

TRT™ Security, Privacy & HIPAA Overview

For healthcare information-security, privacy, compliance and vendor-risk review | Version 1.3 | October 17, 2026

The Trial Recruitment Toolbox (TRT) is a browser-based clinical-trial recruitment platform designed and operated to support HIPAA-compliant use by research sites, site networks, SMOs, CROs and other authorized organizations. When Modern Trials handles protected health information (PHI) on behalf of a covered entity or another Business Associate, Modern Trials acts as a Business Associate and enters into an applicable Business Associate Agreement (BAA).

This document summarizes the principal administrative, physical, technical and contractual safeguards protecting information processed through the TRT. It is a security-review summary, not an independent certification, audit report or replacement for the applicable BAA or customer contract.

Security and Privacy at a Glance

- ✓ HIPAA Business Associate Agreement executed with every customer at registration
- ✓ HIPAA security risk assessments completed periodically, most recently September 19, 2026
- ✓ U.S.-based production hosting in AWS's Ohio region under an AWS Business Associate Agreement
- ✓ AES-256-GCM application-level encryption of PHI fields; encrypted storage and backups
- ✓ TLS 1.2 or later for all browser and web-API connections
- ✓ Multi-factor authentication required for every user, including super-administrators
- ✓ Unique named accounts, role-based permissions and organization-level data segregation
- ✓ PHI access, authentication events, document activity and data exports logged
- ✓ Vulnerability and security testing at least annually and after every major production update
- ✓ Encrypted daily backups with tested recovery
- ✓ No candidate records or PHI transmitted to OpenAI or any unauthorized third party
- ✓ Written notice of qualifying security incidents or unauthorized PHI use or disclosure without unreasonable delay and no later than 10 business days after discovery

1. Platform, Data and HIPAA Responsibilities

The TRT supports protocol setup, candidate screening and tracking, authorized outreach, scheduling, study-document preparation and electronic-signature workflows. Depending on customer use, the platform may process participant identifiers, contact information, screening responses, diagnoses, medications, laboratory information, scheduling records, communication history and consent or HIPAA authorization documents.

Customer ownership. Customers retain ownership of their Customer Data. Modern Trials processes Customer Data only to provide and support the contracted services, fulfill documented customer instructions and satisfy applicable legal obligations.

HIPAA relationship. Modern Trials acts as a Business Associate when it creates, receives, maintains or transmits PHI on behalf of a covered entity or another Business Associate. Customer acceptance of the Modern Trials BAA is recorded during organization registration and an executed copy is emailed to the customer administrator at acceptance. The applicable BAA governs the parties' PHI-related obligations.

Permitted use. Modern Trials does not sell PHI, does not use PHI to build advertising or marketing profiles and does not use Customer Data to train general-purpose artificial-intelligence models.

2. Infrastructure and Encryption

Cloud hosting	The TRT is hosted in the AWS us-east-2 region (Ohio) using Amazon EC2, Amazon RDS, Amazon S3, AWS KMS, Amazon Cognito and AWS Secrets Manager. Production data is stored in the United States. Modern Trials maintains a BAA with AWS.
Encryption at rest	RDS storage and snapshots are encrypted and S3 uses server-side encryption. Application-level PHI fields use AES-256-GCM with AWS KMS envelope encryption.
Encryption in transit	Browser and web-API connections use HTTPS with TLS 1.2 or later. Secure session-cookie attributes and browser security headers are configured for web access.
Credentials and documents	Service credentials and API keys are held in AWS Secrets Manager. Documents are stored in private S3 buckets and made available only through authorized, time-limited access links.
Backups and recovery	Encrypted database backups run daily and are retained for 30 days. Recovery procedures are tested to confirm that protected data can be restored.

3. Identity, Access and Application Security

- **Multi-factor authentication.** MFA is required for every user of the TRT, including customer administrators, Modern Trials personnel and super-administrator accounts.
- **Unique accounts.** Each user receives an individually assigned account. Shared user accounts are not permitted.
- **Role-based access.** Server-side authorization, organization-level segregation and record-ownership controls limit access to customer, trial, candidate and document records according to assigned responsibilities.
- **User administration.** Authorized customer administrators provision and deactivate their users. Modern Trials applies documented access-approval, review and revocation procedures to its workforce and privileged accounts.
- **Session controls.** The default inactivity timeout is 15 minutes, with a maximum administrator setting of 30 minutes. An eight-hour absolute session limit and one concurrent session per user are enforced.
- **Application protections.** Server-side input validation, CSRF protections, output encoding, restricted upload types, secure session controls and browser security headers protect application workflows.
- **Auditability.** The TRT records PHI access, authentication activity, document actions and customer-data exports. Audit records are protected from ordinary user modification and retained for at least six years; on termination, audit records containing PHI are handled as the BAA provides.

