vijilan
IT Security: Enabled

ABA COMPLIANCE GUIDE

Meeting Rule 1.6 with DMS Monitoring

How Law Firms Can Demonstrate "Reasonable Efforts" to Protect Client Data in NetDocuments

Understanding Your Ethical Obligations

Attorneys have always had a duty to protect client confidentiality. In the digital age, that duty extends to the electronic systems where client data is stored, accessed, and managed. For the majority of law firms, that system is NetDocuments—and it requires specific security attention that most firms are not providing.

"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

The ABA's Comment 18 to Rule 1.6 clarifies that attorneys must consider:

- The sensitivity of the information
- The likelihood of disclosure if additional safeguards are not employed
- The cost of employing additional safeguards
- The difficulty of implementing the safeguards
- The extent to which the safeguards adversely affect the lawyer's ability to represent clients

The Critical Question

If your firm stores sensitive client documents in NetDocuments but does not actively monitor who accesses those documents, when, and what they do with them—are you making "reasonable efforts"?

The NetDocuments Blind Spot

Why Your Current Security Isn't Enough

Most law firms have invested in firewalls, endpoint detection (EDR), email security, and perhaps a SIEM. While these tools serve important functions, none of them provide visibility into what happens inside your document management system.

Security Tool	What It Sees	What It Misses in NetDocuments
Firewalls	Network traffic	Document access, user behavior
EDR/XDR	Endpoint processes	Cloud DMS activity, matter access
Email Security	Email threats	Document sharing, DMS authentication
Traditional SIEM	Configured sources	NetDocuments logs (unless integrated)

The fundamental problem is that NetDocuments operates as a cloud-native platform with its own authentication, authorization, and audit logging systems. Without ingesting and analyzing these logs, your security team is flying blind in the very system that holds your most sensitive client data.

What the ABA Has Said About Cybersecurity

ABA Formal Opinion 477R (2017)

"A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access."

ABA Formal Opinion 483 (2018)

This opinion specifically addresses data breaches and obligations when client data may have been compromised. Key points:

- Lawyers must employ reasonable security measures
- When a breach occurs, lawyers must investigate promptly
- Lawyers may need to notify affected clients
- Lawyers should have incident response capabilities in place

The Implication: You cannot investigate what you cannot see. Without monitoring of your DMS, you may not even know a breach has occurred—much less be able to investigate it or notify affected clients.

State Bar Requirements

Multiple state bars have issued formal ethics opinions requiring lawyers to:

- Stay informed about technology risks (California, New York, Florida, Texas, and others)
- Implement appropriate safeguards for client data
- Conduct ongoing monitoring of systems that store client information
- Have incident response capabilities

How DMS Monitoring Satisfies Your Obligations

What Vijilan's NetDocuments Monitoring Provides

- **Continuous Monitoring** — NetDocuments audit logs ingested every 5 minutes into SIEM platform. Activity monitored 24/7 by certified SOC analysts.
- **Anomaly Detection** — Automated detection of unusual access patterns, mass downloads, off-hours activity, and potential data exfiltration.
- **Incident Investigation** — When alerts are triggered, SOC analysts investigate immediately and provide detailed incident reports.
- **Access Accountability** — Complete audit trail of who accessed what documents, when, from where, and what actions they took.
- **Permission Monitoring** — Track changes to user permissions, detecting unauthorized escalation or inappropriate access grants.
- **Compliance Reporting** — Monthly security reports and audit-ready documentation demonstrating your monitoring controls.

Client Confidence Statement

With Vijilan, your firm can confidently tell clients:

"All activity in our document management system is monitored 24/7 by a SOC 2 Type II and ISO 27001 certified Security Operations Center. We have real-time visibility into document access, automated detection of suspicious activity, and incident response capabilities to protect your information."

vijilan
IT Security: Enabled

info@vijilan.com www.vijilan.com +1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN

Beyond Ethics: Business Requirements

Cyber Insurance Requirements

Insurance carriers increasingly require evidence of active security monitoring as a condition of coverage. Policies may require:

- 24/7 security monitoring capabilities
- Incident detection and response procedures
- Audit logging and retention
- Regular security assessments

Firms without DMS monitoring may face higher premiums, coverage exclusions, or claim denials after an incident.

Client Due Diligence

Corporate clients—particularly in financial services, healthcare, and technology—require outside counsel to demonstrate specific security controls:

- Outside counsel guidelines increasingly ask about DMS monitoring
- RFP questionnaires require detailed security information
- Annual security assessments may be required
- Some clients require SOC 2 certification from their law firms

Competitive Advantage

Firms that can demonstrate robust DMS monitoring gain advantages in:

- Winning new clients who prioritize security
- Retaining clients with strict security requirements
- Responding confidently to security questionnaires
- Demonstrating compliance during audits

Protect Your Clients. Protect Your Firm.

Monitoring your document management system is not optional—it is an ethical obligation, a business requirement, and a competitive necessity.

Vijilan's NetDocuments Monitoring

- Deploys in under 60 minutes
- Zero impact on firm operations
- 24/7 global SOC coverage
- SOC 2 Type II and ISO 27001 certified
- Pre-built detection rules for legal DMS environments
- Cross-domain correlation with endpoint, identity, and email

GET A FREE NETDOCUMENTS SECURITY ASSESSMENT

See what you're missing. Protect your clients.

vijilan
IT Security: Enabled

vijilan.com| info@vijilan.com | +1 (954) 334-9988