11AI HIPAA Privacy and Security Policy

Understanding HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law enacted to protect the privacy and security of individuals' medical information. HIPAA establishes standards for the handling of Protected Health Information (PHI), ensuring that sensitive health data is safeguarded against unauthorized access and breaches.

Privacy & Security Commitment

At 11AI, we prioritize the confidentiality and security of PHI. We comply with HIPAA regulations to provide a secure environment for the collection, storage, and processing of PHI, thereby ensuring the trust and safety of both clinicians and patients.

Patient Information

- **Data Encryption:** Patient information is always encrypted at rest and during transfer to protect against unauthorized access.
- **Data Retention:** Patient recordings and notes can be manually deleted by the user at any time. Additionally, all patient data will be deleted if the user account is terminated. We ensure that data retention policies comply with HIPAA requirements, allowing users to manage their data securely.

Compliance and Internal Audit

- **Risk Assessments:** 11AI conducts regular risk assessments and reviews vendor security practices to ensure policies are up-to-date and relevant.
- **Vendor Management:** All vendors who may have access to patient information must be HIPAA compliant and have signed Business Associate Agreements (BAAs) with 11AI.
- **Privacy and Security Oversight:** Our Chief Technology Officer (CTO) is responsible for overseeing privacy and security practices.

Secure Development Lifecycle

- **Compliance Review:** All software developments, and changes are thoroughly reviewed and audited for HIPAA compliance.
- **Model Training:** All engineers complete training in secure development practices, ensuring adherence to HIPAA standards in software structure and dependencies.

Cloud Hosting and Availability

- **AWS Hosting:** Our software and database are hosted on Amazon Web Services (AWS), utilizing their robust security measures to protect data and ensure high availability.
- **Data Security:** Our databases are hosted on AWS RDS and S3, with encryption applied to data at rest and during transfer, in compliance with HIPAA requirements.

Artificial Intelligence

- **HIPAA-Compliant AI Models:** 11AI utilizes OpenAI models and infrastructure, ensuring all AI models comply with HIPAA and do not retain data.
- **Data Usage:** Protected Health Information (PHI) is never used for AI training purposes, maintaining patient confidentiality.

Internal Personnel Security

- **Background Checks**: All 11AI employees undergo background checks before being hired to ensure a secure and trustworthy workforce.
- **Training**: Employees complete annual security and HIPAA training to maintain awareness and compliance with privacy and security standards.