PQC+

(Post-Quantum Cryptography Plus)

A Technical Deep Dive for Hospital Leadership

PQC+ is designed to seamlessly integrate with and optimize your existing data infrastructure, not replace it. PQC+ connects, secures, and enhances your hospital's data ecosystem without disrupting current investments in systems like Epic, Oracle, or MEDITECH. We stand firmly against the "rip and replace" approach, prioritizing technological coexistence.

The benefits of PQC+ include:

- A unified connecting layer for internal and external data.
- Automatic enforcement of patient consent across all data flows.
- Enabling AI capabilities with robust governance.
- Creating new revenue opportunities.
- Automated generation of compliance documentation.

Developed and Presented February 2026 by

Transformativ IP

Table of Contents

Benefits and Value for Your Hospital

Before we get into the technical architecture, here's the bottom line: what does PQC+ actually do for your hospital? This section maps platform capabilities directly to the outcomes your leadership team cares about most.

Benefit Area	What PQC+ Delivers	Why It Matters
Data Security	Post-quantum cryptography with access controls embedded in the encryption itself	Even stolen encrypted data can't be decrypted without satisfying access rules
Compliance	Automatic jurisdiction-aware consent enforcement across all 50 states	No more manually tracking which privacy laws apply to which patients
Interoperability	Universal data translation across HL7 v2, C-CDA, FHIR, X12, and DICOM	Your existing systems stay in place—PQC+ bridges the gaps between them
Patient Identity	AI-powered matching to eliminate duplicate records	Clinicians see one complete patient record, not fragments scattered across systems
AI Governance	Controlled gateway for all AI data access with patient-level consent	You're ready for AI regulations before they arrive
Revenue	Medication pricing transparency, RAF scoring, and revenue cycle AI	Concrete, measurable financial returns from day one

Enhanced Patient Data Security and Compliance

The security architecture goes far beyond typical encryption. PQC+'s **SMARTInfoSecur** module uses **Post-Quantum Cryptography (PQC)**—and here's what makes it genuinely different from anything else on the market.

> **What Makes This Different**
> Traditional security systems encrypt data and then layer access controls on top as a separate system. SMARTInfoSecur fuses them together—it embeds access control policies directly into the cryptographic key structure itself. Even if someone obtained encrypted data, they couldn't decrypt it without also satisfying the embedded access rules. The data and its protection are inseparable.

This isn't theoretical technology. It's certified under **NIST FIPS 203, 204, and 205 standards** and holds the **only FDA Authority to Operate (ATO) approval in healthcare** for this type of solution. That certification matters when auditors come knocking.

Automated Compliance: What SMARTCompliance Handles

Compliance Capability	How It Works
Jurisdictional Awareness	Automatically identifies which privacy laws apply based on patient location—HIPAA, CCPA, Utah's privacy laws, and every state regulation in between
Granular Data Tagging	Sensitive categories like reproductive health, substance use disorder (42 CFR Part 2), and behavioral health are tagged and given special handling automatically

Compliance Capability	How It Works
Automatic Audit Trails	Every data share, every view, every access request is logged with timestamps—complete documentation ready for any audit or legal inquiry
AI Compliance Gateway	Uses Model Context Protocol (MCP) to control how AI applications access patient data—enforcing consent rules and applying data masking before data reaches any AI model

Maximized System Uptime and Operational Continuity

The interoperability engine—**SMARTInteroperability**—is where operational continuity comes together. Your hospital likely has data arriving in multiple formats from dozens of sources. Here's how PQC+ handles that complexity:

Data Format	Common Source	What PQC+ Does
HL7 v2	Older EHR systems, lab systems	Ingests and converts to FHIR; converts back for outbound communication
C-CDA Documents	Clinical summaries, referrals	Parses documents and extracts discrete data elements
X12 Transactions	Insurance payers	Handles eligibility, claims, and remittance data
DICOM Images	Radiology, imaging centers	Integrates imaging data into unified patient view
FHIR R4	Modern EHR APIs	Native format—bidirectional exchange with no translation needed

This bidirectional capability means **you're not asking every connected system to change**. PQC+ sits in the middle as a universal translator, handling the complexity so your existing systems don't have to.

The **SMARTEntityResolution** module solves another persistent headache: duplicate patient records. Using AI-powered matching, it builds and maintains a unified Master Patient Index, Master Practitioner Index, and Master Organization Index. When data arrives from labs, imaging centers, or external partners, the system identifies which patient it belongs to—eliminating clinical risk from fragmented records and the operational burden of manual reconciliation.

For connectivity, **SMARTConnectivity** provides direct integration with all major QHINs under TEFCA rules—CommonWell, eHealth Exchange, Epic, Oracle Health, and others. The platform claims connectivity to **over 99% of individual providers in the US market**.

> **No Rip-and-Replace Required**
>
> Your existing EHR stays in place. Your lab systems keep running. PQC+ sits at the center as a secure, compliant fabric that connects everything together.

