Securing MS Intune with PQC+

(SmartCompliance™, SMARTMCP™, Q-InfoSecur™, Q-SecurKey™)

Guide to Securing Medical Devices and Patient Data for Healthcare IT Leaders, CTOs, CISOs, and Compliance Officers

Executive Summary

The document explains that while traditional Mobile Device Management (MDM) tools like Microsoft Intune are essential for securing medical devices, they only protect the device, not the sensitive patient data itself, creating a critical gap for FDA compliance and quantum threats.

- The **Transformativ IP solution, PQC+ with Q-InfoSecur™ and Q-SecurKey™**, provides a second, independent layer of **Object-Level Encryption** where each data record carries an **Embedded Access Control List (ACL)**, making the data "posture-aware" by denying access if Intune flags the device as non-compliant.
- This layered **Defense-in-Depth** architecture, combined with modern cryptographic protocols like TLS 1.3 and a mandatory **Coordinated Vulnerability Disclosure (CVD)** policy, delivers the complete, documented, and post-quantum-ready security stack required for FDA Premarket Cybersecurity Submissions and continuous Post-Market security management.

Mobile Device Management (MDM) Is Not Secure for Medical Data

If your organization manages medical devices or smartphones that store patient data, you already know that Microsoft Intune and Mobile Device Management (MDM) are essential tools. They let you control which devices can connect to your network, push software updates, and enforce basic security policies like requiring a passcode.

But here is the critical gap: **Intune secures the device, not the data itself.** Think of it this way—Intune is the lock on the front door of a building. It controls who gets in. But once someone is inside, the individual file cabinets (your patient records, FHIR resources, and medical images) are wide open. If an attacker gets past that front door—through a stolen credential, a jailbroken phone, or a network interception—your sensitive data is exposed.

This is the problem that **PQC+ with SMARTCompliance, SMARTMCP, Q-InfoSecur™ and Q-SecurKey™** were built to solve. These technologies, work alongside Intune to add a second, independent layer of protection directly around the data. The result is a security architecture that satisfies FDA cybersecurity requirements and is designed to withstand even future quantum-computing threats.

The Solution: Three Layers, The Gatekeeper, the Vault, and the Enforcer

The easiest way to understand the combined system is with a simple analogy. Imagine a hospital with three layers of security:

Layer 1 – The Gatekeeper (Microsoft Intune): Intune checks every device at the door. Is the phone encrypted? Is the operating system up to date? Has it been jailbroken or rooted? If the device fails any of these checks, it gets flagged as "Non-Compliant" and is blocked from accessing company resources.

Layer 2 - The Vault (PQC+ with SMARTCompliance) This layer uses a hybrid design with role base access control and attribute base access control for healthcare data. These granular access control list are built by PQC+ and are embedded into the vault automatically. Utilization of **PQC+ SMARTMPC** server helps in managing patent consent for data sharing on regulatory requirements for managing AI solutions. By documenting this end-to-end stack **PQC+ SMARTCompliance** can demonstrate the "Reasonable Assurance of Safety and Effectiveness" required for FDA certification.. PQC+ moves data into the Enforcer for protection of data in motion or at rest.

Layer 3 – The Enforcer (PQC+ with Q-InfoSecur™ & Q-SecurKey™): Even after a device passes Intune's checks, the actual medical data remains locked inside our "vault." Each piece of data—a patient record, a lab result, a FHIR resource—is individually encrypted with its own unique **Q-SecurKey™**. The data literally "knows" who is allowed to see it, because the access rules are embedded directly into the data payload itself, not stored on a separate server that could be compromised.

This is what **Transformativ IP** calls an **Embedded Access Control List (ACL)**. It means your data carries its own security with it, everywhere it goes—on the device, across the network, and into cloud storage.

What Changes When You Add Q-InfoSecur™ and Q-SecurKey™?

The table below shows the practical difference between using Intune alone and using Intune with **PQC+ with Q-InfoSecur™ and Q-SecurKey™** layered on top.

