QUANTUM CORE INSTITUTE

QCI-QS1-S2

Healthcare Supplement

Quantum Readiness Guidance for Mid-Sized Medical Practices and HIPAA-Covered Entities

Document ID	QCI-QS1-S2
Version	1.2
Status	Public — Free to download and cite
Publisher	Quantum Core Institute (QCI)
Normative ref	QCI-QS1 Version 2.3 (September 23, 2026). Clause references are QCI requirement identifiers.
Applies to	HIPAA-covered entities including medical practices, clinics, and their business associates handling ePHI
Effective date	September 23, 2026
Review cycle	Annual, or upon material HHS, OCR, or HIPAA regulatory developments, or a new edition of QCI-QS1

This supplement extends QCI-QS1 for the specific regulatory, vendor, and data-horizon context of mid-sized medical practices and other HIPAA-covered entities. It maps quantum readiness requirements to HIPAA Security Rule obligations, OCR enforcement patterns, and EHR vendor dependencies that define cryptographic exposure for most practices in this sector.

Foreword

A mid-sized medical practice is not a natural target for a document about quantum computing. Its staff thinks about patient care, billing compliance, and scheduling software — not post-quantum cryptography migration timelines. That disconnect is precisely the problem.

The electronic health records (EHR) systems, patient portals, and billing platforms that practices rely on hold some of the most sensitive and longest-lived personal data in any industry. A patient's medical history, diagnosis records, and genetic information may need to remain confidential for decades. Under HIPAA, the obligation to protect that data does not expire when the practice closes or the software vendor updates its terms.

The harvest-now, decrypt-later threat means that encrypted patient data being transmitted or stored today could be decrypted in the future when quantum computing capabilities mature. This creates a delayed breach scenario that most practices have not modeled — and that HIPAA's breach notification rules may require them to address when the technology arrives.

This supplement translates QCI-QS1 for the specific context of medical practices and HIPAA-covered entities. It is written to be accessible to practice administrators and compliance officers with clinical backgrounds, not just technical security staff. The quantum threat is real but manageable. The organizations that document their exposure and begin working their EHR vendors now will be the ones in the strongest position when HHS guidance and OCR enforcement catch up to the technology.

What changed in version 1.2

Version 1.2 aligns this supplement to QCI-QS1 version 2.3. For a practice, three changes matter. The Defensible readiness band now begins at 81, though no practice profile in this supplement reaches it within twelve months. Gate G70 is no longer satisfied by a documented exception: a practice cannot score above 70 until its EHR vendor and every other critical business associate has provided an adequate response and an officer-signed attestation, and section 3.4 says what that means for a practice on a single EHR. Gate G60 is fixed at 95 percent validated coverage of both critical systems and critical data flows, so the claims and referral flows count alongside the systems. Section 2.4 is new: it turns the HIPAA mapping into the obligations register that QCI-2.2-01 requires. Section 9 also adds one line for the assessment type a practice reports.

1. Scope and applicability

This supplement applies to:

- Medical practices of 10 or more physicians, including specialty and multi-site practices
- Ambulatory surgery centers, imaging centers, and outpatient clinics operating as HIPAA-covered entities
- Business associates that create, receive, maintain, or transmit electronic protected health information (ePHI) on behalf of covered entities
- Health information exchanges (HIEs) and regional health networks
- EHR and practice management software vendors whose products process ePHI for practices in scope

Smaller practices with fewer than 10 physicians may apply this supplement at a proportionally reduced scope, focusing on EHR vendor engagement and horizon analysis rather than the full governance model. Proportionality does not change the gates: the coverage threshold and the

supplier attestation requirement apply to whatever assessment boundary the practice declares (QCI-1.1-01), and a small boundary is easier to cover than a large one.

A note on technical accessibility

This supplement is written for compliance officers, practice administrators, and practice managers — not only for IT professionals. Technical terms are explained on first use. The goal is to give the person responsible for HIPAA compliance in a mid-sized practice enough understanding to ask the right questions of their EHR vendor, their IT support, and their legal counsel.