4. Security Governance and Assurance

Modern Trials maintains a documented privacy and security program addressing the administrative, physical and technical safeguards applicable to its operations and its role as a HIPAA Business Associate.

- HIPAA security risk assessments have been completed multiple times, most recently on September 19, 2026.
- Vulnerability and security testing is performed at least annually and after every major production update. Identified issues are documented, prioritized and remediated according to risk.
- Workforce members receive documented privacy and security training appropriate to their responsibilities.
- Workforce and privileged access is limited by role and business need, periodically reviewed and promptly revoked when no longer required.
- Documented incident-response, contingency and business-continuity procedures are maintained, and backup and recovery procedures are tested.
- Privacy and security policies are periodically reviewed and updated to reflect operational, regulatory and technical changes.

5. Service Providers and AI-Assisted Workflows

Amazon Web Services	Hosting, storage, encryption-key management, identity services and supporting cloud infrastructure. BAA in place.
RingCentral	Candidate voice and SMS communications initiated by authorized platform users. BAA in place.
Google Workspace	Business email used for customer support correspondence. BAA in place.
OpenAI API	Used only for protocol-based extraction and preparation of draft recruitment or study-document materials. The TRT does not transmit candidate records or PHI to OpenAI, and application controls prevent users from using the TRT to do so.
Stripe	Subscription billing and payment cards. The TRT does not store payment-card details and does not transmit participant records or PHI to Stripe.

The TRT does not provide a mechanism for users to transmit PHI to OpenAI, Stripe or any other third-party service that is not expressly authorized to handle PHI. Service providers authorized to create, receive, maintain or transmit PHI on behalf of Modern Trials are identified above as having Business Associate Agreements in place.

AI-generated materials support administrative workflows and require qualified customer review and approval before use. Trial eligibility, informed consent, clinical judgments and regulatory decisions remain the responsibility of the applicable customer, investigator or qualified clinical personnel.

6. Data Lifecycle, Resilience and Incident Response

- **Data export.** Authorized customer users may export Customer Data according to their assigned permissions.
- **Retention and deletion.** Archived trial records and soft-deleted participant records are deleted after seven years unless a different period is required by the applicable customer agreement, study requirements or law.
- **Backups.** Encrypted database backups run daily and are retained for 30 days, after which they age out. Recovery procedures are tested.
- **Customer offboarding.** Customers receive a 30-day period following termination in which to export their data, subject to the applicable agreement.
- **Data return or destruction.** Following termination and the export period, Customer Data is returned or destroyed as the governing agreement and BAA provide, except where continued retention is legally required.
- **Incident response.** Modern Trials maintains documented procedures for identifying, investigating, containing, remediating and documenting suspected security incidents.
- **Customer notification.** The BAA requires written notice of qualifying security incidents or unauthorized uses or disclosures of PHI without unreasonable delay and no later than 10 business days after discovery.

7. Shared Responsibility and Security Review

Modern Trials secures and operates the TRT platform and performs its responsibilities under the applicable agreements and BAA. Customers control the information they submit and remain responsible for:

- Applicable protocol, IRB, privacy and recruitment approvals
- Appropriate notices, permissions and authorizations
- Decisions concerning candidate recruitment and communications
- Limiting submitted information to the minimum necessary
- Provisioning and promptly deactivating their users
- Reviewing generated recruitment and study materials
- Protecting information exported from the TRT or transferred into customer-controlled systems

Additional documentation. Modern Trials responds to reasonable customer security and vendor-risk questionnaires. Additional documentation, including the applicable BAA, subprocessor information and further descriptions of relevant safeguards, is available on request and subject to appropriate confidentiality protections.

Security and privacy inquiries. Modern Trials Inc. • info@moderntrials.com (subject: "Security and Privacy Review") • (833) 587-4257 • 226 Guilford Ave., Haddon Township, NJ 08108. Applicable signed customer agreements govern if they differ from this summary.

Published references: [HIPAA Summary](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Trial Recruitment Toolbox Overview](#)