Reduced Total Cost of Ownership

The modular architecture consolidates what would otherwise require multiple point solutions. Consider what you might currently be paying for separately:

Separate Solution You May Be Paying For	PQC+ Module That Replaces It
Consent management software	SMARTCompliance
Data masking and anonymization tools	AI Compliance Gateway
FHIR server and interoperability engine	SMARTInteroperability
Identity resolution / MPI software	SMARTEntityResolution
Audit logging and compliance documentation	SMARTCompliance audit trails
AI governance tools	AI Compliance Gateway + MCP controls

PQC+ bundles these into **13 core cloud-based modules** that share a common security layer and data foundation. You're not managing separate vendor relationships, separate licensing agreements, and separate integration projects. The modular approach also means you can deploy what you need now and add capabilities later.

Why PQC+ Is Unique and Compelling

Proactive, Trust-by-Design Security

Most security solutions are reactive—they detect threats and respond. PQC+ takes a fundamentally different approach by making patient consent the foundation of every data exchange, not an afterthought.

The **Global Consent Management System** gives patients granular control over exactly who sees what parts of their record. But the critical part is this: those preferences are **enforced automatically at the data layer**. It's not just a policy document that humans are supposed to follow—the system physically prevents data from flowing to unauthorized parties.

AI-Specific Consent Controls

As AI tools proliferate in healthcare, PQC+ provides separate consent controls for each category:

AI Consent Category	What It Covers	Why Patients Care
Clinical Decision Support	AI tools that help clinicians diagnose or treat	Directly benefits their care—most patients accept this
Automated Decision-Making	AI that makes decisions without human review	Higher stakes—patients may want to opt out
LLM Training Data	Using patient data to train language models	Data leaves the institution; patients often object
Third-Party AI Applications	External vendors' AI tools	Patients may not trust unknown third parties
Research AI	AI used in clinical research	Different regulatory framework (IRB oversight)

> **The Quantum Computing Threat Is Real**
> Quantum computing will eventually break current encryption standards—that's not speculation, it's a mathematical certainty. Organizations storing encrypted health data today need to think about whether that data could be harvested now and decrypted later when quantum computing matures. SMARTInfoSecur provides protection against threats that don't fully exist yet—exactly the kind of forward-thinking security healthcare data requires.

Immediate and Measurable ROI

The financial case has concrete numbers worth highlighting:

Revenue / Savings Opportunity	How It Works	Impact
Medication Pricing Transparency	Real-time pricing at point of care across 22,000+ pharmacies via strategic partnership	PBM markups drop from 8–15% to just 2%; hospital participates in transaction-based revenue
Value-Based Care Optimization	SMARTVBR calculates Risk Adjustment Factor (RAF) scores accurately	Captures appropriate reimbursement under value-based contracts; closes undercoding gaps
Revenue Cycle Management	SMARTRCM uses AI to analyze eligibility across state, federal, and private programs	"What-if" projections for different payment models; optimized claims processing
Liability Protection	Time-based audit trails document every data access with verifiable records	Average HIPAA breach costs $4M+; complete audit documentation reduces exposure

Built Specifically for Healthcare

This platform wasn't adapted from generic enterprise software. The ecosystem includes over **26 integrated SMART applications** designed specifically for healthcare workflows:

Category	Application	What It Does
Clinical Care	SMARTDiagnosis	AI-powered diagnostic support with evidence-based ranking
Clinical Care	SMARTTriageCenter	24/7 virtual call center using Schmitt Thompson nursing protocols
Clinical Care	SMARTAmbienBOT	Real-time clinical conversation transcription with automatic coding
Clinical Care	SMARTCDM	Chronic disease management including RPM, CCM, and glucose monitoring
Research	SMARTClinicalTrialMatching	AI matching of patients to clinical trial inclusion/exclusion criteria
Research	SMARTClinicalTrialMonitoring	Real-time recommendations to minimize patient disqualifications
Operations	SMARTWorkflow	BPMN 2.0 for designing complex business processes
Operations	SMARTForms / SMARTQuestionnaire	Data capture with automatic FHIR resource creation

Every one of these applications shares the **same consent management layer, security infrastructure, and patient identity resolution**. They're not bolted-on afterthoughts—they're part of a coherent ecosystem.

Deep Dive: QHIN Integrations

The Big Picture

TEFCA (Trusted Exchange Framework and Common Agreement) is the federal government's push to create a nationwide health information exchange network. **QHINs—Qualified Health Information Networks—are the designated on-ramps to that network.** If your hospital wants to exchange data nationally under standardized rules, you need to connect through a QHIN.

PQC+'s **SMARTConnectivity** module handles this integration. Here's the full picture:

Certified QHIN Connections

QHIN	Primary Strength
CommonWell Health Alliance	Broad ambulatory and hospital network
eClinicalWorks	Large ambulatory EHR user base
eHealth Exchange	Federal agencies, large health systems
Epic	Dominant hospital EHR market share
Health Gorilla	Labs, diagnostics, clinical data
Kno2	Direct messaging, smaller practices
Konza Health	Regional focus, emerging network
MedAllies	HIE services, care coordination
Netsmart	Behavioral health, post-acute care
Oracle Health (formerly Cerner)	Large health systems, federal contracts
Surescripts	Pharmacy network, medication history

> **What This Means in Practice**
>
> Through these combined networks, PQC+ claims connectivity to over 99% of individual providers in the US market. When a patient shows up at your ED and you need records from their primary care physician three states away, this connectivity makes that possible.

