Data Security, Compliance, and Privacy at Nextpoint

The trusted repository for your client data

Protecting client data is a fundamental duty for legal professionals. Nextpoint delivers industry-leading security through Amazon Web Services infrastructure, ensuring the confidentiality, integrity, and availability of your sensitive legal data.

SECURITY AT-A-GLANCE

- **AWS Foundation:** Built on Amazon Web Services — the most secure cloud infrastructure available, trusted by NASA, the CIA, and Fortune 500 companies worldwide.
- **Enterprise Encryption:** AES-256 encryption enforced at all times, both in transit and at rest, rendering your data unreadable to unauthorized parties.
- **SOC 2 Type II Compliant:** Independent auditing validates our security controls and ensures our data protection practices meet industry standards.
- **Granular Access Controls:** Role-based permissions at case, folder, and document levels.
- **Complete Audit Trails:** Comprehensive logging and timestamped reporting provide full visibility into document access and user activity.
- **Multi-Factor Authentication:** Mandatory 2FA for all users and devices, with Single Sign-On (SSO) integration available for Okta, Azure AD, and other enterprise identity providers.

WHY AWS MATTERS FOR LEGAL DATA

Amazon Web Services maintains extensive compliance certifications and security frameworks:

- **Physical Security:** Biometric access controls, 24/7 monitoring, and restricted data center access
- **Network Security:** Distributed denial-of-service (DDoS) protection, firewall management, and intrusion detection
- **Infrastructure Security:** Hardware security modules (HSMs), secure boot processes, and automated security patching
- **Compliance Portfolio:** FedRAMP, SOC 1/2/3, PCI DSS Level 1, ISO 27001, ISO 27017, ISO 27018, FIPS 140-2, and 90+ additional certifications and attestations

99.999999999% durability across multiple availability zones ensures your data is protected against hardware failures and disasters.

WHY NEXTPOINT MATTERS FOR LEGAL DATA

- **Unlimited Data Processing:** No per-GB fees, just predictable pricing — no matter what your caseload brings
- **Access Anywhere:** Secure document review and cloud-based collaboration from any device, location, or network
- **Complex File Format Compatibility:** Keep all your sensitive case content in a single software

PRIVACY AND COMPLIANCE

The privacy of client data is our top priority. All Nextpoint applications are developed, deployed, managed, and optimized internally.

For development and testing environments, Nextpoint restricts access to client data to authorized personnel only through role-based access controls and leverages security measures to protect confidential, personal, and other sensitive information as needed. Nextpoint employs an enterprise Secure Software Development Life Cycle (SDLC) as part of its ongoing commitment to building and maintaining secure applications.

Nextpoint's Site Reliability Engineering Team assesses security risks on an ongoing basis, monitors access logs, addresses known incidents, and applies security patches. Nextpoint conducts a comprehensive, annual IT risk assessment to ensure and maintain SOC II Type 2 Compliance.

Read Nextpoint's full Privacy Policy here.

AI SECURITY

Unlike general-purpose AI tools that may expose confidential data, Nextpoint's AI capabilities operate entirely within our secure cloud environment. All AI processing maintains the same enterprise-grade security protections as the rest of the Nextpoint software.

Our AI features are built on Amazon Bedrock, AWS's fully managed service for foundation models. Key protections include:

- **No Model Training:** AWS Bedrock does not use customer data to train or improve foundation models
- **No Data Storage:** Bedrock doesn't store or log prompts or completions
- **No Third-Party Sharing:** Input and output data are never shared with model providers
- **Encryption:** All AI interactions are encrypted in transit and at rest

FREQUENTLY ASKED QUESTIONS

Q: ***What types of data does Nextpoint handle?***

A: We collect, process, and review all forms of electronically stored information (ESI), including documents, emails, social media posts, and digital evidence across dozens of file formats. Data is encrypted at rest and in transit.

Q: ***Do you have compliance certifications?***

A: Yes, we are SOC 2 Type II compliant, covering security, availability, confidentiality, and privacy. SOC 3 reports are available upon request; SOC 2 reports require an executed NDA.

Q: ***What about data protection regulations?***

A: We comply with CCPA for California residents. GDPR compliance is not currently applicable as we don't have EU deployment.

Q: ***Can I control user access and permissions?***

A: Absolutely. Our role-based access control (RBAC) includes six permission levels: View Only, Reviewer, Basic, Standard, Advanced, and Dashboard Administrator, giving you granular control over both internal teams and external parties.

Q: ***How does Single Sign-On work?***

A: We integrate with Okta and Azure AD, with custom SSO integrations available upon request through Client Success.

Q: ***Are audit logs comprehensive?***

A: Yes, we maintain complete audit trails with document-level view, edit, and markup history, including timestamps. Logs are tamper-resistant and retained permanently unless the database is archived or deleted.

Q: ***How do I delete or export my data?***

A: Complete our **Data Archive Form** to archive (retain with no access), delete permanently, or export your database. Export services may incur additional fees.

LEARN MORE: **nextpoint.com/trust**
CONTACT: **hello@nextpoint.com**
CALL: 1.888.929.NEXT