Empathia AI - Privacy and Compliance Summary

Version: October 2025 | **Prepared by:** Empathia AI Inc.
Website: https://empathia.ai | **Trust Center:** https://trust.empathia.ai

1. Overview

Empathia AI is a HIPAA-compliant, SOC 2-Type II and ISO 27001-certified platform that uses AI to transcribe and summarize clinical encounters into structured notes. It is designed to enhance clinician efficiency, accuracy, and workflow while maintaining the highest standards of privacy and security. Empathia AI operates under robust privacy, security, and breach-response frameworks aligned with HIPAA, HITECH, and U.S. federal healthcare IT requirements.

2. Data Collection and Use

Empathia AI collects limited provider and encounter data - including clinician identifiers, audio recordings, and notes - solely to enable secure, AI-assisted transcription and clinical note generation. Clinicians obtain explicit patient consent before use, and patients may opt out at any time.

3. Privacy and Security Measures

Encryption: All PHI and PII are encrypted both in transit (TLS 1.2+) and at rest (AES-256). Encryption keys are securely managed through AWS Key Management Service (KMS) and authorized Empathia administrators, ensuring continuous protection of sensitive data.

Data Residency & Processing: All U.S. user data are stored and processed exclusively in HIPAA-compliant AWS and Microsoft Azure data centers located within the United States, ensuring full compliance with federal data residency and privacy requirements.

Access Controls: Access to PHI/PII is strictly limited to authorized personnel through role-based access controls. All administrative actions are logged and auditable, while strong password policies and automatic session timeouts are enforced to maintain system security.

Vendor Management: Empathia requires all third-party service providers to sign Business Associate Agreements (BAAs) and undergo regular security, privacy, and compliance reviews to uphold HIPAA and organizational standards.

Data Minimization & Purpose Limitation: Only the minimum personal data required for core functionality is collected. The AI system operates in a stateless mode, meaning no input or output data are stored without explicit consent.

De-Identification:
Data used for limited quality assurance purposes are de-identified in accordance with HIPAA Safe Harbor standards, with re-identification strictly prohibited under company policy.

4. AI System and Safeguards

- Purpose: To convert clinician–patient dialogue into high-quality, structured documentation (e.g., SOAP notes).
- Processing: AI models process data in real time and do not retain PHI/PII after task completion.
- Fairness and Accuracy: Continuous evaluation of model performance, accuracy, and bias mitigation.
- Transparency: Providers are informed of AI use; they review and sign off on all notes.
- Training Data: No client PHI/PII is used to train Empathia AI's models.

5. HIPAA Breach Notification Policy (Summary)

Applies to all Empathia AI personnel and partners handling PHI. Any suspected or confirmed incidents must be promptly reported to the Privacy Officer for assessment under HIPAA. In the event of a confirmed breach, affected individuals, HHS, and (if required) media are notified within 60 days, outlining the incident, data involved, and mitigation steps. Empathia maintains 24/7 monitoring and incident response. Security incidents are triaged within 24 hours and fully investigated per the Breach Notification Policy. All breaches are documented and retained for six years, with annual summaries reviewed by leadership. Staff receive annual HIPAA and breach-response training; good-faith reporting is protected, and violations may result in disciplinary action.

6. Certifications and Compliance

Empathia AI maintains:

- SOC 2 Type II Certification – covering Security, Availability, and Confidentiality
- ISO 27001 Certification – Information Security Management System
- HIPAA / HITECH Compliance Program
  Annual independent audits and continuous monitoring of data security and privacy controls

See our current attestations and documentation at the **Empathia Trust Center**.

7. Contact Information

Empathia AI Inc.
Email: info@empathia.ai | Website: https://empathia.ai
Privacy Officer: Dr. Yang Huang | Email: po@empathia.ai