Security Capability	Intune Alone	Intune + PQC+ (Q-InfoSecur™ / Q-SecurKey™)
Access Control Level	Device-level or app-level. Once you're in, data is accessible.	Object-level. Each data record is individually locked with its own key.
Lost or Stolen Device	Remote wipe erases the device, but data may already have been copied.	Data remains encrypted and unreadable even if copied, because the attacker lacks the Q-SecurKey™ token.
Network Interception	TLS protects data in transit, but standard TLS 1.2 has known weaknesses.	TLS 1.3 with Perfect Forward Secrecy. Even if a long-term key is compromised, past sessions stay safe.

Compromised Device	If jailbroken, apps can access data on the device.	Q-SecurKey™ checks device compliance status via Intune before decrypting. Non-compliant device = no data access.
Post-Quantum Readiness	Standard encryption will be breakable by quantum computers in the near future.	Designed with post-quantum cryptographic algorithms to remain secure against quantum attacks.
FDA Compliance	Provides device management documentation only.	Provides the full Defense-in-Depth stack required for FDA Premarket Cybersecurity Submissions.

Why TLS 1.3 Matters (and Why TLS 1.2 Is No Longer Good Enough)

When a medical device or smartphone sends data to a server, that data travels through a secure tunnel called TLS (Transport Layer Security). Most organizations still use TLS 1.2, but the FDA now expects TLS 1.3 for new medical device submissions. Here is why.

Perfect Forward Secrecy: TLS 1.3 eliminates the older, weaker encryption methods that TLS 1.2 still supports. If an attacker somehow obtains your long-term encryption key in the future, they still cannot decrypt past sessions. Each connection generates a unique, temporary key that is discarded immediately after use.

Faster Connections: TLS 1.3 reduces the number of round-trips needed to establish a connection (the “handshake”). This is especially important for battery-powered medical devices and smartphones that need to transmit life-critical data quickly without draining power.

Regulatory Alignment: The FDA’s cybersecurity guidance increasingly expects modern cryptographic protocols. Using TLS 1.3 in your Intune-managed environment demonstrates that your organization is keeping pace with current security standards.

Meeting FDA Requirements: What You Need to Submit

For medical device manufacturers seeking FDA Authority to Operate (ATO), the combination of Intune, Q-InfoSecur™, Q-SecurKey™, and TLS 1.3 addresses the major components of a Premarket Cybersecurity Submission. Here is how each requirement maps to the technology.

1. Security Architecture Views

The FDA requires clear visual diagrams showing how data moves through your system and where each security control applies. Your documentation should include a Global System View (showing the medical device, the Intune management plane, and your cloud backend), a Data Flow Diagram (labeling where TLS 1.3 encrypts data in transit), and an Access Control Layer Diagram (showing how the Embedded ACL from Q-InfoSecur™ operates independently of the network as a second line of defense).

2. Cybersecurity Traceability Matrix

This is one of the most important documents in your submission. It directly links each identified threat to the specific technology that mitigates it. Below is an example entry.

Req. ID	Threat	Mitigation	Verification	Traceability
SEC-001	Unauthorized access to PHI/PII via lost device or intercepted traffic.	Q-SecurKey™ Embedded ACL encrypts data with a unique key. Access granted only when user identity and Intune device posture both pass.	Penetration test confirms data stays encrypted when Q-SecurKey™ token is absent.	Design Spec §4.2, Test Report TR-102, Patent Ref.

3. Software Bill of Materials (SBOM)

The FDA requires a machine-readable list of every software component in your device. This must include all Microsoft Intune SDKs and management agents, the Transformativ IP proprietary components for Q-SecurKey™ and Q-InfoSecur™, and all cryptographic libraries providing the TLS 1.3 stack, confirmed free from known vulnerabilities.

4. Vulnerability Management Plan

Under Section 524B of the FD&C Act, your submission must include a plan for monitoring and patching security components after the product goes to market. This includes using Intune to push updates if a vulnerability is found in the TLS stack or the Embedded ACL technology.

Proving It Works: The Fail-Safe Test

The FDA does not just want to know that your security works when everything goes right. They want to see that it **fails safely** when something goes wrong. This requires a negative test case—demonstrating that data access is denied when security conditions are not met.

Test Scenario: What Happens When a Device Becomes Non-Compliant?

