Medreception AI

CONFIDENTIAL | COMPLIANCE DOCUMENT

Version 1.1 | Effective Date: June 2025

# MedReception AI – HIPAA Privacy & Security Policy

Applies To: All employees, including executives, contractors, vendors, and third-party service providers with access to MedReception systems and Protected Health Information (PHI)

## 1. Purpose

This policy establishes how MedReception AI, as a Business Associate, protects the privacy and security of Protected Health Information (PHI) in compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

## 2. Scope

This policy applies to all MedReception AI employees, contractors, vendors, and systems (including AI agents such as Katie AI and Annie AI) that access, process, transmit, or store PHI on behalf of HIPAA-covered entities.

## 3. Definitions

**PHI**: Protected Health Information – any individually identifiable health information held or transmitted in any form.

**Covered Entity**: A health care provider, health plan, or clearinghouse that transmits health information electronically.

**Business Associate**: A person or entity performing functions involving PHI on behalf of a Covered Entity.

## 4. Responsibilities

MedReception AI designates a Privacy and Security Officer responsible for implementing, maintaining, and enforcing this policy.

## 5. Administrative Safeguards

HIPAA training is required at onboarding and annually for all team members.

Access to PHI is based on the “minimum necessary” standard.

Business Associate Agreements (BAAs) are executed with all clients and relevant vendors.

Disciplinary actions are taken in response to any HIPAA violations.

## 6. Physical Safeguards

Servers and infrastructure are located in secure, access-controlled environments.

Workstations and mobile devices used to access PHI are password-protected and locked when unattended.

No PHI is stored on employee-owned personal devices.

## 7. Technical Safeguards

All PHI is encrypted in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent).

Role-based access controls and multi-factor authentication are required for internal systems.

Audit logs are reviewed regularly to detect unauthorized access.

## 8. AI-Specific Measures

AI agents are designed to follow structured workflows that minimize unnecessary PHI collection.

AI-generated transcripts and call data are securely stored, encrypted, and purged on a scheduled basis.

AI agents automatically escalate calls to human staff when needed, such as during distress or complex issues.

## 9. Breach Notification

In the event of a breach involving unsecured PHI:

MedReception AI will notify affected clients **without unreasonable delay and no later than 60 calendar days** after the breach is discovered.

Notification will include a description of the breach, the type of PHI involved, steps taken to investigate and mitigate harm, and preventive measures going forward.

MedReception AI will fully cooperate with client-specific breach notification procedures as required by law.

## 10. Policy Review

This policy will be reviewed and updated at least annually or when significant operational or regulatory changes occur.

## 11. Acknowledgment

All employees, contractors, and applicable vendors must review and sign this policy to confirm understanding and compliance. Digital acknowledgment and date-stamped records are maintained.