Epic FHIR Implementation Readiness Checklist

SMART | CMS Rule | Information Blocking | HIPAA | TechFitFlow.com

Complete every section before enabling production FHIR API access. Sandbox testing success does not mean production readiness. Budget 4-8 weeks for production integration testing after sandbox validation completes.

SMART APP REGISTRATION AND SCOPE CONFIGURATION

	Gate Item	Owner	Sign-off
[ ]	App registered in Epic Interconnect with correct client ID and redirect URI	_____	_____
[ ]	FHIR scopes requested enumerate only resource types the app actually reads - no wildcard patient/*.read	_____	_____
[ ]	Privacy officer has reviewed the patient consent screen language before production approval	_____	_____
[ ]	Consent screen text accurately describes what data the app accesses in plain language	_____	_____
[ ]	App developer has completed Epic's app registration process (App Orchard or internal review)	_____	_____
[ ]	EHR Launch context configured correctly if app launches from within Epic clinical interface	_____	_____
[ ]	App uses SMART Backend Services authorization (JWT) if operating as system-to-system without patient auth	_____	_____
[ ]	Access token expiration and refresh token handling confirmed in app implementation	_____	_____
[ ]	App has been tested in Epic sandbox (open.epic.com) with synthetic patients	_____	_____

HIPAA COMPLIANCE AND BAA REVIEW

	Gate Item	Owner	Sign-off
[ ]	Business Associate Agreement (BAA) confirmed with every third-party app receiving PHI via FHIR	_____	_____
[ ]	BAA in place before any production FHIR access is granted - no PHI before BAA	_____	_____
[ ]	HIPAA minimum necessary review: app scopes access only the data needed for its stated purpose	_____	_____
[ ]	PHI data handling reviewed: how does the app store, process, and protect FHIR data it receives?	_____	_____
[ ]	User access to FHIR-connected app is covered by HIPAA access controls appropriate to their role	_____	_____

	Gate Item	Owner	Sign-off
[ ]	Audit logging confirmed: Epic logs FHIR API calls; app-side audit logging also confirmed	_____	_____
[ ]	Data retention policy for FHIR-sourced PHI in the third-party app is documented and appropriate	_____	_____
[ ]	Privacy officer sign-off on all FHIR API access configurations for PHI-containing resources	_____	_____

ONC INFORMATION BLOCKING COMPLIANCE

	Gate Item	Owner	Sign-off
[ ]	Legal and compliance team briefed on ONC information blocking prohibition and recognized exceptions	_____	_____
[ ]	Any decision to restrict FHIR API access is reviewed by compliance before implementation	_____	_____
[ ]	Each access restriction is documented with the specific recognized exception that justifies it	_____	_____
[ ]	No access restriction is based on competitive concern or commercial preference - only recognized exceptions	_____	_____
[ ]	FHIR endpoint is publicly discoverable via the organization's well-known SMART configuration endpoint	_____	_____
[ ]	FHIR API availability does not depend on users having non-Epic-standard agreements with the health system	_____	_____
[ ]	ONC information blocking complaint process documented internally - clear escalation path if complaint received	_____	_____

PRODUCTION INTEGRATION TESTING

	Gate Item	Owner	Sign-off
[ ]	Production FHIR integration test plan developed - 4-8 weeks allocated after sandbox success	_____	_____
[ ]	Real coverage records used in production PA API testing (not synthetic sandbox data)	_____	_____
[ ]	Payer FHIR sandbox validated first, then payer FHIR production endpoint tested separately	_____	_____
[ ]	Coverage resource identifier format confirmed matching between Epic and payer FHIR endpoint	_____	_____
[ ]	FHIR resource data quality audited: Condition, MedicationRequest, and Observation resources checked for completeness	_____	_____

	Gate Item	Owner	Sign-off
[ ]	OperationOutcome error handling tested - app gracefully handles FHIR error responses	_____	_____
[ ]	Rate limiting behavior confirmed - app handles 429 (too many requests) responses from Epic FHIR	_____	_____
[ ]	FHIR conformance validation run with HL7 FHIR validator or ONC Inferno testing framework	_____	_____
[ ]	Production test results documented and reviewed by both technical and compliance staff	_____	_____

CMS INTEROPERABILITY RULE COMPLIANCE (2026 REQUIREMENTS)

	Gate Item	Owner	Sign-off
[ ]	Prior Authorization API: Epic configured to submit FHIR-based PA requests to regulated payers	_____	_____
[ ]	Da Vinci PAS Implementation Guide requirements reviewed for all applicable payers	_____	_____
[ ]	CRD (Coverage Requirements Discovery) hooks configured in Epic CPOE for applicable payers	_____	_____
[ ]	DTR (Documentation Templates and Rules) configured if applicable payer supports it	_____	_____
[ ]	Provider directory information confirmed up to date with all regulated payers' FHIR directories	_____	_____
[ ]	Payer-to-provider care record exchange via PDex reviewed and configured for applicable payers	_____	_____
[ ]	FHIR ID vs Epic internal ID documentation provided to all developers using FHIR integrations	_____	_____
[ ]	CMS compliance status documented per payer: which payers have implemented required FHIR APIs	_____	_____