HIPAA & Security Overview

MyoSimplified — practice management for orofacial myofunctional therapy. Prepared for IT consultants and compliance reviewers evaluating the platform on behalf of a practice.

Your practice is the Covered Entity. MyoSimplified is your Business Associate. We execute a Business Associate Agreement with every practice, on every plan — HIPAA coverage is included, never sold as an add-on. Our own subprocessors that touch PHI operate under BAAs with us, so the vendor chain is covered end to end.

PROTECTING THE DATA ITSELF

Encryption at rest	All PHI, attachments and database backups are encrypted with AES-256.
Encryption in transit	Modern TLS (1.2+, TLS 1.3 where supported) on every session and transfer. PHI-bearing email is delivered through HIPAA-compliant infrastructure; SMS reminders are minimal-content by design.
Tenant isolation	Each practice's data is isolated by row-level security enforced in the database itself — separation is a property of the data layer, not only the application.
Role-based access control	Practitioners, front-desk staff and billers see only what their role requires, with granular clinical and financial permissions.
Append-only audit logging	Views, edits, creations, exports and deletions of PHI captured with user identity and timestamp. Logs cannot be silently altered.
Session protection	Automatic idle timeouts and stale-session checks on both portals, for shared and family devices.
Two-factor authentication	App-based TOTP on every account. Active sessions are listed so an owner can revoke a device they no longer use.

HOW WE OPERATE

Business Associate Agreements	Executed with every practice on every plan, and with every subprocessor that touches PHI.
Written policies	A documented set covering risk assessment, breach notification, contingency, retention and access control. Available to a practice or its reviewer on request.
Breach notification	A documented incident response and breach notification procedure. Affected practices are notified without unreasonable delay, so they can meet their own obligations under the Breach Notification Rule.
Retention and deletion	A documented retention schedule governs how long records are kept and what happens if a practice leaves. Clinical records outlive a subscription; the practice decides when they go.
Your data stays yours	Export the entire practice — clients, notes, documents, invoices — at any time, in open formats, without asking us. A single client's record can be exported alone to satisfy a patient access request.
No third-party tracking	The authenticated application carries no third-party analytics, advertising trackers or external error-reporting services. Application errors are handled in-house.

SUBPROCESSORS

Function	What they handle	BAA
Hosting	Vercel — application hosting and edge delivery. US regions.	Yes
Database and storage	Supabase, on AWS — encrypted database and file storage for practice and client records. US regions.	Yes
Email delivery	Amazon Web Services (SES) — PHI-bearing and transactional email, with TLS required on delivery.	Yes
Practice's own mailbox	Google — where a practice connects its own Google Workspace account to send from its own address. Mail travels through that practice's mailbox. Personal accounts cannot be connected.	Practice's own
SMS delivery	Twilio — appointment reminders. Minimal-content by design; no clinical detail in a message. Moving to Amazon Web Services (End User Messaging).	Yes
Telehealth video	Amazon Web Services (Chime SDK) — encrypted video sessions. Calls are not recorded by the platform.	Yes
Payments	Stripe — card processing and payouts. Amount and billing details only; no clinical information, and card numbers never reach our servers.	Not required — no PHI
Shipping and fulfilment	Shippo — labels and carrier rates for physical items. Name and delivery address only; no clinical information.	Not required — no PHI

Current as of September 2026. Every subprocessor that receives PHI operates under a BAA with MyoSimplified; those that do not are marked as such rather than omitted. Practices under BAA are notified of changes; the current list is at myosimplified.com/security.

CERTIFICATION POSTURE

There is no such thing as HIPAA certification — it is a program, not a certificate. Our status is stated plainly so a reviewer can judge it.

Today	HIPAA-aligned platform with the safeguards above in production. BAA executed with every practice.
Underway	Formal program documentation aligned to the NIST Cybersecurity Framework. International privacy readiness — GDPR for the EU and UK, and the Canadian provincial health privacy requirements. Practices outside the United States should talk to us before signing up, so we can confirm what we support today.
Planned	SOC 2 Type I, then SOC 2 Type II, then HITRUST — driven by health-system and hospital requirements. None are held today, and no dates are published: a date we might miss is worth less to you than an honest status.

Security questions, subprocessor registry, BAA requests and vulnerability reports: security@myosimplified.com | myosimplified.com/security