Individual Access Services (IAS)

One specific TEFCA use case PQC+ supports is Individual Access Services—the ability for patients themselves (not just providers) to request and receive their complete medical records from across the network. The 21st Century Cures Act gives patients the right to access their data, and IAS is the TEFCA mechanism to fulfill that right at scale.

Proxy Authorization: A Critical Differentiator

Standard QHIN connections don't handle proxy relationships well. PQC+'s SMARTCompliance module specifically manages the legal relationships involved:

Proxy Scenario	What PQC+ Manages
Parent accessing records for a minor child	Verifies parental rights, applies age-appropriate access rules by state
Adult child with power of attorney for elderly parent	Validates POA documentation, enforces appropriate data boundaries
Legal guardian for someone with cognitive impairment	Confirms guardianship papers, ties to consent framework
Attorney representing a client	Verifies attorney-client agreements, manages medical records requests compliantly

Hospitals currently spend countless hours on the phone verifying proxy relationships and manually processing records requests. Automating this verification while maintaining compliance reduces that administrative burden substantially.

AI Compliance Controls: Governing Data Flows to AI Systems

Why This Matters Right Now

AI is already in your hospital—clinical decision support, ambient documentation, predictive analytics, imaging interpretation. More is coming. But here's the problem: most consent frameworks were designed before AI existed. They ask patients to consent to "treatment, payment, and healthcare operations" without ever contemplating that their data might train a language model or feed an automated diagnostic algorithm.

Regulators are catching up fast. The EU's AI Act has specific provisions for healthcare AI. The FDA is increasing scrutiny on clinical AI tools. State attorneys general are asking how patient data flows into AI systems. **Hospitals that can't answer those questions clearly are exposed.**

How the AI Compliance Gateway Works

The gateway uses Model Context Protocol (MCP)—a standardized way for AI models to request and receive data from external systems. Every AI data request must pass through this checkpoint. It's not optional—it's architecturally enforced.

Step	What Happens	If Authorized	If Not Authorized
1	AI application sends data request via MCP	—	—
2	Gateway checks patient consent settings	—	—
3	Consent evaluation completed	Data returned (with masking if configured)	Request denied + attempt logged
4	Full audit trail recorded	Records what data was shared and to whom	Records the denied request and reason

Automatic Data Masking and Anonymization

When AI applications are authorized to receive data, the gateway can still apply protections:

Masking Type	What It Does	Example
PII Masking	Strips identifying information before data reaches the AI	Names, addresses, SSNs removed
Date Shifting	Modifies dates to prevent re-identification	Preserves clinical meaning while hiding exact dates
Geographic Generalization	Replaces specific locations with broader regions	"123 Main St, Springfield" becomes "Midwest region"
Sensitive Category Redaction	Removes categories based on consent settings	Substance use, reproductive health, behavioral health data excluded

Masking is configured by AI application, data category, and patient consent. AI tools receive sufficient clinical data for insights without accessing patient identification details.

Complete Audit Trail for AI Access

Every AI data request is logged with the following details:

Logged Information	Why It Matters
Which AI application requested data	Accountability for each AI vendor
Which patient's data was requested	Patient-level transparency
What data categories were included	Granular visibility into data flows
Whether the request was approved or denied	Compliance documentation
What masking was applied (if approved)	Proof of data minimization
Timestamp of request and response	Complete chronological record

> **Ready for the Regulatory Question**
> When regulators ask "How is patient data flowing into AI systems at your hospital?"—you have a complete, auditable answer.

Regulatory Alignment

Regulation	How PQC+ Addresses It
HIPAA	AI applications treated as business associates; data minimization enforced
GDPR (EU patients)	Right to object to automated decision-making; data anonymization
FDA AI/ML Guidance	Transparency requirements for clinical AI tools
State Consumer Privacy Laws	Opt-out rights for AI data use enforced automatically

Financial Partnerships: Revenue Opportunities and Cost Reduction

Medication Pricing at Point of Care

This is probably the most immediately tangible financial benefit. **Pharmacy Benefit Managers (PBMs)** sit between drug manufacturers, pharmacies, and health plans. They negotiate prices, but they also take substantial markups—typically 8–15% on transactions.

Feature	What It Delivers
Real-Time Pricing	Shows patient out-of-pocket cost at various pharmacies at point of prescribing
Alternative Suggestions	Generic alternatives with price comparisons; therapeutic alternatives
Mail-Order Options	UPS Healthcare mail-order pricing included
Economic Impact	PBM markups drop from 8–15% to just 2%
Hospital Revenue	Transaction-based revenue sharing on facilitated pharmacy transactions
Clinical Integration	SMARTRxPricing includes automatic HCPCS and CPT code mapping

FDX Banking Integration

FDX provides bidirectional integration between PCI DSS (financial) systems and FHIR (healthcare) data layers. This creates interoperability between healthcare and banking-grade security infrastructure.