Note on the AI-cryptographic provisions

QCI-QS1 carries conditional AI-cryptographic provisions. Where AI systems fall within the assessment scope — for a practice, most often an ambient documentation or clinical decision support tool operated by a vendor — the organization also keeps linked AI artifact records with separate confidentiality and verification horizons (QCI-5.2-03), exercises the D7-AI incident scenarios (QCI-4.4-03), includes AI suppliers' posture in Pillar 5 (QCI-6.4-01), and issues Annex C section G, questions G1 to G5, to suppliers of AI platforms, ML infrastructure, model registries, or key management used with AI artifacts. These provisions have no effect where AI systems are not in scope; a non-AI system records AI applicability as none. They govern cryptographic risk arising from AI systems. They do not govern AI risk generally.

2. HIPAA regulatory context

2.1 The HIPAA Security Rule and cryptographic obligations

The HIPAA Security Rule (45 CFR Part 164) requires covered entities to implement technical safeguards for electronic protected health information. The encryption requirements are addressable — meaning they are not mandatory if the covered entity documents why another measure is reasonable and appropriate. However, encryption is the standard safeguard for ePHI in transit and at rest, and OCR enforcement has treated inadequate encryption as a primary contributing factor in numerous breach investigations.

Five Security Rule provisions are directly relevant to quantum readiness:

HIPAA Security Rule provision	CFR citation	Quantum readiness relevance
Transmission security — encryption	45 CFR 164.312(e)(2)(ii)	ePHI transmitted using algorithms vulnerable to quantum attack may not provide adequate protection when those attacks become feasible
Encryption and decryption of ePHI at rest	45 CFR 164.312(a)(2)(iv)	ePHI whose data keys are protected by quantum-vulnerable key establishment or key wrapping is exposed to harvest-now, decrypt-later attack; decryption constitutes a breach
Risk analysis and risk management	45 CFR 164.308(a)(1)	Risk analysis must identify threats to ePHI confidentiality; quantum computing risk is an identified and documented threat that must be assessed
Evaluation of technical and nontechnical safeguards	45 CFR 164.308(a)(8)	Periodic evaluation must consider whether current safeguards remain adequate; quantum computing capability advances trigger this requirement

HIPAA Security Rule provision	CFR citation	Quantum readiness relevance
Business associate agreements	45 CFR 164.308(b)	Business associates (including EHR vendors) must provide equivalent safeguards; quantum readiness attestation is an extension of this obligation

2.2 The breach notification connection

This is the regulatory argument that moves quantum readiness from best practice to urgent obligation for most practices.

Under HIPAA's Breach Notification Rule (45 CFR Part 164, Subpart D), a covered entity must notify affected individuals, HHS, and in some cases media outlets when unsecured ePHI is accessed, acquired, disclosed, or used without authorization. The rule provides a safe harbor: if ePHI was encrypted using a technology that renders it unusable, unreadable, or indecipherable to unauthorized persons, the disclosure may not constitute a reportable breach.

The critical question for quantum readiness is this: if ePHI was encrypted using RSA or ECC in 2025 and a quantum computer decrypts it in 2035, does the original encryption provide the safe harbor? The honest answer is that current HIPAA guidance does not address this scenario, but the direction of regulatory travel is clear. HHS OCR has consistently interpreted breach notification obligations broadly. A covered entity that cannot demonstrate it used encryption adequate to protect ePHI for the duration of the retention period faces significant exposure.

The legal question your practice needs to answer now

If encrypted ePHI stored or transmitted today is decrypted by a quantum computer in the future, does your practice face a HIPAA breach notification obligation? This question should be put to your HIPAA legal counsel before the scenario becomes reality. The practices that have a documented legal opinion and a remediation plan are in a fundamentally different position from those that have neither.

