Transformativ IP

PQC+, Defense for MS Intune MDM

Triple-Layer Protection Against Stryker Type Hacks of Healthcare Data

Securing Patient Data & Medical Devices Data with
Post-Quantum Encryption and FDA-Ready Compliance

Overview

The Vulnerability

Microsoft Intune has a critical vulnerability. It manages only device connection, updates, and policies, but not the data. Intune is a front-door lock; if an attacker bypasses it via stolen credentials as was the case with Stryker, or a jailbroken phone, or network interception, **your sensitive data (patient records, lab results, images) is fully exposed.**

The Solution

A **three-layered security solution, PQC+ with Q-InfoSecur™and Q-SecurKey™,** designed to integrate with Microsoft Intune to make a Stryker-like problem impossible. This solution protects patient data and medical devices using post-quantum encryption and FDA-certified software, ensuring that the security failures experienced by companies like Stryker are prevented.

Layer 1: The Gatekeeper

While Intune acts as the Gatekeeper by securing the device itself, the critical gap is that MS Intune does not secure the data;

Layer 2: The Vault

Applies the appropriate state-level regulations and generates Access Control Lists (ACLs);

Layer 3: Our Enforcer

Provides object-level encryption, where each data record is individually locked with a Q-SecurKey™ and the ACL is embedded directly within the data.

This combined platform provides **Object-Level Encryption, Posture-Aware Access Control** (where data locks itself if the device is non-compliant with Intune), and **Post-Quantum Readiness**, addressing key FDA Premarket Cybersecurity Submission requirements:

1. **Security Architecture Views**
2. **Cybersecurity Traceability Matrix**
3. **SBO**
4. **Vulnerability Management Plan.**

PQC+ is the Security Solution: Three Layers Working Together

Layer 1 — The Gatekeeper (Microsoft Intune)

Intune checks every device at the door: Is it encrypted? Is the OS up to date? Has the been jailbroken or rooted? Devices that fail are blocked from company resources.

Layer 2- The Vault (PQC+ with SmartCompliance & SMARTMCP)

Our Vault automatically determines the geographic location of the medical data owner to apply the correct state-level regulations, thereby ensuring regulatory compliance and privacy. This process generates Access Control Lists (ACLs) that a medical data owner can share to manage access to their medical data. This enables the medical data owner to assign/revoke privileges to (organization which can be a hospital, company, govt, etc.). Our vault determines the ACLs and assigns start and stop dates for the rules for medical data access. The Vault manages these ACLs, which are then applied to the data before downstream processing by our Enforcer.

Layer 3 — Our Enforcer (PQC+ with Q-InfoSecur™ & Q-SecurKey™)

After passing Intune's stringent checks, each individual record is secured with its own distinct Q-SecurKey™ encryption. Crucially, the access control list (ACL) is embedded directly within the data itself, meaning your information carries its security everywhere: on the device, throughout the network, and when stored in the cloud. Acting on the patient's consent as defined in the ACLs, the Enforcer component automatically de-identifies (masks) the data to ensure compliance with all federal and state regulations.

What Changes When You Add PQC+ with Q-InfoSecur™ & Q-SecurKey™?

Capability	Intune Alone	Intune + Q-InfoSecur™ / Q-SecurKey™
Access Control	Device-level. Once you're in, data is accessible.	Object-level. Each record is individually locked with its own key.
Lost / Stolen Device	Remote wipe erases the device, but data may already have been copied.	Data stays encrypted and unreadable—even if copied—without the Q-SecurKey™ token.
Network Interception	Standard TLS 1.2 has known weaknesses attackers can exploit.	TLS 1.3 with Perfect Forward Secrecy. Past sessions stay safe even if a key leaks.
Compromised Device	Jailbroken apps can access data on the device.	Q-SecurKey™ checks Intune compliance in real time. Non-compliant = zero access.
Post-Quantum Readiness	Standard encryption will be breakable by quantum computers.	Built with post-quantum cryptographic algorithms—future-proof by design.
FDA Compliance	Device management documentation only.	Full Defense-in-Depth stack for FDA Premarket Cybersecurity Submissions.

Why TLS 1.3 Matters

Most organizations still use TLS 1.2, but the FDA now expects TLS 1.3 for new submissions. TLS 1.3 offers several upgrades including delivering **Perfect Forward Secrecy** (each session uses a temporary key discarded immediately—a leaked long-term key cannot decrypt past data), **faster connections** for battery-powered medical devices, and full **regulatory alignment** with current FDA cybersecurity guidance.

FDA Compliance: What the Combined Platform Covers

For FDA Authority to Operate, Intune + PQC+ with Q-InfoSecur™ / Q-SecurKey™ addresses four pillars of a Premarket Cybersecurity Submission:

FDA Requirement	How the Platform Addresses It
Security Architecture Views	Clear diagrams of data flow, TLS 1.3 encryption points, and the Embedded ACL operating as a second line of defense independent of the network.
Cybersecurity Traceability Matrix	Each identified threat is directly linked to the specific technology that mitigates it—verified through penetration testing and documented for audit.
Software Bill of Materials (SBOM)	Machine-readable inventory of all Intune SDKs, Q-SecurKey™ components, and TLS 1.3 cryptographic libraries—confirmed free from known vulnerabilities.
Vulnerability Management Plan	Ongoing monitoring and patching via Intune updates, meeting Section 524B of the FD&C Act for post-market security.

The Fail-Safe Test: Proving Security Under Failure

The FDA requires proof the system fails safely. When a device becomes compromised (encryption disabled or jailbroken), Intune flags it as "Non-Compliant" and **Q-SecurKey™ immediately denies all data access**—even with an active TLS connection. The data locks itself automatically.

After Launch: Continuous Monitoring & Compliance

FDA compliance continues post-launch. The platform automates ongoing security through:

Capability	What It Covers
Vulnerability Monitoring	Continuous scanning of TLS 1.3 stack, Intune agents, and Q-SecurKey™ libraries for emerging threats.
Real-Time Alerting	Automated thresholds: root detection triggers local data lock; 5% fleet non-compliance triggers system-wide review.
Coordinated Disclosure (CVD)	Mandatory FDA 2026 requirement: structured process for researchers to report vulnerabilities safely.
Remediation & Patching	Intune pushes patches within timeframes required by Section 524B of the FD&C Act.

The Bottom Line: Three Capabilities That Change Everything

1. **Object-Level Encryption —** Every piece of medical data is individually encrypted and carries its own access rules—protected no matter where it travels.
2. **Posture-Aware Access Control —** Decryption is tied to real-time device compliance. Compromised device = zero data access, automatically.
3. **Post-Quantum Readiness —** Cryptography designed to withstand quantum computing attacks, protecting your investment and your patients for the long term.

Intune guards the door. Q-SecurKey™ guards the data. Together they give you the documented, testable, end-to-end security stack the FDA requires for certification—and the peace of mind your patients deserve.