Practical Applications

- Patient payment processing tied directly to clinical encounters
- Insurance eligibility verification with real-time payment authorization
- Healthcare-specific financial products (payment plans, HSA/FSA integration)

Additional Partnership Coverage

Partnership	What It Covers	Hospital Benefit
Provider Liability Coverage	SMARTCompliance coverage for consumer privacy under 21st Century Cures Act	Shifts some liability risk from hospital to platform—backed contractually
Insurance Payer Agreements	Pre-established SMARTCompliance agreements with major payers	Smoother data exchange, reduced claims friction, streamlined prior auth
Legal Industry Coverage	SMARTCompliance for attorneys handling consumer privacy	Reduces admin burden of legal records requests while maintaining compliance
Health Networks (In Negotiation)	Substantial provider network for managed care arrangements	Preferred referrals, value-based contracts, shared savings, care coordination at scale

How These Three Pillars Reinforce Each Other

> QHIN connectivity gives you comprehensive patient data. AI compliance controls let you use that data with AI tools while maintaining trust and compliance. Financial partnerships create revenue that funds the platform investment. Patient consent sits underneath all of it.

Integrating PQC+ with Your Existing Hospital Systems

Any platform can promise transformative capabilities, but what matters is whether it can actually work with the systems you've already invested millions in—**without disrupting patient care during the transition.**

The Fundamental Architecture: A Connecting Layer, Not a Replacement

PQC+ doesn't replace your EHR, your lab information system, your imaging PACS, or your billing platform. Instead, it sits as a secure, compliant fabric in the middle—connecting everything and adding capabilities your existing systems lack.

Layer	Components
External Connections (Top)	QHINs, Insurance Payers, Labs, Imaging Centers, HIEs
PQC+ Platform (Middle)	SMARTInteroperability + SMARTEntityResolution + SMARTCompliance + SMARTDataLake + other modules
Your Existing Systems (Bottom)	EHR (Epic/Oracle/etc.), Lab System, PACS, Billing, Practice Management

Your staff keeps using the systems they know. PQC+ works behind the scenes to unify data, enforce consent, and enable new capabilities.

Integration with Major EHR Platforms

If You're Running Epic

Integration Path	What It Does
FHIR R4 APIs	Bidirectional flow of demographics, encounters, diagnoses, medications, labs, and clinical notes. PQC+ modules can surface within Epic via App Orchard and SMART on FHIR.
Care Everywhere Integration	Extends Epic's external data exchange to non-Epic sources while adding consent management that Epic doesn't provide natively
ADT/HL7 Feeds	Real-time operational data (admissions, discharges, transfers) via standard HL7 v2 ADT messages. Your existing interface engine keeps working.

If You're Running Oracle Health (Cerner)

Integration Path	What It Does
FHIR R4 APIs	Clinical data exchange through Oracle's FHIR R4 implementation
Millennium Data Integration	Deeper access to clinical documentation, orders, results, scheduling, and revenue cycle data
CommonWell Connectivity	Complements Oracle's CommonWell membership—gives you data from networks CommonWell doesn't reach directly

If You're Running MEDITECH, Allscripts, or Other Systems

PQC+'s interoperability engine is format-agnostic, supporting systems with less mature FHIR implementations.

Method	How It Works
HL7 v2 Messaging	Ingests ADT, ORM, ORU, MDM, etc., transforms to FHIR resources, and converts back for outbound communication. Your existing interfaces don't need to change.
C-CDA Document Exchange	Parses Consolidated Clinical Documents, extracts discrete data elements, converts to FHIR resources
X12 Transactions	Handles eligibility, claims, and remittance; maps to appropriate FHIR resources
Direct Messaging	Sends and receives clinical documents through Direct secure messaging addresses

Handling Your Existing Data: The Migration Reality

> **Your Data Doesn't Move**
>
> You're not migrating 15 years of patient data out of your EHR. Instead, PQC+ creates a unified index that knows where data lives and can retrieve it on demand. The data stays where it is. PQC+ provides the intelligence layer that makes it accessible and compliant.

How On-Demand Retrieval Works

1. PQC+ queries your EHR for internal historical data
2. Simultaneously queries connected QHINs for external data
3. Applies identity resolution to match records correctly
4. Enforces consent rules to filter what's viewable
5. Presents a unified view to the clinician

As new clinical data is generated, PQC+ captures it in real-time. The **SMARTDataLake** then builds a comprehensive, FHIR-based repository over time, containing structured clinical data, AI-ready vector representations (for CDS), and knowledge graph relationships (for care gap identification).

