Regulatory Data Backup Policy for Healthcare

1. Purpose

This policy establishes the mandatory requirements for backup and recovery of all regulated healthcare data to ensure data integrity, availability, and compliance with applicable healthcare regulations.

2. Scope

This policy applies to all healthcare information systems, electronic health records, and other critical data assets managed by the organization.

3. Policy Statement

- All regulated healthcare data must be backed up regularly according to defined schedules.
- Backups must be encrypted and stored securely, both onsite and offsite.
- Backup retention periods must comply with relevant laws and regulations (e.g., HIPAA, regional health data acts).
- All backup and restore procedures must be documented and regularly tested.
- Access to backup data must be restricted to authorized personnel only.

4. Roles and Responsibilities

- **IT Department:** Manage, implement, and monitor backup solutions.
- **Compliance Officer:** Ensure policy alignment with current healthcare regulations.
- **All Staff:** Report data loss incidents or backup-related issues promptly.

5. Backup Frequency and Retention

- **Critical data:** Daily backups, with minimum retention of 7 years.
- **Non-critical data:** Weekly backups, with retention as required by policy.
- **Backup logs:** Retained for a minimum of one year.

6. Testing and Validation

- Backup media and restoration procedures must be tested at least quarterly.
- Test results shall be documented and reviewed for improvement.

7. Compliance

Failure to comply with this policy may result in disciplinary action and/or legal penalties as defined by applicable healthcare laws.

8. Review and Maintenance

This policy will be reviewed annually or as needed to reflect changes in regulations or operating circumstances.

9. Approval

Effective Date: _____

Approved By: _____