2.3 OCR enforcement patterns

OCR enforcement actions consistently cite inadequate encryption and failure to conduct thorough risk analysis as primary findings. Quantum readiness maps directly to both:

- Failure to conduct thorough risk analysis (45 CFR 164.308(a)(1)): A risk analysis that does not address quantum computing threats to current cryptographic controls is increasingly difficult to defend as comprehensive. OCR has broad authority to find that a risk analysis was inadequate.
- Failure to implement technical safeguards (45 CFR 164.312): As quantum computing capabilities advance, regulators will eventually take the position that adequate technical safeguards require quantum-resistant protection for long-lived ePHI. Practices that have begun migration planning are better positioned to demonstrate good faith.
- Business associate oversight failures (45 CFR 164.308(b)): EHR vendors are business associates. A covered entity that has not assessed its EHR vendor's quantum readiness has a gap in its business associate oversight program that OCR audits may identify.

2.4 Obligations register entries for this sector

QCI-2.2-01 requires an applicability register listing each relevant external obligation with its issuer, exact document and revision, date, authoritative URL, applicable sections, status, affected systems and suppliers, required actions and deadlines, exception authority, accountable owner, and last verification date. For a practice, the register can be a single page in the HIPAA compliance binder. The entries below are the minimum; each practice adds its state medical-record retention statute and any payer or network contract terms, and verifies every entry against the source.

Obligation	Issuer and document	Status	Affected systems and suppliers	Action and deadline
Security Rule technical safeguards	HHS; 45 CFR 164.312(a)(2)(iv), 164.312(e)(2)(ii)	Regulation; encryption addressable	EHR, patient portal, billing, telehealth, imaging	Document current protection and the quantum threat in the risk analysis
Risk analysis, risk management, evaluation	HHS; 45 CFR 164.308(a)(1), 164.308(a)(8)	Regulation	All ePHI systems	Add the quantum threat assessment (section 9) at the next annual risk analysis
Business associate agreements	HHS; 45 CFR 164.308(b), 164.314	Regulation	EHR vendor, billing clearinghouse, telehealth platform, cloud host	Quantum readiness attestation at next BAA renewal; Annex C request now
Breach notification	HHS; 45 CFR Part 164 Subpart D	Regulation; safe harbor scope unresolved for delayed decryption	All ePHI in transit and at rest	Written counsel opinion on the delayed breach scenario (section 4.2)
Medical record retention	State statutes; CMS Medicare and Medicaid record requirements	Law and regulation; varies by state	Clinical records, minor records, imaging, billing	Set confidentiality horizons in the QASI from the longest applicable retention

3. EHR and practice management vendor landscape

3.1 Why EHR vendor dependency defines practice exposure

A mid-sized medical practice rarely builds or controls the cryptographic infrastructure protecting its patient data. Epic, Oracle Health (formerly Cerner), athenahealth, eClinicalWorks, Allscripts, and their peers determine how ePHI is encrypted, how it is transmitted, and when post-quantum cryptography support will be available.

This creates a dependency structure that mirrors the core banking problem in the financial sector: the practice's quantum exposure is largely determined by its EHR vendor's roadmap. The difference is that healthcare data carries longer retention obligations and higher individual harm potential than most financial data types. Under QCI-QS1 v2.3 the dependency has a scoring consequence too: the practice's Q-Risk Score is capped at 70 until the EHR vendor attests (section 3.4).

3.2 EHR vendor considerations

The status of each vendor's post-quantum roadmap changes with every release; confirm the current position with the vendor and record it, with the date, in the QASI supplier record (QCI-5.2-01).