Identity Resolution: Solving the Duplicate Patient Problem

Most hospitals have a duplicate patient rate between **8–12%**—roughly 1 in 10 patient records is actually a duplicate. This creates clinical risk and administrative burden. Here's how SMARTEntityResolution works alongside your existing MPI:

Capability	How It Works
Probabilistic Matching	AI evaluates name variations (Robert vs. Bob vs. Roberto), address changes, phone updates, DOB discrepancies, SSN, and insurance member IDs
Cross-Reference Table	Maintains links between your EHR's internal patient IDs, external identifiers (lab accounts, imaging IDs, payer numbers), and a PQC+ Enterprise Patient Identifier (EPI)
Ongoing Stewardship	Potential duplicates are queued for review in SMARTDashboard. Your HIM team adjudicates matches; the system learns from their decisions.

Real-World Scenario: Emergency Department

Situation	Without PQC+	With PQC+
Patient arrives at your ED. They were last seen at an unaffiliated PCP across town and had lab work at a commercial reference lab.	You might not know about the PCP visit or lab results. Even HIE data may not clearly match your patient. Treatment decisions are based on incomplete information.	System queries connected QHINs, identifies matching records, confirms identity despite demographic variations, checks consent, and shows the ED physician a unified view with PCP notes, medications, and recent lab results.

Workflow Integration: Where Clinicians Actually Experience It

Within the EHR (Embedded View)

Feature	How It Works
SMART on FHIR Apps	Clinicians launch PQC+ modules directly from the patient chart. SMARTLayers (external data), SMARTDiagnosis (AI diagnostic support), and SMARTRxPricing (medication pricing) all open in context—no separate login required.
Results Integration	External clinical data can be written back into your EHR as discrete data (labs, medications, problem lists) or as documents (clinical summaries, care plans).

Standalone Dashboard (For Specific Use Cases)

Interface	Used By	For What
SMARTDashboard	Administrative users	User access management, consent configuration, audit log review, system health monitoring
SMARTAnalytics	Population health / quality teams	Business intelligence, care gap identification, value-based care performance
SMARTWorkflow	Operations teams	Care coordination workflows, automated alerts, referral routing logic

Mobile Access

SMARTOpenHealth provides iOS and Android access for clinicians on the move—hospitalists rounding, care managers doing home visits, physicians checking remotely. Full consent enforcement and post-quantum encryption protect data on every device.

A Phased Implementation Approach

No hospital should implement all 26+ SMART modules simultaneously. PQC+'s modular architecture supports a phased approach that demonstrates value at each stage:

Phase	Timeline	What Gets Deployed	Immediate Value
Phase 1: Foundation	Months 1–3	SMARTInteroperability, SMARTEntityResolution, SMARTCompliance, SMARTDataLake, EHR integration, QHIN connectivity, SSO	Unified patient view with external data; consent management operational; audit trail begins
Phase 2: Clinical Enhancement	Months 4–6	SMARTDiagnosis, SMARTHealthInsite, SMARTCDM, SMART on FHIR apps in EHR, additional QHIN and ancillary connections	AI diagnostic support for physicians; care gap identification; chronic disease management
Phase 3: Revenue Optimization	Months 7–9	SMARTRxPricing, SMARTRCM, SMARTVBR, strategic partner integration, payer connectivity	Medication pricing transparency; RAF scoring; transaction-based revenue sharing begins
Phase 4: Advanced Capabilities	Ongoing	SMARTClinicalTrialMatching, SMARTAnalytics, SMARTAmbienBOT, SMARTNonStructure-to-Structure, full AI Compliance Gateway	Research matching; full BI deployment; ambient documentation; unstructured data processing

What Your IT Team Needs to Know

Infrastructure Requirements

Requirement	Details
Cloud-Based Platform	No on-premises hardware to deploy. Scalability and updates handled centrally by the platform.
Network Connectivity	Standard HTTPS outbound traffic to PQC+'s cloud environment. Typically no firewall changes beyond normal outbound web access.
Interface Engine Compatibility	Works with Rhapsody, Mirth, Cloverleaf, and other standard healthcare interface engines. Existing HL7 interfaces extend to include PQC+ as a destination.

Security Integration

Security Feature	Implementation
Single Sign-On	Integrates with SAML, OAuth, and OpenID Connect. Staff use existing credentials—no separate passwords.
Attribute-Based Access Control	Your existing role definitions (physician, nurse, registration, HIM) map to PQC+ access levels via SMARTDashboard.
Encryption	Post-quantum cryptographic standards for data in transit and at rest. Exceeds current HIPAA requirements.
Data Governance	Your data stays yours. PQC+ provides processing and integration but your data remains under your control.
BAA Coverage	Transformativ IP executes a Business Associate Agreement, taking on HIPAA obligations for data processed on your behalf.

