Data Handling Policy Template

1. Purpose and Scope

1.1 Purpose

This policy establishes requirements for the secure handling of healthcare data throughout its lifecycle, from collection to disposal, ensuring compliance with HIPAA, HITECH, and other applicable regulations.

1.2 Scope

This policy applies to:

- All employees, contractors, and business associates
- All Protected Health Information (PHI) in any format
- All systems and applications that store, process, or transmit PHI
- All phases of AI/ML model development and deployment

2. Roles and Responsibilities

2.1 Privacy Officer

- Overall responsibility for privacy compliance
- Review and approval of data access requests
- Incident response coordination
- Policy maintenance and updates

2.2 Security Officer

- Implementation of technical safeguards
- Security risk assessments
- Access control management
- Security incident response

2.3 Data Stewards

- Data quality and integrity
- Metadata management
- Data lifecycle management
- User support and training

2.4 Data Users

- Compliance with data handling procedures
- Reporting security incidents
- Completing required training
- Using minimum necessary data

3. Data Classification

3.1 Classification Levels

Level 1: Public

- No identifiable patient information
- Aggregate statistics
- Published research findings **Handling**: No special restrictions

Level 2: Internal Use Only

- De-identified data
- Synthetic data for training
- Research datasets without PHI **Handling**: Internal access controls, encryption in transit

Level 3: Confidential

- Limited datasets with some identifiers removed
- Research data with partial de-identification **Handling**: Access controls, encryption at rest and in transit, audit logging

Level 4: Restricted (PHI)

- Protected Health Information
- Identified patient records
- Any data subject to HIPAA **Handling**: Strict access controls, encryption, comprehensive audit logging, special approval required

3.2 Classification Marking

All datasets must be clearly marked with their classification level in:

- File names or metadata
- Documentation
- System labels
- Email subject lines (when sharing)

4. Data Collection

4.1 Collection Principles

- Collect only data necessary for specified purpose
- Obtain appropriate consent or authorization
- Document legal basis for collection
- Ensure data quality at point of collection

4.2 Collection Methods

- Direct from patients (consent required)

- From healthcare providers (authorization required)
- From existing databases (data use agreement required)
- Generated synthetically (document methodology)

4.3 Data Quality Requirements

- Verify accuracy at collection
- Implement validation rules
- Document data source and lineage
- Establish completeness thresholds

5. Data Storage

5.1 Storage Requirements

Physical Storage

- Store in access-controlled facilities
- Implement environmental controls
- Maintain physical security logs
- Use locked cabinets for physical media

Electronic Storage

- Encrypt all PHI at rest (AES-256 or stronger)
- Use approved storage systems only
- Implement redundancy and backup
- Segregate production and development environments

5.2 Backup and Recovery

- Daily incremental backups
- Weekly full backups
- Monthly archive backups
- Quarterly disaster recovery testing
- Encrypted backup media
- Secure offsite backup storage

5.3 Retention Periods

- Active research data: Duration of project
- Completed research data: 7 years post-completion
- AI training data: 7 years or duration of model use
- Audit logs: 6 years minimum
- De-identification logs: 6 years minimum

6. Data Access

6.1 Access Control Principles

- Least privilege access
- Role-based access control (RBAC)
- Regular access reviews
- Automatic account expiration

6.2 Access Request Process

1. Submit formal access request with justification
2. Manager approval
3. Privacy Officer review (for PHI)
4. Security Officer provisioning
5. Documentation of access granted
6. Initial and ongoing training requirement

6.3 Authentication Requirements

- Unique user IDs (no shared accounts)
- Complex passwords (12+ characters, mixed case, numbers, symbols)
- Multi-factor authentication for PHI access
- Automatic logoff after 15 minutes of inactivity
- Account lockout after 5 failed login attempts

6.4 Authorization Levels

- **Read Only**: View data, generate reports
- **Read/Write**: Modify existing records
- **Admin**: Create/delete records, manage users
- **System Admin**: Full system access, configuration changes

7. Data Use

7.1 Minimum Necessary Standard

- Use only minimum PHI needed for task
- Limit access to specific fields when possible
- Use de-identified or synthetic data when sufficient
- Document justification for PHI access

7.2 Permitted Uses

- Treatment, payment, and healthcare operations
- Research with IRB approval and appropriate authorization
- AI/ML model training with proper safeguards
- Quality improvement with de-identified data
- Public health reporting as required by law

7.3 Prohibited Uses

- Marketing without authorization
- Sale of PHI

- Personal use
- Sharing with unauthorized parties
- Re-identification attempts

7.4 Special Considerations for AI/ML

- Document data used for model training
- Implement techniques to prevent model memorization of PHI
- Test models for data leakage
- Maintain human oversight for clinical decisions
- Provide explainability for AI-assisted decisions

