NEXTPOINT

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:** Encryption enforced at all times, TLS 1.2+ in transit and AES-256 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 Hosting:** 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 2 Type II 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

Please see more complete Nextpoint AI Security provisioning in our **AI Security Overview** document.

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 ABOUT NEXTPOINT AI AND SECURITY

VISIT: **nextpoint.com/trust**
EMAIL: **hello@nextpoint.com**
PHONE: **1.888.929.NEXT**

AI at Nextpoint

Built for legal work. Secure by design.

Nextpoint is built on a simple promise: a platform that keeps up with your caseload — reliable, fast, and built for how litigation actually works. We combine ediscovery and case-building software with hands-on expert services, so you have a team behind you at every stage of litigation.

That vision extends directly to how we think about AI: legal teams are exploring it faster than ever and asking harder questions about it. This document outlines the principles, architecture, and safeguards behind every AI feature at Nextpoint.

Our AI Principles

Purpose-Built for Legal Work

Tools designed with your day-to-day in mind.

Every Nextpoint AI feature is designed around real legal workflows, with input from legal experts on what attorneys actually need. Intelligent Transcript Summaries, for example, offers Narrative, Chronological, and Table of Contents formats — each serving a unique purpose, but all reducing time spent on transcript review.

Architectural Security

Your case data stays on AWS and is never sent to an outside AI company.

Nextpoint's AI features run entirely on AWS. Search models are hosted in Nextpoint's own AWS account, and generative features use Amazon Bedrock, AWS's managed AI service, under Nextpoint's AWS agreement. Your data keeps the same protections as the rest of the platform: AES-256 encryption, SOC 2 Type II controls, and role-based access.

No Training on Your Data

Confidential case information isn't used to make AI smarter.

Your data is never used to train or improve any AI model, by Nextpoint or by AWS. AWS also never shares your inputs or outputs with model providers.

Human in the Loop, Always

AI accelerates your review — it doesn't replace judgment.

Nextpoint's AI features are designed to help attorneys decide where to focus, not to make decisions for them. Summaries, results, and generated content are starting points for review. Human judgment remains essential to every case decision.

Our Approach to AI

Legal work requires judgment, expertise, and insight that no tool can replicate. AI should surface key information and accelerate review, so your team can focus on strategy and winning the case. Our philosophy is that powerful, secure technology shouldn't be reserved for the firms with the biggest cases or biggest budgets. We build tools that make every attorney faster, sharper, and more effective.

How We Build AI Responsibly

Nextpoint's AI features run entirely on AWS. Depending on the feature, processing uses models Nextpoint hosts in its own AWS account, Amazon Bedrock, or both. Case content is never routed to a public or consumer AI tool.

The Architecture Behind Nextpoint AI

- **No provider retention or sharing:** Prompts and outputs sent to the managed foundation-model service are neither retained by nor shared with any external model provider.
- **Processing stays in your environment:** AI processing for all Nextpoint regions takes place in AWS data centers in the United States. Semantic search and ranking run on models Nextpoint hosts in its own AWS account. Generative steps (such as transcript summaries and match explanations) run on Amazon Bedrock, AWS's managed AI service, under Nextpoint's AWS agreement. AWS does not store your content or use it for training, and the model's developer never receives it. Your case content is never sent to an outside AI company.
- **Encryption everywhere:** All AI interactions are encrypted in transit and at rest.
- **Consistent controls:** The same security program that governs the rest of the platform — role-based access, multi-factor authentication — also applies to AI-powered features.

AI in Practice: Intelligent Transcript Summaries

Intelligent Transcript Summaries are a practical example of these principles at work. Instead of hours of manual review, attorneys can generate Narrative, Chronological, and Table of Contents summaries of a deposition in minutes — directly inside the same workspace where their transcripts, exhibits, and case materials already live.

Attorneys get faster context on testimony without introducing a new point of exposure for confidential case data.

AI in Practice: Intelligent Search *Rolling out to select clients now*

Intelligent Search pairs keyword precision with natural language understanding. Instead of relying on Boolean queries alone, legal teams can describe what they need in plain language and surface semantically relevant documents.

Your documents are never shared with outside providers. Semantic search and ranking run on models Nextpoint hosts in its own AWS account. Generative steps, such as match explanations, run on Amazon Bedrock, AWS's managed AI service, under Nextpoint's AWS agreement.

Intelligent Search only searches within the database it is enabled for. During Limited Release, we are validating that user-level restrictions, such as documents hidden from specific users, are applied to Intelligent Search results. We will confirm this is fully in place before general availability. Intelligent Search does not change who can see your data or modify access permissions.

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. Nextpoint hosts data in the United States and Canada, so GDPR compliance should be separately confirmed.

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.

Q: ***Do Nextpoint's AI features train on my data?***
A: No. Your data is never used to train or improve any AI model.

Q: ***Where does AI processing actually happen?***
A: AI processing for all Nextpoint regions takes place in AWS data centers in the United States. Semantic search and ranking run on models Nextpoint hosts in its own AWS account. Generative steps, such as transcript summaries and match explanations, run on Amazon Bedrock, AWS's managed AI service, under Nextpoint's AWS agreement. AWS does not store your content or use it for training, and the model's developer never receives it. Your case content is never sent to an outside AI company.

Q: ***How accurate are AI-generated results?***
A: AI features are built to accelerate attorney review, not replace it. We validate features through extensive testing before release. Generated summaries, results, and insights are intended as starting points, with attorney judgment guiding case strategy. Always review AI-generated results before relying on them.

Q: ***Is our data shared with outside AI providers?***
A: No. Inputs and outputs are never shared with or retained by any outside model provider.

Q: ***How is this different from using a tool like ChatGPT and Claude directly on case files?***
A: General-purpose consumer AI tools are not purpose-built for confidential legal data, and some may use inputs to improve their models depending on the plan or subscription. Nextpoint's AI runs inside an isolated environment with no model training, no data retention by the model provider, and no third-party sharing.

Q: ***What compliance framework covers Nextpoint's AI features?***
A: AI features are covered by the same security program as the rest of the platform, including SOC 2 Type II compliance and Nextpoint's annual IT risk assessment.

LEARN MORE ABOUT NEXTPOINT AI AND SECURITY

VISIT: **nextpoint.com/trust**
EMAIL: **hello@nextpoint.com**
PHONE: **1.888.929.NEXT**