**SecureHealth Inc. Data Governance**

**Roles and Responsibilities Policy**

**1. Executive Level**

**1.1 Executive Steering Committee**

**Composition**: C-suite executives, including CEO, CIO, CISO, and CMO

**Responsibilities**:

* Provide strategic direction for data governance initiatives
* Approve data governance policies and standards
* Allocate resources for data governance programs
* Review and approve major data-related decisions
* Ensure alignment between data governance and business objectives

**1.2 Chief Data Officer (CDO)**

**Responsibilities**:

* Overall accountability for enterprise data strategy
* Lead the data governance program
* Report to executive steering committee on data governance progress
* Oversee data quality and compliance initiatives
* Coordinate with other C-level executives on data-related matters
* Final authority on data-related disputes

**2. Management Level**

**2.1 Data Governance Committee**

**Composition**: Department heads, senior managers, and key stakeholders

**Responsibilities**:

* Implement data governance policies
* Review and approve data standards
* Coordinate cross-departmental data initiatives
* Monitor compliance with data governance policies
* Resolve escalated data-related issues
* Report to CDO on governance implementation

**2.2 Data Security Manager**

**Responsibilities**:

* Implement data security controls
* Monitor security compliance
* Conduct security risk assessments
* Manage access control systems
* Respond to security incidents
* Coordinate with IT security team
* Train staff on security procedures

**2.3 Compliance Manager**

**Responsibilities**:

* Ensure HIPAA and GDPR compliance
* Maintain compliance documentation
* Conduct regular compliance audits
* Coordinate with legal department
* Manage regulatory reporting
* Update policies based on regulatory changes

**3. Operational Level**

**3.1 Data Stewards**

**Responsibilities**:

* Day-to-day data quality management
* Implement data standards in their domain
* Monitor data quality metrics
* Coordinate with data owners
* Report data quality issues
* Provide domain expertise
* Train end users on data procedures

**3.2 Data Owners**

**Responsibilities**:

* Accountable for specific data sets
* Define data access requirements
* Approve access requests
* Ensure data accuracy
* Coordinate with data stewards
* Maintain data documentation
* Define data retention requirements

**3.3 Database Administrators**

**Responsibilities**:

* Maintain database systems
* Implement technical controls
* Manage database performance
* Handle backup and recovery
* Monitor system health
* Implement security patches
* Support data migration efforts

**3.4 Data Analysts**

**Responsibilities**:

* Analyze data quality
* Generate reports
* Support data-driven decisions
* Identify data patterns
* Report anomalies
* Assist with data validation
* Support data improvement initiatives

**4. Support Level**

**4.1 IT Support Team**

**Responsibilities**:

* Provide technical support
* Maintain systems access
* Assist with data issues
* Support user training
* Document technical procedures
* Monitor system performance

**4.2 Privacy Officers**

**Responsibilities**:

* Monitor privacy compliance
* Handle privacy complaints
* Conduct privacy impact assessments
* Train staff on privacy procedures
* Review privacy policies
* Coordinate with legal team
* Manage consent procedures

**5. User Level**

**5.1 Data Users**

**Responsibilities**:

* Follow data governance policies
* Report data quality issues
* Maintain data confidentiality
* Complete required training
* Use data appropriately
* Protect access credentials
* Report security incidents

**6. Special Roles**

**6.1 Data Governance Office**

**Responsibilities**:

* Coordinate governance activities
* Maintain governance documentation
* Track governance metrics
* Facilitate governance meetings
* Support governance committees
* Manage governance communications
* Monitor governance effectiveness

**6.2 Audit Team**

**Responsibilities**:

* Conduct internal audits
* Review compliance
* Assess control effectiveness
* Report audit findings
* Track remediation efforts
* Validate corrections
* Maintain audit trails

**7. Implementation Guidelines**

1. **Role Assignment**:
   * Formal appointment process
   * Clear documentation of assignments
   * Regular review of roles
   * Backup personnel identified
   * Training requirements specified
2. **Accountability Measures**:
   * Regular performance reviews
   * Metrics for success
   * Reporting requirements
   * Escalation procedures
   * Consequence management
3. **Communication Channels**:
   * Regular status meetings
   * Reporting structures
   * Escalation paths
   * Collaboration tools
   * Documentation requirements

**8. Review and Updates**

* Policy Review Frequency: Annual
* Last Updated: [Current Date]
* Next Review: [One Year from Current Date]
* Review Responsibility: Data Governance Committee