 4: The Theft

By the time anyone realizes what happened, the money is gone. BEC losses are rarely recoverable.

> *The FBI's Internet Crime Complaint Center (IC3) reports that BEC attacks caused over $2.9 billion in losses in 2023 alone. Law firms and real estate transactions are among the most frequently targeted.*

Protecting Your Firm from BEC

- Implement email authentication protocols (SPF, DKIM, DMARC) to prevent domain spoofing.
- Require verbal confirmation for any wire transfer instructions — every time, no exceptions.
- Use advanced email filtering that detects impersonation attempts, not just spam.
- Train every person in your office to recognize BEC red flags: urgency, secrecy, changes to payment details.
- Enable MFA on all email accounts. A compromised email account is the starting point for most BEC attacks.
- Never trust a change of wire instructions received by email alone. Always verify through a known phone number — not one provided in the suspicious email.

Malpractice Insurance & Cybersecurity Requirements

Here's something most attorneys don't realize until it's too late: your malpractice insurance policy likely has cybersecurity requirements baked into it. And if you don't meet them, your carrier can deny your claim — even if you've been paying premiums for years.

What Carriers Are Requiring

Insurance carriers have gotten smarter about cyber risk. Most professional liability and cyber insurance policies now require or strongly incentivize the following:

- Multi-factor authentication (MFA) on all email accounts and remote access systems.
- Endpoint detection and response (EDR) software on all workstations and servers — basic antivirus is no longer sufficient.
- Regular data backups with tested restore procedures.
- Employee cybersecurity awareness training at least annually.
- Encrypted email for sending sensitive client information.
- A documented incident response plan.
- Patch management processes to keep all software current.

> *If you're breached and your carrier discovers you weren't meeting the security requirements in your policy, they can — and will — deny your claim. The premiums you paid won't matter.*

The Practical Impact

This isn't theoretical. Carriers are actively investigating claims and denying coverage when firms can't demonstrate they had basic security controls in place. The most common denial triggers:

- No MFA on email when a BEC attack succeeds.
- No EDR/advanced endpoint protection when ransomware hits.
- No backup testing when data needs to be restored.
- No documentation that security training was conducted.

Your IT provider should be helping you meet these requirements — not as an upsell, but as a core part of the service. If they can't tell you exactly how your current setup aligns with your insurance requirements, that's a problem.

Cloud vs. On-Premise: Making the Right Choice

The "cloud vs. on-premise" question comes up in every law firm technology discussion. There's no one-size-fits-all answer, but there are clear guidelines for making the right decision based on your firm's size, practice areas, and risk tolerance.

The Case for Cloud

- Enterprise-grade security that most small firms could never afford to build themselves. Microsoft 365 and Google Workspace invest billions in security infrastructure.
- Automatic updates and patching — no more running outdated software because "the update might break something."
- Built-in redundancy and disaster recovery. Your data is replicated across multiple data centers.
- Accessibility from anywhere, which matters when attorneys need to work from court, home, or while traveling.
- Predictable monthly costs instead of large capital expenditures for server hardware.

The Case for On-Premise (or Hybrid)

- Some practice areas (e.g., national security, certain government contracts) may have data residency requirements that limit cloud use.
- Firms with very large document repositories may find cloud storage costs add up significantly.
- Legacy practice management software that doesn't have a cloud version may require local servers.
- Some firms prefer the perceived control of having their data physically on-site.

Our Recommendation

For most small and mid-sized law firms, a cloud-first approach with Microsoft 365 is the right answer. Here's why:

- Microsoft 365 Business Premium includes enterprise-grade email security, MFA, device management, and data loss prevention — all in one license.
- It meets the security requirements of virtually every malpractice insurance carrier.
- It provides the encryption capabilities you need for ABA Rule 1.6 compliance.
- It's easier and less expensive to maintain than on-premise servers for firms under 50 attorneys.

> *The question isn't "Is the cloud secure enough?" The question is "Can your firm maintain the same level of security on-premise?" For most small firms, the honest answer is no.*

Email Security & Data Handling

Email is the primary communication tool for most law firms — and it's also the primary attack vector. Securing your email isn't just about spam filters anymore. It requires a layered approach that addresses both inbound threats and outbound data protection.

