TRIAL OPTIMA
(RE)SEARCH REDEFINED

TrialOptima Security & Compliance Overview

Contents

1. Purpose and Scope

This document describes the security, privacy and compliance practices implemented for the TrialOptima platform. It is intended to provide customers, partners and auditors with a clear understanding of how TrialOptima protects data, manages access and operates the platform in a secure and controlled manner. This document may be updated periodically to reflect changes in technology, regulations or operating practices.

2. Introduction

TrialOptima is an intelligence platform that brings global clinical trial and regulatory data and turns it into actionable format. Registered subscribers use the platform to search, filter and analyze trial data, plan and conduct feasibility assessments and track regulatory pathways. Because TrialOptima is used for decision-making across sponsors, CROs, investigators and sites, the security and privacy of the underlying data is a core design principle. This overview summarises the key technical and organisational controls that help protect TrialOptima and the information entrusted to it.

3. Governance and Policy Framework

TrialOptima operates under documented information security and data protection policies that define how systems, data and access are managed. These policies cover information security, data privacy, acceptable use, incident response and access control.

Overall responsibility for information security oversight rests with designated senior personnel within the organisation. Security policies and procedures are reviewed periodically and updated as required, particularly following significant system changes or identification of new security risks.

4. Scope of Data Handling and Data Classification

TrialOptima primarily processes publicly available clinical trial registry information, regulatory and compliance intelligence, aggregated and derived analytics, and customer shared feasibility documents such as protocol synopses and questionnaires.

The platform does not store patient level identifiable data or protected health information. Any personal data handled by TrialOptima is limited to basic user account information required for authentication, access management and customer support.

For clarity, data handled by the platform is classified into public data such as publicly available trial information, confidential customer data such as feasibility materials shared by customers, and internal operational data.

5. Hosting & Infrastructure Security

TrialOptima is hosted on Amazon Web Services (AWS) within a dedicated Virtual Private Cloud (VPC) in a secure region. The platform uses Amazon RDS for PostgreSQL and cloud servers that run inside a private network. Only the main HTTPS application endpoints that customers use are reachable from the internet; other internal components remain on private network addresses.

AWS-native firewall controls, including VPC security groups and network access control lists (ACLs), are used to limit inbound and outbound traffic to the ports and protocols that are necessary for the service. An AWS Web Application Firewall (WAF) helps protect against common web-based attacks and abusive traffic. All end-user access to TrialOptima is enforced over HTTPS with TLS certificates managed via AWS services, and clear-text HTTP is redirected to HTTPS.

Access to the live application is limited to registered users with valid subscriptions. Administrative and infrastructure access is restricted to authorized personnel only.

6. User Access and Account Management

User access to TrialOptima is managed through individual user accounts. Accounts are created following registration and subscription approval. Shared user accounts are not permitted in line with the platform Terms of Use.

Role based access control is implemented to ensure that users can access only those features and data appropriate to their role and subscription plan. Administrative functions and sensitive configuration settings are restricted to authorised roles.

User accounts are deactivated or removed upon subscription expiry or upon customer request including cases where a user leaves the customer organisation. Basic password controls and periodic access reviews are applied to reduce the risk of unauthorised access.

7. Data Protection, Encryption & Backups

Data security is a central design principle for TrialOptima. Application data is stored in Amazon RDS for PostgreSQL with encryption enabled for data at rest, including automated backups and snapshots. Automated backups are enabled for production databases. Backups are encrypted and retained for a defined period in line with operational and recovery requirements. Storage and backup configurations are periodically reviewed to ensure that they follow AWS security best practices and support recovery requirements.

Data in transit between the application, database and trusted third-party services is encrypted using TLS/SSL, so that information moving across networks cannot be read or tampered with by unauthorised parties. Sensitive configuration values such as database passwords and integration secrets are maintained in server-side environment configuration and are not embedded in client-side code.

For feasibility services, protocol synopses and feasibility questionnaires shared by customers are treated as confidential information. These materials remain the intellectual property of the customer and are used only for the agreed assessment purposes.

Confidentiality undertakings or agreements are put in place so that customers are assured that their information is handled securely and in line with TrialOptima's Terms of Use, Privacy Policy.

