PangeaEmr Privacy Policy

Last Updated: February 2026

PangeaEMR ("PangeaEMR," "we," "us," or "our") is a HIPAA-compliant healthcare technology company. We provide electronic health record (EHR) software, medical billing services, credentialing services, RPM services, AI Scribe, Prior Auth, review and reputation management tools, and payment processing platforms (collectively, the "Services") to healthcare providers, clinics, and their patients.

This Privacy Policy explains how we collect, use, disclose, and safeguard information, including Protected Health Information (PHI), when you use our Services. This policy is modeled in part on industry standards and healthcare platform practices and is intended to comply with applicable U.S. federal and state privacy laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

---

1. Scope of This Privacy Policy

This Privacy Policy applies to:

- Clinics, providers, and healthcare organizations that use PangeaEMR
- Patients whose information is stored or processed through PangeaEMR
- Visitors to our websites and portals
- Users who create accounts directly with PangeaEMR

This policy does not apply to information collected by third parties that integrate with PangeaEMR, which are governed by their own privacy policies.

---

2. Our Role Under HIPAA

Depending on the context:

- Clinics and providers are the Covered Entities under HIPAA.
- PangeaEMR acts as a Business Associate when we create, receive, maintain, or transmit PHI on behalf of a Covered Entity.

We enter into Business Associate Agreements (BAAs) with our clinic and provider customers as required by HIPAA.

---

3. Information We Collect

3.1 Protected Health Information (PHI)

We may collect, store, and process PHI as directed by healthcare providers or entered by patients, including but not limited to:

- Patient names, addresses, phone numbers, and email addresses
- Dates of birth, gender, and demographic data
- Medical history, diagnoses, treatment notes, medications, allergies, lab results, and clinical documentation
- Insurance details, policy numbers, payer information, and claims data
- Appointment details and care coordination information

PHI may be:

- Entered by clinic staff
- Submitted by patients through patient portals or intake forms
- Generated as part of clinical care, billing, or operational workflows

We do not collect or store biometric identifiers or biometric information.

3.2 Payment and Billing Information

For billing and payment processing, we may collect:

- Insurance eligibility and claims data
- Explanation of Benefits (EOBs)
- Payment transaction data

Payment card information is processed through PCI-DSS-compliant third-party payment processors. PangeaEMR does not store full credit card numbers.

3.3 Account and User Information

We may collect:

- Usernames, passwords (hashed and encrypted)
- Roles, permissions, and audit logs
- Contact information for providers, staff, and administrators

When patients create an account themselves, they explicitly agree to this Privacy Policy and our Terms of Service at the time of registration.

3.4 Communications Data (SMS, Email, Notifications)

We may collect:

- Phone numbers and email addresses
- Message delivery status and timestamps
- User communication preferences

SMS Messaging Notice:

- SMS and data rates may apply
- Message frequency may vary
- Clinics are solely responsible for obtaining proper patient consent before initiating SMS communications using our Services

3.5 PHI Data Residency and Platform Restriction

All Protected Health Information (PHI) and Personally Identifiable Health Information (PHI/PII) processed through PangeaEMR remains within the PangeaEMR platform at all times. Specifically:

- PHI is not exported, transferred, or stored outside of the PangeaEMR environment except as required to provide Services (e.g., claims submission, payment processing, or regulatory reporting)
- Clinics and users do not have the ability to transmit PHI via unrestricted messaging or external communication channels within the platform
- All access, storage, and transmission of PHI is governed by PangeaEMR's security controls, audit logging, and HIPAA-compliant safeguards

PangeaEMR acts as a HIPAA Business Associate and maintains PHI in accordance with applicable federal and state healthcare privacy laws and executed Business Associate Agreements.

3.6 Website and Technical Information

We may automatically collect:

- IP addresses
- Browser type and device information
- Log files and usage analytics
- Cookies and similar technologies

This information is used for security, performance, and system improvement purposes.