8. Data Transmission

8.1 Encryption Requirements

- TLS 1.3 or higher for data in transit
- End-to-end encryption for email containing PHI
- VPN required for remote access
- Encrypted file transfer protocols (SFTP, HTTPS)

8.2 Email Guidelines

- Encrypt all emails containing PHI
- Use secure email gateway
- Include confidentiality notice
- Verify recipient before sending
- Avoid PHI in subject lines

8.3 Physical Transport

- Use encrypted portable media only
- Courier service for sensitive materials
- Chain of custody documentation
- Secure packaging

8.4 Cloud and Third-Party Services

- Business Associate Agreement required
- HIPAA-compliant services only
- Verify encryption and security controls
- Regular security assessments
- Data residency considerations

9. Data Sharing

9.1 Internal Sharing

- Verify recipient's need to know
- Use secure sharing mechanisms

- Maintain audit trail
- Limit sharing duration

9.2 External Sharing

- Business Associate Agreement required
- Data Use Agreement for research
- Verify recipient's security measures
- De-identify when possible
- Track all external disclosures

9.3 Research Collaborations

- IRB approval required
- Formal data sharing agreement
- De-identification preferred
- Limited dataset if de-identification not feasible
- Regular compliance monitoring

10. Data Disposal

10.1 Disposal Methods

Electronic Media

- Secure deletion (DoD 5220.22-M standard)
- Cryptographic erasure
- Physical destruction of media (degaussing, shredding)
- Certificate of destruction

Physical Media

- Cross-cut shredding (minimum 1/8" x 1/2")
- Incineration
- Pulverization
- Witnessed destruction

10.2 Disposal Schedule

- Disposed upon retention period expiration
- Annual review of data for disposal eligibility
- Secure disposal within 30 days of determination
- Documentation of all disposals

10.3 Disposal Documentation

- Date of disposal
- Method of disposal
- Data description

- Authorizing person
- Witness (for physical destruction)

11. Incident Response

11.1 Reportable Incidents

- Unauthorized access to PHI
- Loss or theft of devices containing PHI
- Inadvertent disclosure
- Malware or ransomware
- System breaches
- Suspected re-identification

11.2 Reporting Procedures

1. Immediately report to Security Officer
2. Document incident details
3. Preserve evidence
4. Do not discuss externally
5. Cooperate with investigation

11.3 Response Process

1. Contain incident
2. Assess scope and impact
3. Determine if breach notification required
4. Implement remediation
5. Document lessons learned
6. Update procedures as needed

12. Training and Awareness

12.1 Required Training

- HIPAA Privacy and Security (annual)
- Data handling procedures (annual)
- Role-specific training (as assigned)
- Security awareness (quarterly)

12.2 Training Documentation

- Training completion records
- Test scores (80% minimum to pass)
- Acknowledgment of policies
- Remedial training for failures

13. Monitoring and Auditing

13.1 Access Monitoring

- Review access logs weekly
- Investigate anomalous access patterns
- Monitor failed login attempts
- Track data exports and large queries

13.2 Compliance Audits

- Quarterly internal audits
- Annual external audits
- Regular policy compliance reviews
- Penetration testing (annual)

13.3 Audit Logs

- Retain for minimum 6 years
- Include: user ID, date/time, action, data accessed
- Protect log integrity (append-only)
- Regular log reviews

14. Policy Compliance

14.1 Violations

Violations of this policy may result in:

- Retraining requirement
- Access suspension
- Disciplinary action up to termination
- Legal action
- Regulatory penalties

14.2 Sanctions

- First violation: Written warning and retraining
- Second violation: Suspension of access and formal review
- Third violation: Termination and reporting to authorities
- Severe violations: Immediate termination

15. Policy Maintenance

15.1 Review Schedule

- Annual comprehensive review
- Ad hoc reviews for regulatory changes
- Post-incident reviews
- Technology change reviews

15.2 Update Process

1. Draft revisions

2. Stakeholder review
3. Legal and compliance review
4. Management approval
5. Staff notification and training
6. Policy publication

16. Related Policies and Procedures

- Information Security Policy
- Acceptable Use Policy
- Privacy Policy
- Breach Notification Procedure
- Incident Response Plan
- Business Continuity Plan

17. References

- HIPAA Privacy Rule (45 CFR Part 160 and Part 164, Subparts A and E)
- HIPAA Security Rule (45 CFR Part 160 and Part 164, Subpart C)
- HITECH Act
- State privacy laws
- Institutional policies

18. Approval

Policy Owner: Privacy Officer
Effective Date: [Date]
Review Date: [Date]
Version: 1.0

Privacy Officer: _____ Date: _____

Security Officer: _____ Date: _____

Chief Information Officer: _____ Date: _____

Legal Counsel: _____ Date: _____

This is a template for educational purposes. Organizations should customize this policy with assistance from legal counsel and compliance professionals.