RegSecure

SECURITY & COMPLIANCE WHITEPAPER

RegSecure — Security Whitepaper

A customer-facing overview of the RegSecure security architecture.

This whitepaper summarises how RegSecure protects video consultations, document signing, and session recordings for regulated industries. It describes the cryptographic standards we apply, the privacy properties of our architecture, and how the platform supports HIPAA, GDPR, FINRA, and attorney–client confidentiality obligations. Procurement, compliance, and risk teams should be able to evaluate RegSecure from this document alone. A detailed technical architecture document is available under NDA for security reviewers.

1. Architecture at a Glance

RegSecure is a **zero-knowledge, browser-native platform**. All cryptography, content handling, recording, and signing happen entirely inside the user's browser. RegSecure servers never see, process, or store decrypted user content.

This produces three properties that matter for regulated work:

- **No content on our servers.** Video, audio, documents, recordings, signatures, and chat exist only in participants' browsers and on devices they choose to download to.
- **No accounts, no databases.** RegSecure does not maintain user accounts, content databases, or analytics back-ends. There is nothing to subpoena, breach, or leak from our infrastructure.
- **No Business Associate Agreement required.** Because no Protected Health Information ever transits or rests on our infrastructure, RegSecure operates outside the BAA scope under HIPAA.

Layer	Purpose	What it sees
Web application	Runs all encryption, signing, and recording in-browser	Plaintext content (in user's browser only)
Static hosting	Serves the application code	Application code only
Signalling relay	Helps two browsers find each other to start a peer-to-peer call	Ephemeral connection metadata — no media, no messages, no keys
Media relay (TURN)	Forwards encrypted packets when direct peer-to-peer fails (≈10–20% of calls)	Encrypted packets only — content is unreadable

Once the call connects, browsers communicate **directly with each other**. RegSecure infrastructure is no longer in the data path.

---

2. Encryption Standards

RegSecure uses widely vetted cryptographic primitives — all standardised by NIST or the IETF and implemented through the browser's native Web Crypto API. We do not roll our own crypto.

Purpose	Algorithm
Symmetric encryption	**AES-256-GCM** (authenticated encryption for media frames, data-channel messages, file encryption)
Key agreement	**ECDH P-256**, fresh per session — forward secrecy
Key derivation	**HKDF-SHA-256** (NIST SP 800-56A) applied to every shared secret before use
Hashing	**SHA-256** for document hashes, audit-chain integrity, evidence Merkle roots
Transport security	**TLS 1.2+** for HTTPS, **DTLS-SRTP** for WebRTC media
Key recovery	**Shamir Secret Sharing (3-of-5)** — three of five custodial shares reconstruct the master key; two or fewer reveal nothing
Signature binding	**WebAuthn / FIDO2** with platform biometric, used to bind a signature to a verified human at the moment of signing

End-to-end encryption (E2EE) means E2EE. Encryption keys are generated and held in participants' browsers. They are not escrowed, not transmitted to RegSecure, and not recoverable by RegSecure under any circumstance — including legal request.

---

3. Data Flow Summary

A typical session flows as follows. Encrypted material is in **bold**; plaintext exists only in browser memory.

1. **Session creation.** A host opens RegSecure in a browser. The browser generates a random session code, an ephemeral key pair, and (on first use) a master key stored locally.
2. **Invitation and waiting room.** The host shares the session code out-of-band (email, SMS, calendar) and explicitly admits each participant from a waiting room.
3. **Connection setup.** Browsers exchange connection details through the signalling relay, which sees only the metadata needed to bring two browsers into contact — never content or keys.
4. **Key exchange and verification.** Each pair of browsers performs an ECDH key exchange, derives a unique shared key, and displays a six-digit **Safety Code**.

Participants read it aloud to confirm there is no man-in-the-middle.

5. **Encrypted communication.** Audio, video, screen share, chat, document content, and signatures flow **directly between browsers** over an encrypted peer-to-peer channel. RegSecure infrastructure is no longer in the data path.
6. **Optional recording.** Recording requires explicit on-screen consent from every participant; the recording is composed and held in the recorder's browser only.
7. **Optional download.** When the session ends, the user may download recordings, signed documents, and the audit log either as standard files or encrypted with the user's own key.

At no point does a RegSecure server hold a decrypted copy of session content.

---

4. Local Storage and Data Residency

Because nothing is uploaded, "data residency" for content is straightforward: **content resides where the user's browser runs.**

Item	Where stored	Persisted?
Master key (used for optional file encryption)	Browser-local secure storage	Yes, until the user rotates or clears it
Session metadata (start time, duration, compliance label, file hashes)	Browser-local storage	Yes — for the user's own session history
Video, audio, recording content, documents, signatures, chat	Browser memory only	No — discarded on tab close unless downloaded

Users can clear local storage at any time via standard browser controls. RegSecure never receives a copy of the master key, the recording, the document, or the signature.