Email Security Essentials

- Advanced threat protection that scans attachments and links in real-time, not just at delivery.
- Email authentication (SPF, DKIM, DMARC) to prevent attackers from spoofing your firm's domain.
- Encryption for messages containing sensitive client information — both in transit and at rest.
- Data Loss Prevention (DLP) policies that flag or block emails containing sensitive information sent to unauthorized recipients.
- Email archiving and retention policies that meet your jurisdiction's requirements and your firm's document retention obligations.
- Mobile device management (MDM) to secure email access on personal phones and tablets.

Secure Data Handling Practices

Beyond email, your firm needs clear policies for how client data is stored, accessed, and transmitted:

- Client files should be stored in encrypted, access-controlled environments — not on individual attorney desktops or USB drives.
- File sharing with clients should use secure portals, not email attachments for sensitive documents.
- All remote access to firm systems should require VPN or zero-trust network access with MFA.
- Former employee access must be terminated immediately — not "when IT gets around to it."
- Physical security matters too: lock screens, clean desk policies, and secure disposal of paper files containing client information.

> *Ask yourself: if a laptop were stolen from your office today, could the thief access client files? If the answer is yes — or even "maybe" — you have a problem that needs to be fixed immediately.*

Law Firm Security Compliance Checklist

Use this checklist to evaluate your firm's current security posture against your ethical obligations. Be honest — this is for your firm's protection, not for show. Any item you can't confidently check off represents a gap that needs to be addressed.

ACCESS CONTROLS & AUTHENTICATION

- [ ] MFA is enabled on all email accounts and remote access systems.
- [ ] Unique passwords are required for all users (no shared accounts).
- [ ] Former employee and contractor access is revoked within 24 hours of departure.
- [ ] Administrative access to systems is limited to authorized IT personnel only.
- [ ] Password policies require complex passwords changed at regular intervals.

EMAIL & COMMUNICATION SECURITY

- [ ] Email encryption is available and used for sending sensitive client information.
- [ ] SPF, DKIM, and DMARC are configured on your email domain.
- [ ] Advanced threat protection scans all inbound email attachments and links.
- [ ] Wire transfer requests are verified verbally through a known phone number.
- [ ] A clear policy exists for what can and cannot be sent via unencrypted email.

DATA PROTECTION & BACKUP

- [ ] All client data is stored in encrypted, access-controlled environments.
- [ ] Data backups run daily and are stored in a separate, secure location.
- [ ] Backup restores are tested at least quarterly to verify data integrity.
- [ ] A documented data retention and destruction policy is in place.
- [ ] Mobile devices accessing firm data are managed and can be remotely wiped.

INCIDENT RESPONSE & TRAINING

- [ ] A written incident response plan exists and has been shared with key staff.
- [ ] All employees receive cybersecurity awareness training at least annually.
- [ ] Phishing simulation exercises are conducted to test staff readiness.
- [ ] The firm knows exactly who to contact (IT, insurance, bar association) in case of a breach.
- [ ] Cyber insurance is current and the firm meets all policy requirements.

COMPLIANCE & DOCUMENTATION

- [ ] The firm has reviewed ABA Model Rule 1.6 and Formal Opinion 477R.
- [ ] Technology competence is part of ongoing CLE and professional development.
- [ ] Client engagement letters address electronic communication and data handling.
- [ ] Third-party vendors with access to client data have signed BAAs or security agreements.
- [ ] An annual security risk assessment is performed and documented.

How Did You Score?

20+ items checked: You're in good shape — keep it up and review annually. 10–19 items: Significant gaps exist that could expose your firm. Under 10: Your firm is at serious risk of a breach, ethical violation, or insurance denial. Take action now.

Your Clients Trust You With Their Most Sensitive Information. Can You Trust Your IT?

Flyght IT works with law firms across Northwest Ohio to implement security and compliance solutions that meet your ethical obligations — without overcomplicating things or breaking the budget.

We'll start with a free, no-pressure IT assessment — a straightforward look at where your firm stands today and what needs to happen to protect your clients and your practice.

SCHEDULE YOUR FREE ASSESSMENT

flyght.support/contact

(419) 670-7100

support@flyght.support

7430 W Central Ave., Toledo, OH 43617