MySleepScoring™

Corporate Compliance & Information Security Program

Volume 1 – Corporate Governance Manual

Version 1.0 | Effective July 6, 2026 | Internal Confidential

1. Purpose

The purpose of this manual is to establish the governance framework for MySleepScoring™.

It defines leadership responsibilities, compliance oversight, quality expectations, information security governance, and organizational accountability.

It applies to all workforce members, contractors, and business associates.

2. Mission & Vision

Deliver accurate, secure, and timely remote sleep scoring services.

Protect patient privacy while exceeding client expectations.

Become a nationally recognized provider of outsourced sleep scoring services.

3. Organizational Governance

The Chief Executive Officer has ultimate responsibility for governance.

A Compliance Officer oversees policies, audits, and investigations.

An Information Security Officer oversees cybersecurity.

A Quality Assurance Coordinator oversees inter-scorer reliability and competency.

4. Corporate Ethics

All personnel shall act honestly and professionally.

Patient confidentiality is mandatory.

Conflicts of interest must be disclosed.

Fraud, falsification, and unauthorized access are prohibited.

5. Compliance Program

Maintain written policies.

Conduct annual compliance reviews.

Investigate incidents.

Track corrective actions.

Maintain documentation for required retention periods.

6. Risk Management

Perform annual enterprise risk assessments.

Maintain a risk register.

Assign risk owners.

Review mitigation progress quarterly.

7. Quality Management

Follow current AASM scoring criteria required by each client.

Conduct peer reviews and ISR activities.

Document corrective actions.

Monitor turnaround times and quality metrics.

8. Information Security Governance

Protect confidentiality, integrity, and availability of company information.

Use least-privilege access.

Require MFA where available.

Encrypt company devices and approved data storage.

9. Workforce Responsibilities

Complete onboarding training.

Complete annual HIPAA and security training.

Immediately report incidents.

Protect company and client information.

10. Document Control

Every controlled document shall contain a version number, owner, effective date, review date, and revision history.

Superseded documents are archived and retained according to company policy.

11. Annual Management Review

Leadership reviews audit findings, client feedback, risk assessments, training completion, security incidents, and improvement opportunities annually.

Appendix A

Approval Page

CEO Signature: ___________________

Compliance Officer: ___________________

Review Date: ___________________