Realistic Implementation Timelines

Phase	Timeline	Key Milestones
Contracting & Planning	Weeks 1–2	Scope definition, BAA execution, project kickoff
Phase 1 (Foundation)	Weeks 1–3	Core platform live, EHR connected, basic consent operational
Phase 2 (Clinical)	Weeks 1–2	Clinical modules deployed, SMART apps in EHR workflows
Phase 3 (Financial)	Weeks 1–2	Revenue modules active, partnerships generating value
Phase 4 (Advanced)	Ongoing	Continuous capability expansion

Risk Mitigation

Risk	Mitigation Strategy
Integration Complexity with Legacy Systems	PQC+ supports HL7 v2 and C-CDA—even older systems can integrate. Start with the cleanest integration path (usually ADT feeds and results), then expand.
Clinician Adoption Resistance	SMART on FHIR means clinicians never leave their EHR. New capabilities surface within familiar workflows. Phased rollout allows training and adjustment.
Patient Consent Configuration Complexity	Start with simple consent categories, then add granularity. PQC+ provides default templates based on regulatory requirements.
Data Quality Issues Surfacing	Identity resolution will reveal duplicates you didn't know you had. Plan HIM resources for the initial backlog—long-term, you end up with cleaner data.

Deep Dive: Major Integration Aspects

This section provides the technical detail your implementation team needs. It covers the decisions you'll make, the work involved, and how the pieces fit together.

1. Data Integration Architecture

Data Flow Patterns

Data moves through a PQC+-enabled environment in three primary patterns:

Pattern	How It Works	Use Case
Real-Time Transactional	Source System → Interface Engine → PQC+ → Consent Check → Data Lake. Source systems continue normal operation; PQC+ receives a copy.	Patient registrations, orders, results, clinical documentation as they happen
Query-Response	Clinician Request → EHR → PQC+ Query Broker → Multiple Sources → Identity Resolution → Consent Filtering → Unified Response	On-demand retrieval when a clinician needs a complete patient record including external data
Batch Synchronization	Scheduled Job → Bulk Extract → PQC+ Ingestion → FHIR Transformation → Identity Resolution → Data Lake Update	Historical data loads, periodic reconciliation, analytics data refreshes

HL7 v2 Messaging: The Workhorse

Message Type	Purpose	Typical Use Case
ADT (A01, A02, A03, A04, A08, etc.)	Admissions, Discharges, Transfers	Real-time patient movement tracking
ORM / OML	Orders	Capturing order activity
ORU	Observation Results	Lab results, vital signs, clinical observations
MDM	Medical Document Management	Clinical document notifications
SIU	Scheduling	Appointment creation and updates
DFT	Detailed Financial Transaction	Charge capture
BAR	Billing Account Record	Account updates

Implementation detail: Your interface engine routes copies of these messages to PQC+. The FHIR transformation happens within PQC+, not in your interface engine—keeping your existing interfaces unchanged. Configuration requires message routing rules, endpoint configuration (typically HTTPS with mutual TLS), message filtering, and error handling/retry logic.

FHIR R4 APIs: The Modern Standard

For EHRs with mature FHIR implementations (Epic, Oracle Health, some MEDITECH Expanse), API-based integration provides richer, more flexible exchange.

FHIR Resource Category	Resources Supported
Patient Identity	Patient, RelatedPerson, Person
Clinical	Condition, Procedure, Observation, DiagnosticReport, DocumentReference
Medications	MedicationRequest, MedicationDispense, MedicationStatement, MedicationAdministration
Care Planning	CarePlan, Goal, ServiceRequest, CareTeam
Encounters	Encounter, EpisodeOfCare, Appointment
Financial	Coverage, Claim, ExplanationOfBenefit, Account
Administrative	Organization, Practitioner, PractitionerRole, Location

PQC+'s SMARTLayers module can display all 150+ FHIR resource types, with consent-based masking applied dynamically.

C-CDA Document Exchange

Document Type	Content
Continuity of Care Document (CCD)	Comprehensive patient summary
Discharge Summary	Hospital discharge information
Referral Note	Information for receiving provider
Progress Note	Clinical encounter documentation
Consultation Note	Specialist consultation findings
History and Physical	Complete H&P documentation
Operative Note	Surgical procedure documentation

Processing pipeline: Incoming C-CDA documents are parsed and discrete data elements extracted—problems become Condition resources, medications become MedicationStatement resources, allergies become AllergyIntolerance resources, and so on. PQC+ can also generate C-CDA documents from FHIR data for outbound communication with systems that don't support FHIR.

X12 Transaction Sets

Transaction	Purpose
270/271	Eligibility inquiry and response
276/277	Claim status inquiry and response
278	Prior authorization request and response
837	Healthcare claim submission
835	Electronic remittance advice

2. Identity and Access Management Integration

Single Sign-On (SSO) Integration

Protocol	Use Case	Configuration Elements
SAML 2.0	Standard enterprise SSO via Active Directory or similar	IdP metadata exchange, attribute mapping, session timeout, single logout
OAuth 2.0 / OpenID Connect	Mobile app auth, API access, SMART on FHIR app launches	Client credentials, scope configuration, token management

Role-Based Access Mapping

Role	Module Access	Data Access Level
Physician	SMARTDiagnosis, SMARTRxPricing, SMARTLayers	Full clinical data access
Nurse	SMARTLayers, SMARTCDM, SMARTTriage	Nursing-scope data access
Registration Staff	SMARTForms	Demographics only
HIM Professional	SMARTDashboard, Audit tools	Access management scope
Administrator	Full SMARTDashboard	Configuration and monitoring

Granular Permission Configuration

Permission Category	Options
Module Access	Which SMART apps each role can use
Data Category Access	Which FHIR resource types are visible
Patient Population Scope	All patients, assigned patients only, department-specific
Action Permissions	View, create, modify, delete, export
Sensitive Data Access	Behavioral health, substance use, reproductive health

> **Seamless EHR Context**
> When PQC+ modules launch from within your EHR via SMART on FHIR, patient context, encounter context, user identity, and role all flow automatically. The clinician doesn't re-authenticate or re-select the patient. The module opens directly in context, ready to provide value. This seamless experience is critical for adoption.

