HIPAA PRIVACY AND SECURITY POLICY
Method Ketamine Therapy

Legal Entity: Serenity Wellness & Infusion LLC
DBA: Method Ketamine Therapy
Address: 401 S Mill Ave #204, Tempe, AZ 85281

HIPAA Privacy Officer: James Jett Summers – Manager
HIPAA Security Officer: James Jett Summers – Manager

1. Purpose

This policy establishes safeguards to protect Protected Health Information (PHI) generated during ketamine-assisted therapy services.

The practice complies with all requirements under the Health Insurance Portability and Accountability Act (HIPAA).

2. Scope

This policy applies to all workforce members including:

• Medical Director
• Prescribing provider (Nurse Practitioner)
• Registered Nurse
• Administrative staff
• Front desk staff

3. Electronic Medical Records

All patient records are maintained electronically using the Boulevard practice management system.

The system manages:

• intake documentation
• treatment records
• scheduling
• billing
• automated reminders

4. Patient Communications

Patients may communicate with the practice through:

• phone calls
• secure patient portal
• email communications through Google Workspace

Text messaging is used only for appointment reminders.

Clinical discussions are not conducted via SMS.

5. Telehealth

Telehealth may occasionally be used for:

• follow-up visits
• integration discussions
• treatment consultations

All telehealth interactions must occur through secure HIPAA-compliant platforms.

6. Clinical Monitoring Cameras

For patient safety during ketamine-assisted therapy sessions, monitoring cameras are installed in designated treatment rooms.

These cameras are used solely for patient safety monitoring during active treatment sessions.

Monitoring is limited to authorized clinical staff.

Recordings, if stored, are treated as Protected Health Information and secured accordingly.

7. Workforce Access Controls

Access to PHI is limited based on job duties.

Clinical staff:
• Medical Director
• Nurse Practitioner
• Registered Nurse

Administrative staff:
• Front desk
• administrative staff
• practice manager

Employees may only access PHI necessary for their role.

8. Technical Safeguards

The organization uses the following safeguards:

• encrypted electronic records
• unique user login credentials
• password protection
• audit logging
• automatic logoff features

Access is restricted to clinic-managed devices.

9. Physical Safeguards

Security measures include:

• secured treatment areas
• password-protected computers
• restricted access to clinical spaces
• security cameras in common areas

10. Network Security

The clinic operates:

• a secure staff network
• a separate guest WiFi network

Only the staff network may access PHI systems.

11. Business Associates

Business Associate Agreements are maintained with vendors that may access PHI including:

• Boulevard EMR
• Google Workspace
• Cherry financing platform

12. Data Retention

Patient medical records are retained for at least seven years following the last patient visit.

13. Breach Reporting

Any suspected privacy breach must be reported immediately to the HIPAA Officer.

Incidents will be investigated and addressed according to federal requirements.

14. Workforce Training

All staff must complete HIPAA training upon hire and annually thereafter.

Training is administered by the HIPAA Officer.

15. Policy Enforcement

Failure to follow HIPAA requirements may result in disciplinary action, including termination of employment.

Effective Date: _____

Approved By:
James Jett Summers
HIPAA Privacy & Security Officer