1. **Setup:** A medical device is enrolled in Intune, marked “Compliant,” and the user has a valid Q-SecurKey™ token to access a specific FHIR resource.
2. **Trigger:** The device encryption is disabled or the device is jailbroken, causing Intune to flag it as “Non-Compliant.”
3. **Policy Sync:** Intune syncs the updated status to Azure AD / Microsoft Entra ID.
4. **Access Attempt:** The user tries to open or decrypt the FHIR resource.
5. **Expected Result:** Q-SecurKey™ rejects the decryption request. The application returns a “Security Compliance Failure” error. No medical data is exposed.

This test proves a critical point: the Embedded ACL is **posture-aware**. It does not just check who the user is—it checks whether the device itself is currently trustworthy. If the device is compromised, Q-SecurKey™ acts as a kill-switch, locking the data even if the TLS 1.3 tunnel is still active.

After Launch: Real-Time Monitoring and Post-Market Security

FDA compliance does not end at product launch. Under the FDA's Post-Market Cybersecurity Management requirements, you must demonstrate continuous monitoring and rapid response throughout the device's entire lifecycle. The Intune and Q-SecurKey™ architecture makes this straightforward.

How the Automated Response Chain Works

1. **Detection:** Intune detects a compliance failure—for example, a user removes their device passcode or the OS falls behind on patches.
2. **Notification:** Intune immediately signals the Azure Health Data Services backend via Microsoft Entra ID.
3. **Enforcement:** The Q-SecurKey™ service denies the next request for a FHIR resource key, even if the TLS 1.3 tunnel is still active. The data stays locked.

Post-Market Monitoring Plan Components

Plan Section	What It Covers
Vulnerability Monitoring	Ongoing scanning of the TLS 1.3 stack, Intune agents, and Q-SecurKey™ encryption libraries for new threats.
Real-Time Alerting	Automated thresholds—e.g., a single root detection triggers a local data lock; 5% fleet non-compliance triggers a system-wide security review.
Coordinated Vulnerability Disclosure	A public, structured process for security researchers to safely report flaws in your Q-SecurKey™ or TLS implementation.
Remediation & Patching	Use Intune Software Updates to push security patches within the "reasonable time" required by Section 524B of the FD&C Act.
Documentation & Reporting	Minor security updates under the CVD program do not require a new FDA filing, provided no patient harm occurs.

Coordinated Vulnerability Disclosure: A Mandatory FDA Requirement

The FDA's 2026 guidance makes a Coordinated Vulnerability Disclosure (CVD) policy mandatory for market approval. This is not optional—it is a condition of certification. The policy provides a safe, structured channel for external security researchers to report flaws in your system before they can be exploited in a clinical setting.

A compliant CVD policy should cover the scope of your systems (listing specific medical devices managed by Intune, cloud infrastructure including FHIR API endpoints and Q-SecurKey™ authentication services), a clear reporting process (with a dedicated email or portal for submissions), response-time commitments (acknowledgement within 3 business days, initial triage within 10, and patches deployed via Intune within 30–60 days depending on severity), and a Safe Harbor statement assuring researchers that good-faith reporting will not result in legal action. For vulnerabilities affecting the broader healthcare ecosystem, the policy should include provisions for coordinating with CISA and the FDA to ensure synchronized public alerts.

The Bottom Line

Microsoft Intune is an excellent tool for managing devices. But for organizations handling medical data, device management alone is not enough. The combination of Q-InfoSecur™ and Q-SecurKey™ transforms a standard MDM deployment into a complete, FDA-ready security platform by adding three critical capabilities.

1. **Object-Level Encryption:** Every piece of medical data is individually encrypted and carries its own access rules, so it stays protected no matter where it travels.
2. **Posture-Aware Access Control:** Data decryption is tied directly to the device's real-time compliance status in Intune. A compromised device means zero data access—automatically.
3. **Post-Quantum Readiness:** The cryptographic foundation is designed to withstand attacks from future quantum computers, protecting your investment and your patients for the long term.

The result is a Defense-in-Depth architecture where Intune guards the door and **Q-SecurKey™** guards the data—giving you the documented, testable, end-to-end security stack that the FDA requires for certification.

For information on transforming standard MDM into a future-proof security platform.
contact: Info@TransformativIP.com

Additional Educational Resources available at: insert link here

- Videos
- Slide decks (some narrated)
- Tech Audios
- White papers
- FAQs