Privacy Policy

How NarrateEMS collects, uses, processes, and protects information

NarrateEMS Inc. provides EMS documentation software. This Privacy Policy describes the information NarrateEMS processes and how it is used and protected. When NarrateEMS processes PHI for a Covered Entity, the Business Associate Agreement additionally governs that processing.

1. Information collected

- Account and organization information such as name, email, role, squad/agency name, and squad membership.
- Subscription and billing metadata. Payment-card details are processed by Stripe and are not intentionally stored by NarrateEMS.
- Authentication, security, operational, error, and audit information reasonably necessary to operate and secure the Service.

2. Patient and clinical information

In the current production voice workflow, audio may be transmitted securely to Microsoft Azure Speech for transcription. Transcript and structured clinical information may then be processed through Microsoft Azure AI services and approved PHI subprocessors, including Groq where applicable, to generate documentation and provide related service functions. NarrateEMS is designed to minimize persistent PHI storage. The ordinary account/subscription database is not intended to store patient care records, and Supabase is used for non-PHI account, authentication, squad, and subscription data.

3. Use of information

- Provide and operate accounts and squad functionality.
- Generate and populate documentation requested by authorized users.
- Authenticate users and enforce access controls.
- Process subscriptions and billing.
- Troubleshoot failed or poor-quality documentation experiences and improve reliability.
- Detect, investigate, and respond to security incidents.
- Communicate about support, service changes, and contractual matters.
- Comply with legal and regulatory obligations.

4. AI training

NarrateEMS does not intentionally use customer PHI to train general-purpose AI models.

5. Retention

- Account, organization, subscription, and business records may be retained while active and thereafter as reasonably necessary for legal, tax, security, dispute, and recordkeeping needs.
- Production troubleshooting logs containing chart information may be retained in Microsoft Azure for up to 30 days under automatic retention controls, unless a specific incident, legal hold, or legal obligation requires longer preservation.
- The current client workflow is designed not to persist PHI after the applicable session refresh/clear process. Customers remain responsible for securing their own devices, browser profiles, and ePCR systems and for not intentionally leaving patient information available to subsequent users on shared devices.

6. Security

NarrateEMS uses safeguards designed to protect information, including encrypted transport, access controls, security logging/auditing, risk assessment, vendor review, incident response, and workforce security practices. No method can guarantee absolute security.

7. Vendors

Current material providers include Microsoft Azure for speech, AI, logging, and related cloud functions; Groq for approved PHI-processing functions where used; Supabase for non-PHI account, authentication, squad, and subscription infrastructure; and Stripe for billing/payment services. NarrateEMS evaluates vendors according to the data they receive and uses appropriate contractual safeguards, including BAAs where required.

8. HIPAA

- Where NarrateEMS acts as a Business Associate, the Covered Entity must execute a BAA before PHI processing.
- Questions involving a customer’s PHI should generally be directed through the applicable EMS agency, subject to the BAA and HIPAA Rules.

9. Requests and contact

Users may contact narrateems@gmail.com regarding account information held by NarrateEMS. Requests are subject to identity verification and applicable legal, contractual, and retention obligations. Website: www.narrateems.com