---

4. How We Use Information

We use information to:

- Provide, maintain, and improve the Services
- Support clinical documentation and patient care
- Process claims, billing, and payments
- Support credentialing and enrollment workflows
- Enable patient portals and communication tools
- Comply with legal, regulatory, and contractual obligations
- Perform audits, security monitoring, and fraud prevention

We use PHI only as permitted by HIPAA, applicable law, and our agreements with Covered Entities.

---

5. SMS Messaging Restrictions and Data Residency Clause

SMS Messaging Controls and A2P Compliance
PangeaEMR enforces strict controls on all SMS communications sent through the platform. Clinics, providers, and their staff cannot freely compose or send arbitrary or free-text SMS messages to patients.
All SMS communications :

- Use pre-approved message templates
- Are associated with an approved A2P 10DLC messaging campaign
- Comply with applicable carrier, CTIA, TCPA, and regulatory requirements

Message content is limited to approved use cases such as appointment reminders, care notifications, billing alerts, and other healthcare-related communications consistent with the approved campaign registration.
Clinics are solely responsible for:

- Obtaining valid patient consent for SMS communications prior to use
- Ensuring patient opt-in records are accurate and maintained
- Honoring opt-out requests (e.g., STOP responses) as required by law

Message and data rates may apply. Message frequency may vary.

---

6. How We Use and Disclose Information

We do not sell, rent, or share patient information or consumer data with third parties for marketing or promotional purposes.

6.1 With Healthcare Providers

Protected Health Information (PHI) is only made available to the clinic or provider responsible for the patient's care, as required for treatment, payment, or healthcare operations under HIPAA.

6.2 With Infrastructure Service Providers

We use secure third-party vendors solely to support our technology infrastructure, including:

- Cloud hosting (e.g., Google Cloud Platform)

These vendors:

- Act only as data processors
- Do not receive or use data for their own marketing purposes
- Do not sell or share data
- Are contractually required to protect data

- Sign Business Associate Agreements (BAAs) where applicable

6.3 SMS and Communication Data

We do not sell, share, or disclose SMS opt-in data, phone numbers, or messaging consent information to third parties or affiliates for marketing or promotional purposes.
SMS opt-in data is used solely for communication with the patient regarding their healthcare services.

6.4 Legal and Regulatory Requirements

We may disclose information if required by law, court order, subpoena, or regulatory authority.

6.5 Business Transfers

If PangeaEMR is involved in a merger, acquisition, or asset sale, information may be transferred subject to confidentiality and HIPAA obligations.

---

7. Data Security

We maintain administrative, technical, and physical safeguards designed to protect information, including:

- Encryption at rest and in transit
- Role-based access controls
- Audit logging and monitoring
- Regular security assessments
- Secure cloud infrastructure

Despite our safeguards, no system can be guaranteed 100% secure.

---

8. Data Retention

We retain information:

- As required by law and regulation
- As specified in contracts with Covered Entities
- As necessary to provide the Services

PHI is retained in accordance with HIPAA and applicable state medical record retention laws.

---

9. Patient Rights

Patients have rights under HIPAA, including the right to:

- Access their medical records
- Request corrections
- Request restrictions on certain uses or disclosures
- Receive an accounting of disclosures

Requests should generally be directed to the clinic or provider. PangeaEMR assists Covered Entities in fulfilling these requests.

---

10. Children’s Privacy

PangeaEMR does not knowingly collect information directly from children except as part of healthcare services provided by a Covered Entity.

---

11. International Use

Our Services are intended for use in the United States. Data is stored and processed in accordance with U.S. healthcare privacy laws.

---

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Updates will be posted with a revised "Last Updated" date.

---

13. Contact Information

If you have questions about this Privacy Policy or our privacy practices, contact:
PangeaEMR
Email: support@pangeaemr.com

By using PangeaEMR, you acknowledge that you have read and understand this Privacy Policy.