

Security and compliance summary

Two pages for a security or procurement review. Each section names the page on simplyrcs.ai it was read from, and this document was read against those pages on 8 October 2026. For the SOC 2 report, a completed questionnaire, or anything not covered here, write to security@simplyrcs.ai.

SOC 2 TYPE II

Independently audited controls for security, availability and confidentiality. Type II means the controls are verified as operating effectively over a period, not at a single point in time. The report is shared under NDA on request.

Source: [simplyrcs.ai/security/](#), [/trust/](#)

ACCESS CONTROL

- Role-based permissions (Admin, Brand Admin, Agent, Viewer), enforced in the interface and at every API endpoint.
- API keys scoped to read, write or admin; rotatable and revocable; the secret is shown once at creation.
- Every webhook is cryptographically signed so its origin can be verified.
- Single sign-on through the customer's own identity provider.
- Integrations connect through scoped, least-privilege access; a model is never handed a raw API key.

Source: [/security/](#), [/trust/](#)

DATA HANDLING

- Encrypted in transit (HTTPS and TLS) and at rest, including message content and contact records.
- Credentials stored encrypted with per-record keys; media served through signed URLs, not open links.
- US-based infrastructure: data and message traffic kept in-country. Direct Tier-1 carrier connections, so fewer intermediaries handle traffic.
- Data minimisation: the data needed to run and report on your messaging, used to deliver your service and not repurposed. Customer data remains the customer's.
- Message logs, recordings and metadata are retained for at least 90 days; on account closure the customer requests an export, after which data is deleted on schedule.

Source: [/security/](#), [/trust/](#), [/acceptable-use/](#) (section 13)

TCPA AND CTIA HANDLING

- STOP, START and HELP are honoured immediately and unconditionally, enforced at the platform layer above AI bots, agents and application code.
- Consent is tracked per channel and checked before every send; sends to anyone not opted in on that channel are suppressed.
- Quiet hours enforced; every consent event and submission is written to an audit trail.
- On RCS and SMS the AI only sends replies the customer authored, through flows the customer built; it hands off to a human when unsure.
- Customers agree under the Acceptable Use Policy to follow the TCPA, 47 CFR 64.1200, the CTIA Messaging Principles and Best Practices, and the carriers' messaging policies.

Source: [/security/](#), [/trust/](#), [/acceptable-use/](#) (section 9)

10DLC REGISTRATION AND SENDER VETTING

Brand and campaign registration through The Campaign Registry, carrier vetting for every sender, and Google verification of each RCS sender (business verified, brand name and logo registered) are handled by SimplyRCS. Registry and vetting fees are passed through at cost:

Item	When	Fee
TCR brand registration	One-time	\$4.50
TCR campaign vetting	One-time	\$15.00
Standard vetting (Aegis / WMC)	One-time	\$41.50
Enhanced vetting (Aegis)	One-time	\$101.50
Aegis sender review, required to send RCS	Annual, per sender	\$200.00

Source: [/pricing/](#) (registry and carrier tables, last verified 29 September 2026), [/trust/](#)

SUBPROCESSORS

A subprocessor list is not published on [simplyrcs.ai](#). Ask for the current list when requesting the SOC 2 report at [security@simplyrcs.ai](#). What the site does state: infrastructure is US-based, and carrier connections to AT&T, Verizon and T-Mobile are direct.

Source: [/security/](#)

HIPAA POSITION

No messaging channel is HIPAA compliant on its own, and RCS is no exception; compliance is a property of the programme, not the channel. A provider handling protected health information on a customer's behalf is a business associate and needs a signed Business Associate Agreement. SimplyRCS's stated position: design the programme so PHI stays out of the thread, and if the programme requires a BAA, raise it with Signalmash directly rather than assuming one is in place. HIPAA does not displace the TCPA; consent and opt-out handling still apply to every healthcare message.

Source: [/learn/is-rcs-hipaa-compliant/](#), [/learn/healthcare/](#)

REPORTING AND APPEALS

- Security vulnerabilities: [security@simplyrcs.ai](#). Responsible disclosure; researchers are credited.
- Abuse or Acceptable Use violations: [abuse@signalmash.com](#); reports acknowledged within 24 hours.
- Appeals against a suspension or termination: [legal@signalmash.com](#); response within 5 business days.
- Amendments to the Acceptable Use Policy are posted and e-mailed to registered contacts at least 30 days before they take effect.

Source: [/security/](#), [/acceptable-use/](#) (sections 11, 15, 16)

Signalmash is the trading name of Mash Technologies Corporation, registered in Oregon on 27 April 2021 (Oregon Secretary of State registry number 181585598). SimplyRCS and Signalmash are registered trademarks and DBAs of Mash Technologies Corporation. 3000 NE Stucki Ave, Ste 230, Hillsboro, OR 97124 · +1 (866) 217-9750 · [hello@simplyrcs.ai](#) · Terms: [simplyrcs.ai/terms/](#) · Privacy: [simplyrcs.ai/privacy/](#) · Acceptable use: [simplyrcs.ai/acceptable-use/](#)

Read against the named pages on 8 October 2026. The pages are the current statement; where this summary and a page differ, the page governs.