# QAPIShield™ HIPAA & Data Security Policy

**Effective Date:** December 2024
**Version:** 1.0
**Document Type:** Official Policy Documentation

---

## Purpose

This policy establishes the data security standards and HIPAA compliance framework for QAPIShield™, ensuring the protection of all information processed within the system while supporting quality improvement initiatives in skilled nursing facilities.

---

## Scope

This policy applies to all data processed, stored, or transmitted through QAPIShield™, including clinical risk assessments, care plans, and QAPI analytics.

---

## Policy Statement

### 1. Data De-identification

QAPIShield™ operates exclusively with de-identified data in accordance with HIPAA Safe Harbor guidelines.

**De-identification Standards:**

| Data Element | Status | Implementation |
|---|---|---|
| Resident Names | Not Collected | Reference IDs used instead |
| Social Security Numbers | Not Collected | Never requested or stored |
| Dates of Birth | Not Collected | Age ranges used instead |
| Contact Information | Not Collected | Facility manages separately |
| Medical Record Numbers | Encrypted | Used as Reference ID only |
| Geographic Data | Limited | Facility-level only |

## 2. Encryption Standards

All data within QAPIShield™ is protected by industry-standard encryption.

**Data in Transit:**

- TLS 1.3 encryption for all API communications
- HTTPS required for all web connections
- Certificate pinning for mobile applications

**Data at Rest:**

- AES-256 encryption for database storage
- Encrypted backups with separate key management
- Hardware security modules (HSM) for key storage

## 3. Access Control Framework

QAPIShield™ implements role-based access control (RBAC) to ensure users only access data appropriate to their responsibilities.

**Role Definitions:**

| Role | Access Level | Capabilities |
|---|---|---|
| Nurse | Unit-level | View/create assessments for assigned residents |
| Charge Nurse | Unit-level | All nurse capabilities plus care plan approval |
| DON | Facility-wide | Full facility access, analytics, reporting |
| Administrator | Facility-wide | User management, configuration, all data |
| Corporate | Multi-facility | Aggregate analytics, compliance reporting |

## 4. Authentication Requirements

All users must authenticate before accessing QAPIShield™.

**Authentication Standards:**

- Minimum 12-character passwords with complexity requirements
- Multi-factor authentication (MFA) required for administrative access
- Session timeout after 15 minutes of inactivity
- Account lockout after 5 failed login attempts

## 5. Audit Logging

QAPIShield™ maintains comprehensive audit logs for compliance and security monitoring.

**Logged Events:**

- User login/logout events
- Data access and modifications
- Administrative actions
- Failed authentication attempts
- System configuration changes

**Log Retention:**

- Audit logs retained for minimum 6 years

- Logs stored in tamper-evident format
- Regular log review and anomaly detection

---

# HIPAA Compliance Framework

## Administrative Safeguards

QAPIShield™ implements the following administrative safeguards:

1. **Security Management Process** - Regular risk assessments and security reviews
2. **Workforce Security** - Background checks and security training for all personnel
3. **Information Access Management** - Role-based access with minimum necessary principle
4. **Security Awareness Training** - Annual training for all staff with system access
5. **Security Incident Procedures** - Documented response plan for security events

## Physical Safeguards

1. **Facility Access Controls** - Data centers with $^{24}/_{7}$ security monitoring
2. **Workstation Security** - Policies for secure workstation use
3. **Device and Media Controls** - Encrypted devices and secure disposal procedures

## Technical Safeguards

1. **Access Control** - Unique user identification and automatic logoff
2. **Audit Controls** - Comprehensive logging of all system activity
3. **Integrity Controls** - Data validation and error checking
4. **Transmission Security** - Encryption for all data in transit

---

## Business Associate Agreement

QAPIShield™ operates under a Business Associate Agreement (BAA) with each covered entity.

**BAA Requirements:**

- Signed BAA required before system access
- Annual BAA review and renewal
- Immediate notification of any security incidents
- Cooperation with facility audits and assessments

---

## Incident Response

In the event of a security incident:

1. **Detection** - Automated monitoring and manual reporting channels
2. **Containment** - Immediate isolation of affected systems
3. **Investigation** - Root cause analysis and impact assessment
4. **Notification** - Timely notification to affected facilities per BAA terms
5. **Remediation** - Implementation of corrective measures
6. **Documentation** - Complete incident documentation for compliance

---

## Staff Responsibilities

All staff with QAPIShield™ access must:

1. Maintain confidentiality of login credentials
2. Report suspected security incidents immediately
3. Complete required security training
4. Follow facility policies for workstation security
5. Log out when leaving workstations unattended

## Policy Violations

Violations of this policy may result in:

- Immediate suspension of system access
- Disciplinary action per facility policy
- Reporting to appropriate regulatory authorities
- Legal action for willful violations

---

## Questions and Support

For questions about this policy or to report security concerns:

- Contact your facility’ s Privacy Officer
- Submit a support request through QAPIShield™
- Report urgent security concerns to security@qapishield.com

---

## Document Control

| Version | Date | Author | Changes |
|---|---|---|---|
| 1.0 | December 2024 | QAPIShield Security Team | Initial release |

---

**QAPIShield™** — AI-Powered Risk Prevention & Survey Protection for Skilled Nursing Facilities

*This document is confidential and intended for authorized facility use only.*