Vendor	Market presence	Key crypto exposure areas	Recommended practice action
Epic	Large health systems and affiliated practices	Patient portal TLS, ePHI at rest, FHIR API authentication, MyChart identity	Request the PQC roadmap and attestation via the account team; escalate to VP level if no adequate response within the 60-day deadline
Oracle Health (Cerner)	Mid to large practices and health systems	Millennium encryption, HIE data exchange crypto, patient identity	Issue the formal Annex C request; reference BAA obligations and quantum risk
athenahealth	Small to mid-sized practices	Cloud-hosted ePHI encryption, patient portal, billing data transmission	Contact the compliance team directly; reference the HIPAA BAA and request a written PQC roadmap and attestation
eClinicalWorks	Small to mid-sized practices	ePHI at rest, patient portal, telehealth crypto, billing integration	Request a scoped CBOM or crypto library inventory meeting QCI-5.4-03; ask specifically about TLS and at-rest key-protection roadmap
Allscripts / Veradigm	Mid-sized practices	EHR data encryption, practice management crypto, connectivity platform	Engage the account manager; reference HIPAA technical safeguard obligations in the request

3.3 What to ask your EHR vendor

Most practices will not have a dedicated security officer to manage vendor engagement. The following questions are written to be asked by a practice administrator or compliance officer in plain language. They correspond to Annex C sections A to F; the vendor's answers, with the officer-signed attestation on the Annex C form, are what the standard counts.

1. What encryption does your system use to protect patient data stored in your system, and what protects the keys? Is it vulnerable to quantum computers?
2. Do you have a roadmap for upgrading to post-quantum cryptography? If so, what is the timeline, which product release, and what will we need to do on our end?
3. Will our patient data be protected against future quantum computing capabilities, or will we need to re-encrypt it when you upgrade? What about backups and copies already made?
4. Are you aware of the harvest-now, decrypt-later threat? Has your team assessed whether current encryption protects data for the full retention period?
5. As our business associate, what is your plan for ensuring that ePHI we share with you remains protected against emerging threats including quantum computing, and will an officer of your company sign the attestation form we send?

If your EHR vendor cannot answer these questions or does not take them seriously, that is itself a finding that belongs in your risk analysis documentation. Document the question, the date, the person you asked, and the response — or the absence of one. Set a response deadline no later

than 60 days after you send the request (QCI-7.2-04); a vendor that has not answered by then goes on the exception register.

3.4 What gate G70 means for a practice

Under QCI-QS1 v2.3, an organization cannot score above 70 until every critical supplier has provided a current, adequate response and an officer-signed attestation (gate G70, QCI-6.3-01). An approved exception, however well managed, does not lift the cap. For a practice on a single EHR whose vendor has not attested, the score stays at 70 no matter how complete the practice's own work is, and the vendor's name appears in every quarterly leadership briefing until it does.

That is the rule working as designed. A practice cannot fix its EHR vendor's cryptography, and the standard does not pretend it can; it moves the pressure to the vendor. For the practice, the practical consequences are three: send the request in writing with a deadline, put the non-response on the exception register with an expiry and review triggers (QCI-4.3-02), and raise the attestation at the next BAA renewal as a contractual term (QCI-7.1-02). A practice that has done all three and is held at 70 has a defensible position with OCR. A practice that reports 74 with an unattested EHR vendor has a finding.

4. ePHI horizons and HNDL exposure

4.1 Medical data retention obligations

Medical records carry some of the longest confidentiality obligations of any data type in any industry. QCI-QS1 v2.3 records that obligation as a confidentiality horizon: a date, or a duration with a start date (QCI-5.2-01). Retention requirements vary by state and data type, but the following represent common minimum standards that practices should apply when setting horizons and assessing HNDL exposure:

ePHI data type	Typical retention minimum	HNDL risk level	Notes
Adult patient medical records	10 years from last treatment (many states longer)	High	Some states require lifetime retention for specific record types
Minor patient records	Until age of majority plus 3 to 10 years depending on state	High	Records created today for a minor patient may carry a 25-year confidentiality obligation
Mental health and behavioral health records	Varies; often longer than standard medical records	High	Many states apply stricter protections; some require perpetual confidentiality for psychiatric records
Genetic and genomic data	Indefinite in many contexts	Very High	Genetic data is inherently permanent and identifies not just the patient but their family members
Billing and financial records	7 years minimum for Medicare/Medicaid	Medium	Financial records are sensitive but typically have clearer retention endpoints than clinical records
Imaging (radiology, pathology)	Often 10 years or more; varies by specialty and state	High	Large file sizes make imaging archives common harvest targets

