SecureHealth Inc. Data Governance Policy

Core Principles and Framework

1. Data Quality and Integrity

Policy Statement

SecureHealth Inc. is committed to maintaining the highest standards of data quality and integrity across all systems and processes.

Core Principles

- **Accuracy**: All data must be accurate, verified, and free from errors
- **Completeness**: Data records must contain all required fields and information
- **Consistency**: Data must be consistent across all systems and databases
- **Timeliness**: Data must be updated in real-time or according to defined schedules
- **Validity**: Data must conform to defined formats, ranges, and business rules

2. Data Accountability and Stewardship

Policy Statement

Clear ownership and accountability for data assets must be established at all organizational levels.

Core Principles

- **Data Ownership**: Each data asset must have a designated owner responsible for its quality
- **Stewardship**: Data stewards must be appointed for different data domains
- **Responsibilities**: Clear definition of roles and responsibilities for data management
- **Decision Rights**: Established framework for data-related decision-making
- **Performance Metrics**: Regular evaluation of data governance effectiveness

3. Data Security and Privacy

Policy Statement

All patient and organizational data must be protected according to HIPAA, GDPR, and other applicable regulations.

Core Principles

- **Confidentiality**: Access to sensitive data must be strictly controlled
- **Privacy by Design**: Privacy considerations must be incorporated into all data processes
- **Security Controls**: Implementation of appropriate technical and organizational measures
- **Data Classification**: All data must be classified based on sensitivity and criticality
- **Breach Prevention**: Proactive measures to prevent unauthorized access and data breaches

4. Data Accessibility and Sharing

Policy Statement

Data must be accessible to authorized personnel while maintaining security and privacy requirements.

Core Principles

- **Authorized Access**: Clear procedures for requesting and granting data access
- **Data Sharing Agreements**: Formal agreements for external data sharing
- **Documentation**: Comprehensive documentation of data structures and meanings
- **Standardization**: Use of standard formats and protocols for data exchange
- **Access Monitoring**: Regular review and audit of data access patterns

5. Data Lifecycle Management

Policy Statement

Data must be managed effectively throughout its entire lifecycle, from creation to disposal.

Core Principles

- **Data Creation**: Standards for data entry and acquisition
- **Data Storage**: Appropriate storage solutions based on data classification
- **Data Retention**: Clear policies for how long different types of data should be kept
- **Data Archival**: Procedures for archiving inactive data
- **Data Disposal**: Secure methods for data deletion and disposal

6. Regulatory Compliance

Policy Statement

All data management practices must comply with relevant healthcare regulations and standards.

Core Principles

- **HIPAA Compliance**: Adherence to all HIPAA requirements
- **GDPR Compliance**: Implementation of GDPR requirements where applicable
- **Documentation**: Maintenance of compliance documentation
- **Audit Readiness**: Preparation for regulatory audits
- **Training**: Regular compliance training for all staff

7. Data Risk Management

Policy Statement

A comprehensive approach to identifying, assessing, and mitigating data-related risks must be maintained.

Core Principles

- **Risk Assessment**: Regular evaluation of data-related risks
- **Risk Mitigation**: Implementation of controls to address identified risks
- **Incident Response**: Clear procedures for handling data incidents

- **Business Continuity**: Plans for maintaining data availability during disruptions
- **Risk Monitoring**: Continuous monitoring of risk indicators

8. Data Quality Monitoring and Improvement

Policy Statement

Regular monitoring and continuous improvement of data quality must be performed.

Core Principles

- **Quality Metrics**: Definition and tracking of data quality metrics
- **Quality Assessment**: Regular data quality assessments
- **Issue Resolution**: Process for addressing data quality issues
- **Continuous Improvement**: Regular review and updating of data quality processes
- **Stakeholder Feedback**: Integration of feedback from data users

Implementation and Enforcement

1. This policy applies to all employees, contractors, and third parties handling SecureHealth Inc. data
2. Regular training will be provided on these principles
3. Compliance with this policy will be monitored and enforced
4. The policy will be reviewed and updated annually
5. Violations will be subject to disciplinary action

Review and Updates

- Policy Review Date: Annually
- Last Updated: [Current Date]
- Next Review Due: [One Year from Current Date]