8. Disaster Recovery and Business Continuity

TrialOptima maintains basic disaster recovery capabilities through encrypted backups and defined restoration procedures. In the event of system failure or data loss, backups can be used to restore services within a reasonable timeframe. Disaster recovery arrangements are reviewed periodically to ensure continued effectiveness.

9. Application Security Controls

TrialOptima uses a modern web application framework that provides built-in defences against common web vulnerabilities, including safeguards for injection, cross-site scripting (XSS) and cross-site request forgery (CSRF). Server-side input validation and business-rule checks are applied to user-supplied data, and error messages are designed to avoid exposing stack traces or implementation details.

Users can sign in with a standard login form, and Google sign-in (OAuth) is also supported.

Role-based access control (RBAC) ensures that administrative functions, configuration pages and bulk data operations are restricted to authorised roles. Standard users can access only those features and data elements that correspond to their subscription plan and organisation. User accounts are individual and are not intended to be shared between multiple people, consistent with the TrialOptima Terms of Use.

Integrations with external services and any exposed APIs are protected using authenticated requests, such as API keys or signed calls. These secrets are stored only in secure server-side configuration and are rotated as part of operational maintenance. API credentials are not exposed in browser code or client-side storage.

10. Monitoring, Logging & Change Management

Application and infrastructure logs are collected using AWS monitoring services to support troubleshooting, incident investigation and detection of unusual activity. Logs are retained for a defined period and reviewed periodically.

Application changes and updates follow controlled deployment processes including review and testing prior to production release. Security related fixes are prioritised and tracked to closure.

11. Incident Management and Breach Handling

Security incidents are logged, assessed and investigated in a structured manner. Root cause analysis and corrective actions are documented and implemented as required.

In the event of a confirmed data security incident that may impact customer information, affected customers are informed in line with contractual obligations and applicable legal requirements.

12. Third Party and Vendor Controls

TrialOptima uses trusted third-party service providers including cloud infrastructure and supporting services selected based on reliability and security considerations. No unauthorised third parties are permitted access to confidential customer data.

Basic vendor due diligence is performed to ensure that third party services meet acceptable security and operational standards.

13. Audit and Customer Assurance

TrialOptima supports reasonable customer security questionnaires and audit requests subject to confidentiality and non-disclosure agreements. Additional security documentation can be shared upon reasonable request.

14. Vulnerability Assessment & Penetration Testing (VAPT)

TrialOptima is subject to periodic vulnerability assessment and penetration testing by an independent security vendor. The scope includes the primary web application and key AWS components that support the service. Testing is planned in a way that avoids disruption to customers while still exercising the relevant attack surface.

The security testing approach is aligned with recognised industry practices, including the OWASP Top 10 for web application security and common cloud security guidelines. A combination of automated scanning tools and manual testing techniques is used to identify vulnerabilities related to authentication, session management, access control, injection, configuration weaknesses and exposed services.

Findings from VAPT exercises are categorised by severity (critical, high, medium and low) and tracked through to closure. Identified vulnerabilities are remediated in line with their risk level, and re-testing is carried out to confirm that fixes are effective.

The platform practices are designed to align with recognised security and compliance frameworks such as ISO IEC 27001, the NIST Cybersecurity Framework and the CIS Critical Security Controls.

15. Regulatory and Legal Compliance

TrialOptima operates in compliance with applicable laws and regulations. Where applicable personal data handling aligns with applicable Data Protection Act.

16. Summary

TrialOptima combines secure cloud hosting on AWS, encryption of data at rest and in transit, layered application controls, monitored access to infrastructure and independent security testing to provide a robust security posture for users of the platform. By aligning its practices with well-known security frameworks and continually reviewing controls as the threat landscape evolves, Jehangir Clinical Development Centre aims to ensure that

TrialOptima remains a trusted environment for clinical trial and regulatory intelligence data.

17. Definitions and Abbreviations

AWS refers to Amazon Web Services

VPC refers to Virtual Private Cloud

VAPT refers to Vulnerability Assessment and Penetration Testing

RBAC refers to Role Based Access Control.

18. Document Control

Version 1.1 Last Updated February 2026

Owner TrialOptima Jehangir Clinical Development Centre