ePHI data type	Typical retention minimum	HNDL risk level	Notes
Telehealth session data and transcripts	Same as underlying clinical records	High	Telehealth data often stored in third-party platforms with their own crypto posture

4.2 The delayed breach scenario in plain terms

Here is the scenario that every practice compliance officer needs to understand:

The delayed breach scenario

In 2025, a threat actor gains access to encrypted ePHI transmitted between your practice and your EHR vendor. The session keys were established with RSA-2048 or elliptic-curve key exchange — the standard method used by most healthcare software today. The threat actor cannot read the data in 2025, so they store it. In 2034, a sufficiently capable quantum computer becomes available. The threat actor uses it to recover the session keys and decrypt the stored data. They now have access to patient records from your 2025 transmission. Under HIPAA's breach notification rule, this decryption event may constitute a reportable breach — requiring notification to affected patients, HHS, and potentially media. The original encryption that was adequate in 2025 may not satisfy the safe harbor in 2034. Note what does not help: replacing the key protection in 2027 does not recover the 2025 copy. QCI-QS1 requires that a current rewrap is never reported as remediation of copies an adversary may already hold (QCI-4.6-03).

This is not a hypothetical designed to create alarm. It is the forward projection of documented adversary behavior combined with the stated trajectory of quantum computing development. The practices that document this risk in their HIPAA risk analysis, engage their EHR vendors, and begin migration planning are building a defensible compliance posture. The ones that do not are accumulating undocumented liability.

5. QASI record guidance for medical practices

The following guidance supplements the QASI record groups in QCI-5.2-01 with healthcare-specific context. A field may hold a known value, an explicit unknown with an investigation action, owner and due date, or a justified not-applicable value (QCI-5.1-02). For a practice that depends on a vendor for the answer, "unknown — asked vendor on [date], due [date]" is the honest entry, and it is better than a guess. A record whose algorithm, profile, or key-protection mechanism is unknown stays outside validated coverage until the vendor answers.

QASI field	Healthcare guidance
Business criticality	EHR system: always High. Patient portal: High. Billing and claims system: High. Telehealth platform: High. Internal staff scheduling (no ePHI): Low. When in doubt, any system touching ePHI is High (QCI-1.1-02).
Data classification	Any system touching patient data is Regulated. This includes billing systems (which contain diagnosis codes and treatment information), not just clinical record systems.

QASI field	Healthcare guidance
Confidentiality and verification horizons	Use the longest applicable retention period for the data types in the system as the confidentiality horizon. For adult records: 10 years minimum. For minor records: calculate from current patient ages. For genetic data: indefinite. Default to the longest when uncertain. Record a separate verification horizon for signed records such as consents and e-prescriptions.
Critical data flows	New in v2.3: flows are a separate coverage denominator (QCI-5.1-03). Inventory at minimum: practice-to-EHR-host sessions, claims submission to the clearinghouse, e-prescribing, HIE exchange, telehealth sessions, and lab and imaging interfaces, with protection and authentication at each hop.
Vendor dependencies	Name the EHR vendor, product, deployed release, and hosting model (cloud-hosted vs. on-premise). A cloud-hosted EHR means the vendor controls the crypto. An on-premise installation may give the practice more control but also more responsibility. This record drives the Annex C request and the G70 determination.
PQC support status	Most EHR platforms will be at None or early Roadmap as of late 2026. Distinguish what the vendor supports, what is configured, and what is observed (QCI-4.5-01). Do not accept verbal assurances — require written documentation and the attestation before upgrading this field.
Exposure flags	Raise the long-lived-confidentiality flag (QCI-5.3-01) for any system holding ePHI with retention exceeding five years under vulnerable protection. This includes most clinical record systems. Treatment status is recorded separately (QCI-5.3-02); a vendor roadmap is a plan, and a plan does not clear the flag.
Compensating controls	HIPAA-compliant encryption at rest is a baseline, not a compensating control — it is already required. Compensating controls include data minimization (retaining only what is legally required), segmentation (isolating long-lived records), and enhanced access logging. None is assumed to remove HNDL risk without analysis of the protected path.
Evidence link	For a medical practice, evidence is often vendor documentation, an email exchange with the EHR vendor's support team, or a section of the BAA. These are valid evidence artifacts when they are retained with producer, date and reviewer (QCI-4.8-01). A screenshot of a document is weaker than the document; keep the source.