---

5. Compliance Posture

RegSecure does not claim certified compliance with any framework. Compliance is an organisational process; what RegSecure provides is a **technical architecture that supports compliance** by ensuring no decrypted user content leaves the customer's environment.

HIPAA (US — Healthcare). No Protected Health Information is stored, transmitted, or processed by RegSecure servers. **No Business Associate Agreement is required**, because RegSecure never enters a business-associate relationship with respect to PHI. Recording starts only after explicit on-screen consent from all participants, and session events are logged locally in the FHIR AuditEvent format.

GDPR (EU — Personal Data). No server-side processing of personal data or content. No cross-border data transfer of content — sessions stay between the participating browsers. Local audit logs and data-subject access are under the customer's exclusive control. Consent for recording is captured explicitly in-product and logged.

FINRA (US — Financial Services). All client communications and recordings remain under the firm's exclusive control. E2EE recording with a tamper-evident audit trail (Merkle-anchored evidence chain). Records are downloaded and archived by the firm under its own retention policy.

Attorney–Client Privilege. Communications never traverse a third party in plaintext. No third party — including RegSecure — can compel disclosure of session content because none exists outside the participants' devices.

What customers still need to do

Requirement	Provided by RegSecure	Customer responsibility
User authentication / SSO	Not provided	Implement own access controls
Record retention	Encrypted download + local history	Archive records per retention policy
Privacy policy and notices	Not provided	Publish customer's own policy
Staff compliance training	Not provided	Train on internal procedures
Risk assessments	Architecture and reference docs available	Conduct own assessment

---

6. Recording, Signing, and the Audit Trail

Recording. Composed entirely in the initiator's browser; never uploaded. Two-party consent flow: every participant is notified and must accept before recording starts. A

persistent banner shows when recording is active. Output may be saved as a standard video file or encrypted with AES-256-GCM for safe cloud storage.

Triangle Authentication™ for digital signatures. When a document is signed in RegSecure, three independent factors are bound cryptographically into a single signature certificate: (1) a **biometric** webcam snapshot of the signer, (2) the **video** session context with timestamps, and (3) the **document** SHA-256 hash. The certificate, generated client-side, contains the document hash, signer identity, timestamps, snapshot, audit log, and binding proof. Signatures verified with platform biometrics carry a stronger forensic-grade flag than those captured via in-app confirmation alone.

Audit log. Every notable event — session start, peer joined / left, admission, recording consent, document shared, signature applied, evidence downloaded — is logged in the FHIR AuditEvent format and linked into a hash chain so tampering is detectable. The log is held locally and may be downloaded as part of the evidence package.

7. Threat Model Summary

Threat	How RegSecure mitigates it
Server-side data breach	No user content is stored on our servers — there is nothing to breach.
Subpoena for server-held data	No data exists for RegSecure to produce.
Eavesdropping on a call	DTLS-SRTP encrypts media; ECDH + AES-256-GCM encrypt the data channel.
Cloud-storage breach of recordings	Recordings can be downloaded encrypted (AES-256-GCM) using the user's own key.
Lost device	Master key is sandboxed in the browser; encrypted files are useless without the key.
Lost master key	Shamir 3-of-5 backup allows recovery from any three custodial shares.
Hidden recording	Recording requires explicit consent from every participant.
Session hijacking	Random session codes, host-controlled waiting room, peer-authenticated signalling.
Man-in-the-middle by the signalling relay	Out-of-band Safety Code lets participants verify their direct connection.
Malicious file transfers	Inbound files are size-capped, filename-sanitised, and checked against an executable-type denylist.
Unauthorised viewer in a relayed media path	Relayed media is end-to-end encrypted; the relay sees ciphertext only.

Acknowledged limitations. RegSecure cannot defend a device that is already controlled by an attacker; customers operate their own endpoint hygiene and SSO. Users should keep browsers patched. Once a recording is downloaded in plaintext, custody passes to the user.

---

8. Browser Support and Verification

RegSecure runs on modern desktop browsers — Chrome 85+, Firefox 79+, Safari 15+, Edge 85+ — with no plug-in required. Mobile browsers are supported on a best-

effort basis; we recommend desktop for sessions that involve recording or document signing.

The cryptographic claims in this document are exercised by an automated test suite that runs on every code change. Tests cover key derivation, frame-level encryption and tamper detection, Shamir share recovery, audit-chain integrity, the Safety Code derivation, filename sanitisation, executable-type filtering, and ICE-server configuration. Customers performing a security review may request the detailed technical architecture document and access to the test results under NDA.

Contact. All enquiries — security, compliance, and procurement: **contact@regsecure.com**.

RegSecure — Compliance-ready video and digital signatures for regulated industries.