3. Consent Management Implementation

This is PQC+'s core differentiator. Here's the implementation detail.

Consent Dimensions

Dimension	Description	Examples
Grantor	Who is giving consent	Patient, legal guardian, healthcare proxy
Grantee	Who receives the consent	Specific provider, organization, AI application, payer
Data Scope	What data is covered	All records, specific categories, date ranges
Purpose	Why data is being shared	Treatment, payment, research, AI training
Time Bounds	When consent is valid	Effective date, expiration date
Conditions	Special requirements	Break-glass override, emergency access

Consent Capture Workflows

Capture Method	How It Works
Patient Portal Integration	Patient logs in, makes consent selections, portal sends FHIR Consent resource to SMARTCompliance
In-Person Registration	Staff uses SMARTForms to present consent questionnaire; patient signs electronically or on paper
Mobile App (SMARTOpenHealth)	Patients view/modify consent settings, receive notifications when consent is used, review data access audit trail

Jurisdictional Compliance Engine

When a data access request arrives, SMARTCompliance evaluates all applicable laws—federal (HIPAA, 42 CFR Part 2, Cures Act), the patient's state of residence, the provider's state, and data category rules—then applies the most restrictive combination plus the patient's explicit consent choices.

> **Multi-State Example**
> A patient lives in California (CCPA applies), receives care at a Texas hospital, and records are requested by a New York insurer. PQC+ evaluates California Consumer Privacy Act requirements, Texas Health and Safety Code provisions, New York insurance regulations, the HIPAA federal baseline, and the patient's explicit consent choices—then applies the most restrictive combination.

Sensitive Data Categories

Category	Special Requirements	How PQC+ Handles It
42 CFR Part 2 (Substance Use)	Stricter than HIPAA; requires separate written consent; re-disclosure prohibited	Requirements enforced automatically; separate consent tracked

Category	Special Requirements	How PQC+ Handles It
Reproductive Health	Increasingly protected under state laws	Tagged for special handling; consent rules separate from general clinical data
Behavioral Health	Many states have additional protections	Supports granular behavioral health consent; patients control mental health record access
Minor's Records	Complex rules about parental access vs. minor's privacy; varies by state and service type	Applies appropriate rules based on patient age and jurisdiction automatically

4. Security Architecture Integration

Post-Quantum Cryptography: What It Actually Means

Most healthcare encryption uses RSA or elliptic curve cryptography. These rely on mathematical problems that are hard for classical computers but **potentially easy for quantum computers**. A sufficiently powerful quantum computer could decrypt data that was encrypted years earlier. PQC+ implements algorithms designed to resist both classical and quantum attacks:

NIST Standard	Algorithm	What It Protects
FIPS 203	ML-KEM (Module-Lattice-Based Key-Encapsulation)	Data encryption key exchange
FIPS 204	ML-DSA (Module-Lattice-Based Digital Signature)	Digital signatures and authentication
FIPS 205	SLH-DSA (Stateless Hash-Based Digital Signature)	Additional digital signature protection

Protection Layer	Implementation
Data at Rest	Encrypted with PQC algorithms in SMARTDataLake
Data in Transit	TLS 1.3 with PQC key exchange
Access Control	Embedded in cryptographic key structure—can't decrypt without satisfying access rules

Network Security Integration

Security Measure	Details
Mutual TLS (mTLS)	Both sides present certificates for interface connections, ensuring data only flows to/from verified endpoints
IP Whitelisting	PQC+ accepts connections only from your organization's known IP ranges
SIEM Integration	Exports audit logs to Splunk, Microsoft Sentinel, IBM QRadar, etc. via syslog, CEF, or JSON formats

Audit Record Detail

Every PQC+ action generates a comprehensive audit entry:

Audit Field	What's Captured
Timestamp	High-precision timing
User Identity & Role	Who performed the action and their role
Action Type	View, create, modify, export, etc.
Patient Identifier	Whose data was accessed
Data Categories	What types of data were accessed
Consent Basis	The legal basis for the access
Source IP / Device	Where the access originated
Success/Failure	Whether the action succeeded, and if not, why

5. Clinical Workflow Integration

EHR-Embedded Experience

The goal is for clinicians to gain PQC+ capabilities without leaving their EHR. Here's how the key modules integrate:

SMARTDiagnosis: Clinician opens patient chart → Clicks "Diagnostic Support" → Module opens in EHR sidebar → Receives patient context via SMART on FHIR → Queries complete patient history (including external data) → AI generates ranked differential diagnoses with evidence citations → Clinician selects diagnosis to add to problem list → Written back to EHR.