6. Governance model for mid-sized practices

QCI-QS1's governance model is designed for enterprises with dedicated security teams. QCI-4.1-01 allows roles to be combined where conflicts are managed. The following adaptation makes it workable for a medical practice where the HIPAA Security Officer may also handle compliance, contracts, and staff training.

QCI-QS1 required role	Typical practice mapping	Minimum commitment
Executive Sponsor	Practice Administrator, COO, or Managing Partner	Quarterly: review Q-Risk Score and vendor status; approve the assessment boundary; sign off on the risk register update

QCI-QS1 required role	Typical practice mapping	Minimum commitment
Quantum Risk Owner	HIPAA Security Officer or IT Director — whoever owns the security risk analysis	Monthly: QASI updates, vendor follow-up, exposure flag review; quarterly obligations register check
Steering function (risk committee)	Existing compliance committee or practice leadership team; add quantum risk as a quarterly agenda item	Quarterly: 20-minute review of Q-Risk Score and open exceptions
Governing body	Practice board, partners meeting, or governing body — whoever approves the compliance program	Quarterly: receive the one-page insert (Annex D) as part of the compliance report; approve any accepted risk explicitly (QCI-8.2-01)
Vendor risk	Practice Administrator or Compliance Officer for BAA management	As needed: issue Annex C requests, track the 60-day deadline, update the exception register

6.1 Integrating quantum readiness into the HIPAA compliance program

For most practices, the least disruptive path is to integrate quantum readiness into the existing HIPAA Security Rule compliance program rather than building a separate program. QCI-QS1 allows its records to live in existing management systems where content and traceability are preserved (QCI-4.2-01). Specific integration points:

- Risk analysis (45 CFR 164.308(a)(1)): Add a quantum computing threat assessment section to the annual risk analysis. Document the threat, the current cryptographic posture, the vendor dependencies, and the planned response. This satisfies the Security Rule's risk analysis requirement and creates the documentation foundation for a QCI-QS1 QASI.
- Risk management plan (45 CFR 164.308(a)(1)(ii)(B)): Add quantum readiness milestones to the risk management plan. Even early-stage milestones (complete vendor inventory, issue EHR vendor request, produce first Q-Risk Score) demonstrate active management.
- Evaluation (45 CFR 164.308(a)(8)): The periodic evaluation requirement is a natural home for the quarterly Q-Risk Score snapshot. Produce the score, record its assessment type, document movement, and include it in the evaluation record.
- BAA review: Add a quantum readiness attestation request to the next BAA renewal cycle for all EHR and clinical software vendors. This does not require renegotiating existing agreements immediately — it builds the requirement into the next natural renewal window, which is where QCI-7.1-02 expects it.

7. Q-Risk Score guidance for medical practices

7.1 Realistic band targets

QCI-QS1 defines score bands from Exposed (0 to 19) through Defensible readiness (81 to 100). A score of exactly 80 is Advancing, and no score above 80 is possible unless gates G60, G70 and G80 have all passed (QCI-6.3-01, QCI-6.5-01). The targets below are planning guidance for this sector, not Core-profile thresholds (QCI-6.3-02). None reaches 70, and none could while the EHR vendor is unattested.

