

QAPIShield™ Staff Responsibility Policy

Effective Date: December 2024

Version: 1.0

Document Type: Official Policy Documentation

Purpose

This policy establishes the responsibilities and expectations for all staff members who access and use QAPIShield™ in the performance of their duties, ensuring accurate documentation, proper system usage, and compliance with facility policies.

Scope

This policy applies to all nursing staff, clinical personnel, supervisors, and administrators who have been granted access to QAPIShield™.

Policy Statement

1. Reference ID Usage

Staff members are responsible for using correct Resident Reference IDs when entering data into QAPIShield™.

Reference ID Requirements:

| Requirement | Description | Example |
|--------------|---|--------------------------------------|
| Accuracy | Verify Reference ID matches resident's EHR record | Cross-check with census or EHR |
| Consistency | Use the same Reference ID format facility-wide | MRN-12345, not "12345" or "MRN12345" |
| Verification | Confirm ID before submitting assessments | Double-check before clicking submit |
| Reporting | Report any Reference ID discrepancies immediately | Notify charge nurse or supervisor |

Common Reference ID Errors to Avoid:

- Transposing numbers (e.g., 12345 vs 12354)
- Using outdated or discharged resident IDs
- Creating duplicate entries for the same resident
- Using informal identifiers or nicknames

2. Documentation Expectations

All staff must maintain accurate and timely documentation in QAPIShield™.

Documentation Standards:

| Standard | Requirement | Timeframe |
|--------------|---|-------------------------|
| Completeness | All required fields must be completed | At time of assessment |
| Accuracy | Observations must reflect actual clinical findings | Real-time documentation |
| Objectivity | Use clinical terminology, avoid subjective language | Always |
| Timeliness | Submit assessments within required timeframes | Per assessment type |

Documentation Best Practices:

- Document observations as they occur when possible

- Use specific, measurable descriptions
- Avoid copying and pasting from previous assessments
- Review entries before submission for accuracy
- Correct errors promptly using proper amendment procedures

3. System Access and Security

Staff must maintain the security of their QAPIShield™ access credentials.

Security Responsibilities:

| Responsibility | Action Required |
|----------------------|---|
| Password Protection | Never share passwords or login credentials |
| Workstation Security | Log out when leaving workstation unattended |
| Session Management | Do not leave active sessions open |
| Incident Reporting | Report suspected unauthorized access immediately |
| Device Security | Do not access QAPIShield™ on unauthorized devices |

4. Risk Alert Response

Staff must respond promptly to risk alerts generated by QAPIShield™.

Alert Response Protocol:

1. **Review Alert** - Read the complete alert information
2. **Assess Resident** - Perform bedside assessment as indicated
3. **Implement Interventions** - Apply appropriate prevention measures
4. **Document Response** - Record actions taken in QAPIShield™
5. **Notify Supervisor** - Escalate high-risk situations as required

Response Timeframes:

| Alert Level | Response Time | Escalation |
|---------------|----------------|-----------------------------------|
| High Risk | Within 1 hour | Immediate supervisor notification |
| Moderate Risk | Within 4 hours | Document and monitor |
| Low Risk | Within shift | Standard care planning |

5. Training and Competency

Staff must complete required training and maintain competency in QAPIShield™ usage.

Training Requirements:

| Training Type | Frequency | Requirement |
|----------------------|---------------|--|
| Initial Training | Before access | Complete all modules, pass competency test |
| Annual Refresher | Yearly | Review updates, complete assessment |
| New Feature Training | As released | Complete within 30 days of release |
| Privacy Training | Annually | HIPAA and privacy policy review |

6. Shift Handoff Procedures

Staff must include QAPIShield™ information in shift handoff communications.

Handoff Requirements:

- Report any new high-risk alerts
 - Communicate pending assessments due
 - Share intervention effectiveness observations
 - Note any system issues or access problems
 - Transfer responsibility for alert monitoring
-

Role-Specific Responsibilities

Nursing Staff (CNAs, LPNs, RNs)

- Complete assigned risk assessments accurately
- Respond to risk alerts within required timeframes
- Document interventions and resident responses
- Report changes in resident condition promptly
- Participate in care plan development

Charge Nurses

- Oversee assessment completion for assigned unit
- Review and approve care plans
- Monitor alert response compliance
- Provide guidance to nursing staff
- Escalate concerns to DON as needed

Directors of Nursing

- Ensure facility-wide compliance with documentation standards
- Review QAPI analytics and trends
- Lead quality improvement initiatives
- Manage user access and permissions
- Coordinate survey readiness activities

Administrators

- Ensure adequate staffing for documentation requirements
- Support training and competency programs
- Review facility performance metrics
- Allocate resources for quality improvement

- Maintain BAA and compliance documentation

Performance Expectations

Staff performance related to QAPIShield™ usage will be evaluated based on:

Key Metrics:

| Metric | Target | Measurement |
|----------------------------|---------------------------|--|
| Assessment Completion Rate | 100% | Completed vs. assigned assessments |
| Documentation Timeliness | 100% on time | Submissions within required timeframes |
| Alert Response Time | Within required timeframe | Time from alert to acknowledgment |
| Documentation Accuracy | % error rate | Audit findings and corrections |

Policy Violations

Violations of this policy may result in progressive disciplinary action:

First Violation:

- Verbal counseling and additional training

Second Violation:

- Written warning and supervised documentation review

Third Violation:

- Performance improvement plan

Serious Violations:

- Immediate suspension of system access

- Disciplinary action up to and including termination
- Reporting to appropriate regulatory authorities if required

Examples of Serious Violations:

- Intentional falsification of documentation
 - Sharing login credentials
 - Accessing records without legitimate purpose
 - Failure to report security incidents
-

Support and Resources

Staff can access support through:

- **Immediate Supervisor** - First point of contact for questions
 - **Charge Nurse** - Clinical documentation guidance
 - **DON** - Policy interpretation and escalation
 - **IT Help Desk** - Technical issues and access problems
 - **QAPIShield™ Support** - System-specific assistance
-

Acknowledgment

All staff must acknowledge receipt and understanding of this policy before receiving QAPIShield™ access. Acknowledgment can be completed through the Policy Acknowledgment Form on the Policies & Procedures page.

Document Control

| Version | Date | Author | Changes |
|---------|---------------|--------------------|-----------------|
| 1.0 | December 2024 | QAPIShield HR 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.