SMARTRxPricing: Clinician creates medication order → Module auto-launches → Queries network for insurance coverage, out-of-pocket costs, generics, and mail-order options → Pricing displayed → Clinician selects alternative if desired → Order updated in EHR.

Care Management Workflow

SMARTCDM (Chronic Disease Management): Daily batch process identifies patients due for Annual Wellness Visits, CCM touchpoints, RPM reviews, and TCM follow-ups. Worklists appear in SMARTDashboard. Care managers see a complete longitudinal view across all providers—conditions, medications, encounters, care gaps, and RPM device data—and time is tracked automatically for billing with HCPCS/CPT codes suggested.

Automatic Billing Code Mapping

Many SMART modules include AI-powered coding assistance:

1. Clinical activity is documented
2. AI analyzes the documentation
3. Appropriate codes are suggested (CPT, HCPCS Level II, ICD-10)
4. Coder reviews and confirms
5. Charges generated for billing system

This reduces coding delays, improves accuracy, and captures revenue that might otherwise be missed.

Ambient Clinical Documentation (SMARTAmbienBOT) With patient consent, SMARTAmbienBOT transcribes and identifies speakers in clinician-patient conversations in real-time, structuring the output into a SOAP note (CC, HPI, ROS, PE, A/P). The clinician reviews and approves the note, which then flows to the EHR with suggested codes. Integration covers room mics, clinician devices, telehealth, and EHR templates.

6. External Connectivity Integration

Phased QHIN Enablement

Phase	QHINs	Rationale
Initial	eHealth Exchange, CommonWell	Broadest coverage, most mature
Expansion	Epic, Oracle Health	Direct connectivity to large health systems
Specialized	Surescripts, Health Gorilla	Pharmacy data, lab data specifically
Complete	All certified QHINs	Maximum coverage

Lab and Imaging Integration

Reference Lab Integration: Lab orders placed in EHR are transmitted normally. Results return via HL7 ORU. PQC+ receives a copy, transforms to FHIR Observation and DiagnosticReport resources, applies identity resolution, tags with consent categories, and stores in the DataLake for the unified patient view.

Imaging Center Integration: Radiology reports arrive via HL7 MDM or ORU and become FHIR DiagnosticReport resources. DICOM images are referenced in FHIR ImagingStudy resources. Consent rules are applied, including sensitive data masking for images when appropriate.

7. Testing and Validation

Testing Phase	What's Tested
Phase 1: Connectivity	Network connectivity, authentication (SSO, API credentials), message routing in interface engine
Phase 2: Data Transformation	Sample HL7 messages sent, FHIR conversion accuracy verified, data mapping completeness validated
Phase 3: Identity Resolution	Test patients with variations (name misspellings, address changes), matching algorithm accuracy, false positive handling
Phase 4: Consent Enforcement	Every consent combination tested, data visibility/masking verified, break-glass override tested, audit trail completeness
Phase 5: End-to-End Workflows	Clinical user scenarios, administrative scenarios, external data queries, AI module testing
Phase 6: Performance	Concurrent user load, large data volumes, query response times, failover and recovery

Go-Live Readiness Checklist

Category	Checkpoints
Technical	All interfaces operational and monitored; SSO verified; backup/recovery tested; performance benchmarks met
Security	BAA executed; security assessment completed; audit logging verified; incident response documented
Operational	Support escalation paths defined; user training completed; helpdesk prepared; go-live communication sent
Compliance	Consent capture workflows operational; jurisdictional rules configured; audit reports reviewed; privacy officer sign-off

8. Ongoing Operations and Support

Monitoring and Alerting

PQC+ provides a real-time dashboard showing interface connectivity status, transaction volumes, error rates, response time metrics, and storage utilization. Alerts for connection failures, unusual error rates, performance degradation, and security anomalies go to both PQC+ operations and your IT team via email, SMS, or SIEM integration.

Support Model

Tier	Responsibility	Response Time
Tier 1	Your helpdesk (basic user questions)	Per your standards
Tier 2	Your IT team (configuration, troubleshooting)	Per your standards
Tier 3	PQC+ support (platform issues)	SLA-defined
Tier 4	PQC+ engineering (complex issues)	SLA-defined

Summary: Integration Success Factors

Having walked through all the major integration aspects, here are the critical success factors:

Success Factor	What It Means in Practice
Technical Excellence	Clean, well-documented interfaces reduce troubleshooting time. Thorough testing prevents go-live surprises. Monitoring enables proactive issue resolution.
Organizational Alignment	IT, clinical leadership, compliance, and operations all engaged. Clear ownership of integration decisions. Executive sponsorship for resource allocation.
Phased Approach	Start with foundational capabilities. Prove value before expanding. Learn and adjust with each phase.
User-Centric Design	Clinicians shouldn't feel the burden of new technology. Workflows should be enhanced, not disrupted. Training should be role-appropriate and practical.