Practice profile	Typical starting score	Realistic 12-month target	Primary constraint
10 to 30 physician practice, single EHR, IT support contract	5 to 15 (Exposed)	22 to 35 (Behind)	Limited dedicated security resources; EHR vendor dependency
30 to 100 physician practice, multiple sites, dedicated IT	10 to 22 (Exposed to Behind)	30 to 48 (Behind to Mobilizing)	Multi-vendor complexity; HIPAA compliance integration workload
Specialty group or ambulatory surgery center with external IT support	8 to 18 (Exposed)	25 to 40 (Behind to Mobilizing)	Specialty software vendors with limited PQC roadmaps; high ePHI horizons
Multi-specialty group, 100 plus physicians, in-house IT and compliance	15 to 30 (Exposed to Behind)	40 to 58 (Mobilizing)	EHR vendor roadmap; complex vendor estate; staff bandwidth

A score in the Behind band (20 to 39) after 12 months of active program work represents meaningful progress for most mid-sized practices. The score is not the goal — the documentation, the vendor engagement, and the governance habit are the goal. The score measures whether those are real. Report it as a self-assessment (QCI-1.2-03) and report conformance status beside it, not inside it (QCI-1.2-04).

8. Healthcare practice 90-day quick start

This sequence adapts the Practitioner Handbook’s establishment sequence and QCI-QS1 Clause 9.1 for a practice. It is a planning aid, not a conformance grace period.

Timeframe	Phase	What to accomplish	Output
Week 1	Assign and bound	Name the HIPAA Security Officer (or equivalent) as Quantum Risk Owner. Name the Practice Administrator as Executive Sponsor. Declare the assessment boundary: the ePHI systems and flows (QCI-1.1-01). Brief practice leadership in one meeting using section 2. Start the obligations register from section 2.4.	Named roles. Boundary approved. Quantum risk added to the compliance agenda. Briefing recorded.
Week 2	Legal question	Consult HIPAA legal counsel on the delayed breach scenario (section 4.2). Document the question and the response. This step is unique to this sector and should not be skipped.	Written legal opinion or documented consultation on HIPAA breach notification and the HNDL scenario.
Week 3	Vendor request	Contact your EHR vendor using the plain-language questions in section 3.3, in writing, with the Annex C attestation form attached and a 60-day deadline. Log the date, the recipient, and the method. Non-responses are a finding.	Vendor request issued and logged. Calendar reminder set for the deadline.
Weeks 4 to 6	Inventory	Build linked QASI records for your three highest-priority systems: EHR platform, patient portal, and billing/claims system, and the flows between them and to the clearinghouse. Use the field guidance in section 5. Record unknowns explicitly.	Three system records and their flows completed. Horizons set. Exposure flags identified.

Timeframe	Phase	What to accomplish	Output
Weeks 7 to 9	Expand	Extend the QASI to remaining clinical systems and flows toward the 95 percent threshold. Include the telehealth platform, any imaging systems, e-prescribing, HIE exchange, and document management. Identify top HNDL exposures.	QASI for all ePHI-touching systems and flows; coverage computed per QCI-5.1-03. Top exposures documented with owners and treatment status.
Week 10	Score	Produce the first Q-Risk Score using the Annex B worksheet and the QCI-6.1-02 formula. Record the assessment type as self-assessment. Use the realistic band targets from section 7 as planning context.	Q-Risk Score snapshot with gate results. Score included in the HIPAA risk analysis documentation.
Weeks 11 to 12	Report and integrate	Add the quantum risk section to the HIPAA risk analysis (section 9). Deliver the one-page insert to practice leadership (QCI-8.1-01). Place a non-responding vendor on the exception register. Add quantum readiness to the BAA renewal checklist.	HIPAA risk analysis updated. Leadership briefed. Exception register active. BAA checklist updated.

