ClinicPix Privacy and Data Use Policy ("Policy")

Effective Date: 18 April 2025

1. Overview

ClinicPix is a secure medical image-sharing platform designed to facilitate safe communication between healthcare providers and patients. This Policy outlines how we collect, use, store, and protect sensitive health information, in accordance with HIPAA and other applicable privacy laws.

2. Data Collection and Use

ClinicPix collects and processes the following categories of data:

- **Patient Information**: Name, email, phone number, date of birth, and medical image access history
- **Provider Information**: Name, email, role, associated patient assignments
- **Medical Images**: X-rays, scans, or other health-related imagery uploaded by authorized providers
- **Audit Logs**: Timestamps of access, uploads, deletions, profile updates, and sharing activity

This data is used strictly to support clinical collaboration and patient care.

3. Patient Consent and Authorization

By creating an account on ClinicPix, **patients acknowledge and agree** that their assigned healthcare providers may share medical images with them through the platform for clinical and treatment purposes.

- This consent is **inferred at the time of signup** by accepting this Policy.
- Patients may **view and download** only the images explicitly shared with them by their assigned provider.
- Patients may revoke access or request account deletion at any time by contacting the ClinicPix Privacy Officer.

4. Provider-Specific Responsibilities

Healthcare providers using ClinicPix are additionally responsible for:

- **Handling patient information with discretion**, especially in shared environments or on mobile devices
- **Not downloading or storing PHI locally** unless required for immediate care and properly secured

- **Avoiding sharing screenshots or printed copies of patient data** unless explicitly authorized by the patient
- Ensuring devices used to access ClinicPix are secured with passcodes and up-to-date security software
- **Not reassigning or unassigning patients without proper documentation** or patient awareness

Failure to adhere to these responsibilities may result in suspension or removal from the platform.

5. Access Control

- Role-based access control (RBAC) is strictly enforced:
  - **Providers** may only access the information and images of their assigned patients
  - **Patients** may only view/download their own shared images
  - **Admins** can manage user accounts but do **not** have access to patient health data or images

6. Data Security

ClinicPix implements the following security measures:

- **Encryption in Transit and at Rest**:
  - HTTPS is enforced for all data transmission
  - AWS S3 objects are encrypted using **SSE-KMS** (AWS Key Management Service)
- **IAM Roles**:
  - EC2 instances run with strict IAM role permissions
  - Root AWS access is disabled for production systems
- **Authentication**:
  - Passwords are hashed using bcrypt
  - Multi-factor OTP login is required for account access
- **Secure Communication**:
  - ClinicPix only transmits PHI over secure HTTPS channels
  - No email-based image sharing is permitted unless through HIPAA-compliant systems

7. Device and Physical Security

All users accessing ClinicPix from desktops, laptops, or mobile devices must take appropriate precautions to protect data:

- Devices should be password-protected or biometrically secured
- Users must avoid storing patient information locally unless encrypted and required for immediate care
- Public or shared devices should not be used to access PHI unless through secure, time-limited sessions

- Users must log out after use on shared machines

8. Audit Trails

ClinicPix logs all critical activity, including:

- Login attempts and OTP verification
- File uploads, deletions, sharing, and views
- Profile and password changes
- Patient assignments

Audit logs are stored securely and retained for forensic and compliance purposes.

9. Data Retention and Disposal

- Medical image and audit log data is retained for **six years**, in compliance with HIPAA regulations
- Upon user account deletion or data expiration, all PHI is securely deleted from storage and database backups in accordance with AWS and ClinicPix procedures

10. Hosting Infrastructure and BAA Coverage

ClinicPix uses the following cloud services:

- **Amazon Web Services (AWS)**: Used for backend, EC2, S3, and database hosting
    - A formal Business Associate Agreement (BAA) with AWS will be executed if the platform moves into production with PHI.
- **Render**: Used only for hosting static frontend assets (Angular application)
    - Render does **not** process or store PHI
    - All PHI is accessed via API calls to the EC2-hosted backend on AWS

11. De-identification for Research Use

If medical images are ever used for research, education, or demonstration purposes:

- All personally identifiable information (PII) is removed from metadata and filenames
- De-identified images will not be associated with patient accounts or profiles

12. User Responsibilities

All users (patients, providers, admins) agree to:

- Use ClinicPix only for lawful and authorized purposes
- Not attempt to access data outside their role's permissions
- Immediately report any suspected breach or misuse

13. Policy Updates

ClinicPix may update this Policy periodically. Users will be notified of any material changes, and continued use of the platform constitutes acceptance of the updated policy.

14. Contact

For privacy questions or requests (e.g., data deletion, consent revocation), contact:

ClinicPix Privacy Officer
Email: clinicpix.system@gmail.com