**SecureHealth Inc.**

**HIPAA and GDPR Compliance Framework**

**1. Data Protection and Privacy Fundamentals**

**1.1 Protected Health Information (PHI) Definition**

* Patient names, addresses, and contact details
* Medical record numbers and health plan beneficiary numbers
* Social Security numbers and account numbers
* Biometric identifiers and full-face photographs
* Any other unique identifying numbers or characteristics
* All electronic protected health information (ePHI)
* Dates directly related to an individual's healthcare

**1.2 Special Categories of Personal Data (GDPR Article 9)**

* Health data
* Genetic data
* Biometric data
* Racial or ethnic origin
* Religious or philosophical beliefs
* Sexual orientation and history
* Mental health information

**2. Access Control Policies**

**2.1 Role-Based Access Control (RBAC)**

**Policy Requirements**:

* Minimum necessary access principle
* Role-based permission sets
* Regular access review and certification

**Implementation**:

Access Levels:

Level 1: View-only access to basic patient information

Level 2: View and modify basic patient information

Level 3: Full access to patient records

Level 4: Administrative access

Level 5: System administrator access

**Role Definitions**:

* Physicians: Level 3
* Nurses: Level 2
* Administrative Staff: Level 1
* IT Staff: Level 4
* System Administrators: Level 5

**2.2 Authentication Requirements**

**Mandatory Controls**:

* Multi-factor authentication (MFA) for all users
* Complex password requirements
* Password rotation every 90 days
* Account lockout after 3 failed attempts
* Automatic session timeout after 15 minutes
* Unique user identification
* Emergency access procedures

**3. Audit Logging and Monitoring**

**3.1 Required Audit Events**

**System Level**:

* User login attempts (successful and failed)
* Password changes
* System configuration changes
* Security policy modifications
* System startup and shutdown
* Backup and restore operations

**Data Level**:

* PHI access and viewing
* Data modifications
* Data exports and downloads
* Patient record creation/deletion
* Consent management changes
* Data sharing activities

**3.2 Audit Log Requirements**

**Log Contents**:

Mandatory Fields:

- Timestamp (UTC)

- User ID - Action performed

- Resource accessed

- Source IP address

- Success/Failure indication

- Affected patient ID (if applicable)

- Changes made (before/after values)

**Retention Period**:

* Minimum 6 years for HIPAA compliance
* Secure storage with encryption
* Regular backup of audit logs
* Tamper-evident logging

**3.3 Monitoring and Review**

* Real-time alerting for suspicious activities
* Daily automated log analysis
* Weekly manual review of significant events
* Monthly compliance reporting
* Quarterly audit log review

**4. Data Retention and Disposal**

**4.1 Retention Periods**

**Medical Records**:

* Adult patients: Minimum 6 years from last visit
* Pediatric patients: Until age 21 or 6 years from last visit
* Deceased patients: 2 years from date of death

**Administrative Records**:

* Payment records: 7 years
* Insurance claims: 10 years
* Employee records: 6 years post-employment
* Training records: 6 years

**System Records**:

* Audit logs: 6 years
* Security incidents: 6 years
* Access logs: 6 years
* System backups: 1 year

**4.2 Data Disposal Procedures**

**Electronic Data**:

* Secure wiping using DOD 5220.22-M standard
* Physical destruction of storage media
* Documented chain of custody
* Verification of destruction

**Physical Records**:

* Cross-cut shredding
* Secure disposal service
* Documented destruction certificates
* Witness verification

**5. Patient Rights and Consent**

**5.1 GDPR Rights Implementation**

* Right to access
* Right to rectification
* Right to erasure
* Right to restrict processing
* Right to data portability
* Right to object
* Rights related to automated decision making

**5.2 HIPAA Rights Implementation**

* Right to examine and obtain copies
* Right to request amendments
* Right to accounting of disclosures
* Right to request restrictions
* Right to confidential communications

**5.3 Consent Management**

**Requirements**:

* Explicit consent for data processing
* Separate consent for different purposes
* Easy withdrawal of consent
* Documentation of consent
* Regular consent review

**6. Security Controls**

**6.1 Encryption Requirements**

**Data at Rest**:

* AES-256 encryption for stored data
* Encrypted backup files
* Encrypted mobile devices
* Hardware security modules

**Data in Transit**:

* TLS 1.3 for all communications
* VPN for remote access
* Secure file transfer protocols
* End-to-end encryption

**6.2 Network Security**

* Network segmentation
* Intrusion detection/prevention
* Firewall configuration
* Regular vulnerability scanning
* Penetration testing

**7. Incident Response and Breach Notification**

**7.1 Incident Categories**

1. Unauthorized access
2. Data loss or theft
3. Malware infection
4. System compromise
5. Physical security breach

**7.2 Response Timeline**

**HIPAA Requirements**:

* 60 days maximum for breach notification
* 72 hours for initial assessment
* Immediate containment actions

**GDPR Requirements**:

* 72 hours for supervisory authority notification
* "Without undue delay" for data subject notification
* Immediate incident documentation

**8. Documentation and Training**

**8.1 Required Documentation**

* Privacy policies
* Security procedures
* Risk assessments
* Training materials
* Incident reports
* Audit results
* Compliance reviews

**8.2 Training Requirements**

* Initial privacy and security training
* Annual refresher training
* Role-specific training
* Incident response training
* Documentation of completion

**9. Compliance Monitoring and Review**

**9.1 Regular Assessments**

* Monthly security reviews
* Quarterly compliance audits
* Annual risk assessment
* External audits every 2 years

**9.2 Review Process**

* Policy effectiveness review
* Control testing
* Gap analysis
* Remediation planning
* Documentation updates

**10. Review and Updates**

* Framework Review: Annual
* Last Updated: [Current Date]
* Next Review: [One Year from Current Date]
* Policy Owner: Compliance Officer