9. Integrating quantum risk into the HIPAA risk analysis

The following template language can be adapted and inserted into the practice's annual HIPAA Security Rule risk analysis. This creates the documentation foundation required to demonstrate compliance and to support any future OCR inquiry.

Template language: quantum computing threat assessment section

Identified threat: Quantum computing advances. Description: Adversaries may harvest encrypted ePHI today for decryption using quantum computing capabilities that are projected to emerge within 10 to 15 years. This threat is particularly relevant for ePHI with retention obligations extending beyond 5 years, including clinical records, minor patient records, and genetic data. Current safeguard assessment: ePHI is currently protected using [describe protection — e.g., TLS 1.3 in transit with classical key exchange; AES-256 at rest with data keys protected by [RSA / vendor-managed KMS]]. These safeguards are adequate for current threat capabilities but the key establishment and key protection may not provide adequate protection against quantum-enabled decryption over the full data retention period. Vulnerability: Current EHR platform [vendor name, release] has [describe roadmap status — e.g., no published PQC roadmap as of [date] / a published roadmap targeting an approved post-quantum key-establishment profile by [date]] and [has / has not] provided an officer-signed attestation. Risk level: [High/Medium] — confidentiality horizon [X years] combined with [current/absent] vendor roadmap. Risk management action: [Describe planned action — e.g., issued vendor request on [date] with a 60-day deadline; awaiting response / vendor on exception register with review date [date] / monitoring vendor PQC roadmap quarterly / piloting a post-quantum capable certificate configuration on the patient portal]. Assessment basis: QCI-QS1 v2.3 self-assessment dated [date]; Q-Risk Score [N], conformance status [conforming / nonconforming: identifiers].

10. Summary and engagement

The quantum computing threat to medical practice data is not theoretical and it is not distant. It is a documented adversary pattern applied to a timeline measured in years, not decades. The practices that act now are not over-preparing. They are building the compliance documentation,

vendor relationships, and governance habits that will define the standard when HHS and OCR guidance catches up to the technology.

Three actions matter most for mid-sized practices in the near term. First: put the delayed breach scenario to your HIPAA counsel in writing and document the response. Second: contact your EHR vendor and ask about their post-quantum cryptography roadmap in writing, with a deadline and the attestation form. Third: add quantum computing as an identified threat in your next annual HIPAA risk analysis. These three steps alone move a practice from undocumented exposure to a documented, managed position — and that distinction matters enormously in an OCR investigation.

QCI engagement support for healthcare practices

QCI works with medical practices and HIPAA-covered entities to deliver assessments calibrated to the healthcare context, facilitate EHR vendor engagement, integrate quantum readiness into existing HIPAA compliance programs, and produce OCR-defensible documentation. Independent assessment under QCI-1.2-03 is available separately. Engagements are scoped to practice size and complexity. Contact QCI to discuss how assessment support is structured for practices like yours.

Revision history

Version	Date	Changes
1.2	September 23, 2026	Aligned to QCI-QS1 v2.3: references by requirement identifier; band targets restated for the 81-point Defensible readiness threshold; gate G70 no longer satisfied by exceptions (new section 3.4); G60 fixed at 95 percent for systems and flows, with critical-flow guidance; obligations register section 2.4 added; horizons replace data longevity; supplier deadline, attestation and BAA renewal rules; key-protection wording corrected; historical-copy caveat added to the delayed breach scenario; risk analysis template gains the assessment basis line; references to the retired QCI-QS1-A worksheet replaced with Annex B.
1.1	June 10, 2026	Aligned to QCI-QS1 v2.2; AI-cryptographic provisions note added.

Independent assessment against QCI-QS1 is performed by the Quantum Core Institute. Scope one at quantumcoreinstitute.com/independent-assessment. An independent assessment is not QCI certification (QCI-1.2-03).