

Security & Privacy Overview

Sensitive records deserve serious protection.

Medical records and legal information are among the most sensitive data your organization handles. Compex maintains a formal, risk-based security and privacy program built to protect that information across our technology, operations, and workflows, backed by robust controls, ongoing testing, and independent audits.

HIPAA TRAINED

| SOC 2 TYPE II

| ENCRYPTED DATA

| SECURE DELIVERY

Protection at every stage

Security isn't something added after the record arrives. Compex applies administrative, technical, and operational safeguards throughout the information lifecycle, from retrieval and processing through access, delivery, and storage.



DATA PROTECTION

Sensitive information is encrypted in transit and at rest, with strict handling procedures, defined retention practices, and secure disposal.



IDENTITY AND ACCESS

Access follows least-privilege and need-to-know principles, using unique accounts, multi-factor authentication, and tightly controlled privileged access.



PHYSICAL

Facilities and work areas are access-controlled. Records are handled under chain-of-custody procedures, stored securely, and disposed of safely.



PERSONNEL

Employees complete pre-employment screening, access to sensitive data is limited to defined business need, and those handling medical information complete HIPAA training.



MONITORING AND RESPONSE

Centralized logging, monitoring, vulnerability scanning, and independent penetration testing help Compex identify, assess, and respond to potential risks, supported by a tested incident response program.



Business continuity

Security also means being ready when something unexpected happens. Compex maintains business continuity and disaster recovery practices designed to reduce the risk of data loss and limit disruption: geographically resilient recovery capabilities, regular backup and restoration testing, documented continuity and recovery plans, and 24/7 infrastructure monitoring and alerting.

Privacy matters

Compex does not sell client data, and client data is never used to train AI models. Information entrusted to Compex is used to deliver our services and meet applicable legal and compliance obligations. The principle is simple: sensitive information should be used only for the purposes for which it was entrusted to us.

Responsible innovation

As Compex expands the use of automation and medical records intelligence, security and privacy remain fundamental to how new technology is developed and deployed. Asabell™ operates inside the Compex security and governance environment, with data processed in controlled, US-based environments, human oversight, and the same enterprise controls that cover the rest of the workflow.

Technology should make sensitive information more useful without making it less protected.

For more information, a demo, or a quote, [visit us online](#) or contact us today.