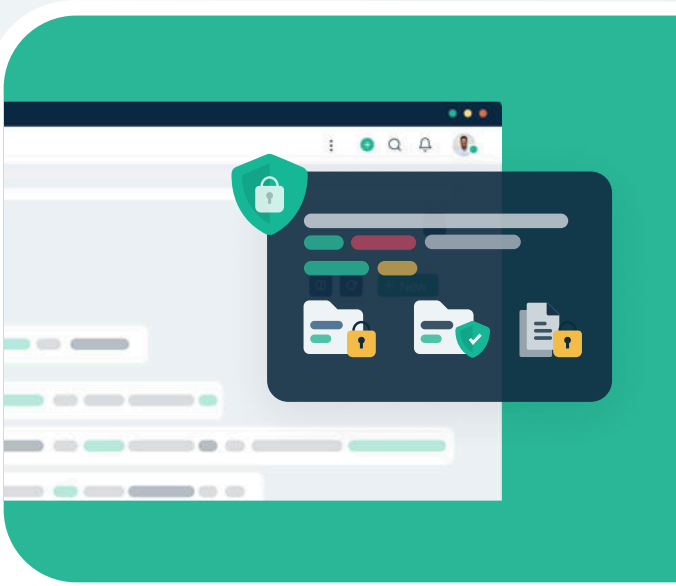
clarra

Secure and Private Case Management with Clarra

Robust security and privacy controls for protecting sensitive legal information



Leading law firms and legal departments rely on Clarra for its case management features and advanced security and privacy controls. Clarra protects sensitive legal data, allowing firms to comply with industry regulations while maintaining operational efficiency.

Why Choose Clarra for Security and Privacy?

Clarra, a cloud-based platform, is optimized for litigation. We empower qui tam litigation law firms to grow, enhance efficiency, protect sensitive cases, and meet every critical deadline. Discover how Clarra's tailored capabilities can elevate your practice.

Multi-Factor Authentication

Clarra mitigates litigation risks by employing multi-factor authentication and top-tier encryption. These measures safeguard sensitive information, ensuring data protection and compliance with legal and cybersecurity standards.

Encryption

Clarra uses military-grade encryption, hosting all data on Microsoft Azure servers that meet HIPAA, SOC 2, and ISO 27001 compliance standards. All data transmitted is encrypted using the latest TLS 1.2 and 1.3 cryptographic standards for enhanced protection.

Roles-Based Access Controls (RBAC)

Users can customize user access with over 70 detailed permission settings. These allow tailored visibility and editing rights based on the user's role and involvement in each case, ensuring secure and efficient case management.

Matter Access Management

Clarra users can control access to individual cases by restricting user, team, or group access. They can share specific case information with third parties, such as co-counsel, contractors, and litigation finance companies, while maintaining strict control over confidential data.

Audit Trails

Clarra's audit trail feature records all user activity within the system, ensuring accountability and enabling traceability for each action. These logs provide a comprehensive view of system interactions, ensuring secure and compliant operations.

Compliance Assurance

Clarra is designed to help firms meet industry standards, including HIPAA, SOC 2, and ISO 27001. Our robust security features ensure compliance with both legal and enterprise cybersecurity requirements.

© 2025 Clarra, Inc. All rights reserved |

Comprehensive Security and Privacy with Clarra

Data Encryption at Rest

All stored data is encrypted, protecting against unauthorized access.

Data Encryption in Motion

Using advanced encryption protocols, Clarra safeguards data during transmission.

Multi-Factor Authentication (MFA)

Secure your accounts with MFA options, including SMS, email, and authenticator apps.

Login with Google

Simplify access with secure Google login options while maintaining strict security controls.

Custom Role-Based Access

Customize access levels for your team with over 70 detailed permission settings, ensuring precise control over who can view and edit specific information.

How to Maximize Security with Clarra

Set Permissions

Define and adjust user permissions effortlessly to control access to cases, documents, and sensitive client information.

Conduct Audits

Utilize Clarra's reporting tools to conduct regular audits and identify potential security risks, ensuring adherence to all protocols.

Customize Reports for Insightful Analysis

Generate standard and custom reports to track every aspect of your billing, providing insights that help improve financial management and ensure security compliance.

Monitor User Activity

Oversee all interactions with Clarra in real-time, ensuring your firm's operations remain secure and compliant.

Manage Authentication

Configure multi-factor authentication settings for added security, providing additional protection for all user logins.

Get Started

Secure your legal practice with Clarra's advanced security and privacy features. Sign up today and enhance your firm's operational capabilities.

© 2025 Clarra, Inc. All rights reserved | Clarra.com