SAMPLE REPORT · ILLUSTRATIVE ENGAGEMENT

QUANTUM-READINESS ASSESSMENT

Know exactly where your cryptography stands. With evidence.

Prepared for Riverbend Regional Health, a fictional three-hospital system created to show the shape, depth, and evidence style of the real deliverable.

EXECUTIVE SUMMARY

Readiness grade C-: inventoried late, exposed on three deadlines, fixable in sequence

C-

Riverbend can name most of its cryptography for the first time as of this assessment. 1,284 cryptographic assets were discovered and catalogued; 31 percent depend on algorithms with announced federal retirement dates, and the system had no named owner for any of the three compliance clocks now running.

1,284	31%	9	14
CRYPTO ASSETS INVENTORIED	ON DEPRECATION-DATED ALGORITHMS	FINDINGS, 2 CRITICAL	ROADMAP ACTIONS, SEQUENCED

What the two weeks produced

A complete, machine-readable cryptographic inventory (CycloneDX CBOM) of the hospital's external surface, internal PKI, integration engine, and top twelve vendor connections; nine findings mapped against PCI DSS 4.0 requirement 12.3.3, the federal post-quantum directive, and the NIST IR 8547 retirement timeline; and a fourteen-action migration roadmap ordered by deadline exposure and effort. Every finding in this report carries an evidence reference: the artifact that proves it, hashed and reproducible, so an auditor, a board, or a cyber insurer can verify the claim without taking anyone's word.

The three clocks

PCI DSS 4.0 requirement 12.3.3 already requires a documented cryptographic inventory and agility plan for the card-handling environment. NIST IR 8547 sets the retirement path for classical public-key cryptography: deprecated after 2030, disallowed after 2035. And federal guidance now directs agencies and their suppliers toward post-quantum migration on that same horizon. Riverbend's patient portal, imaging fleet, and HL7 interconnects all sit on the wrong side of at least one of these dates today.

The deliverable in one sentence: an inventory a reviewer can load, findings a reviewer can reproduce, and a roadmap a board can fund, in two weeks, at a fixed fee.

SCOPE AND METHOD

What we inspected, and why findings here are evidence, not opinion

Scope (fixed)

SURFACE	WHAT WAS INSPECTED	METHOD
External perimeter	46 public endpoints: portal, telehealth, MyChart proxy, VPN, mail, DNS	TLS handshake capture, certificate chain analysis, cipher and key-exchange enumeration
Internal PKI	Enterprise CA hierarchy, 2 issuing CAs, 1,100+ leaf certificates	CA database export, template review, algorithm and lifetime analysis
Integration engine	HL7 and FHIR interfaces, 83 active routes	Configuration review, transport inspection per route
Application estate	Build manifests for 7 in-house apps, container base images	CycloneDX CBOM generation from code and dependencies
Vendor connections	Top 12 data-sharing vendors incl. 2 AI diagnostic tools	Connection-level crypto posture, questionnaire-free

Method: evidence first

Every claim in this report resolves to an artifact: a packet capture, a certificate, a configuration excerpt, or a CBOM entry, each content-hashed at collection time and listed in the evidence appendix. Findings are written so that Riverbend's own team, an external auditor, or a cyber insurer can re-run the check and get the same answer. Nothing in the gap analysis relies on interviews or self-attestation.

Out of scope

Penetration testing, application-layer vulnerability assessment, and policy authorship. This engagement answers one question with precision: where does your cryptography stand against the clocks that are already running, and what do you migrate first.

CRYPTOGRAPHIC INVENTORY

1,284 assets, named and machine-readable

46	1,121	83	34
EXTERNAL ENDPOINTS	PKI CERTIFICATES	INTEGRATION ROUTES	APP / IMAGE MANIFESTS

ALGORITHM FAMILY	WHERE IT LIVES	COUNT	IR 8547 STATUS
RSA-2048	Patient portal, PKI leaves, vendor VPNs	612	Deprecated after 2030, disallowed 2035
ECDSA P-256	External TLS, newer PKI templates	403	Deprecated after 2030, disallowed 2035
AES-128 / AES-256	Storage, VPN transforms, backups	188	Symmetric, retained; 128-bit flagged for upgrade path
SHA-1 (signatures)	Legacy internal CA, imaging consoles	57	Already past retirement; finding F-01
TLS 1.0 / 1.1 endpoints	Imaging fleet, one lab analyzer	19	Already past retirement; finding F-03
Hybrid PQ (X25519MLKEM768)	None found	0	Target state for external surface

Delivered as CycloneDX CBOM

The inventory ships as a CycloneDX 1.6 cryptographic bill of materials, the format auditors and tooling can consume directly. Excerpt:

```
{
  "bomFormat": "CycloneDX", "specVersion": "1.6",
  "components": [{
    "type": "cryptographic-asset",
    "name": "portal.riverbendhealth.example TLS server certificate",
    "cryptoProperties": {
      "assetType": "certificate",
      "certificateProperties": {
        "subjectPublicKeyRef": "RSA-2048", "signatureAlgorithmRef": "SHA256withRSA",
        "notValidAfter": "2027-03-14T00:00:00Z" },
      "oid": "1.2.840.113549.1.1.11" },
    "evidence": { "hash": "sha256:9f31c7…e2ab", "collectedAt": "2026-11-03T15:22:08Z" }
  }]
}
```

FINDINGS AND GAP ANALYSIS · 1 OF 2

Nine findings, each with an evidence reference

ID	SEVERITY	FINDING	MAPS TO
F-01	CRITICAL	Legacy issuing CA still signs with SHA-1; 57 live leaf certificates, including both imaging console fleets. Evidence E-07, E-08.	IR 8547 (past due); PCI 12.3.3
F-02	CRITICAL	Integration engine sends 11 of 83 HL7 routes in cleartext across a flat clinical VLAN, including ADT feeds carrying PHI. Evidence E-11.	HIPAA Security Rule; evidence gap
F-03	HIGH	19 endpoints negotiate TLS 1.0/1.1, imaging fleet and one lab analyzer; vendor firmware pins the stack. Evidence E-04.	IR 8547 (past due); PCI 12.3.3
F-04	HIGH	Patient portal terminates on RSA-2048 with no key-exchange agility; certificate and config allow no hybrid group. Harvest-now-decrypt-later exposure for PHI in transit. Evidence E-01, E-02.	IR 8547 2030/2035; federal PQ directive
F-05	HIGH	No cryptographic inventory existed before this engagement and no owner is named for requirement 12.3.3; the card-handling environment shares PKI with the clinical estate. Evidence E-14.	PCI DSS 4.0 12.3.3

Reading the table: every finding cites evidence by ID. Appendix A lists each artifact with its content hash and collection timestamp, so any reviewer can request the artifact and confirm the finding independently.

FINDINGS AND GAP ANALYSIS · 2 OF 2

The remaining four, including both AI vendors

ID	SEVERITY	FINDING	MAPS TO
F-06	MEDIUM	Two AI diagnostic vendors receive PHI over connections the hospital cannot characterize: one legacy cipher suite, neither vendor able to produce current security test evidence on request. Evidence E-16, E-17.	Vendor oversight; evidence gap
F-07	MEDIUM	Backup encryption keys unrotated for 41 months; rotation runbook exists but has never executed. Evidence E-19.	PCI 12.3.3 agility; ransomware posture
F-08	MEDIUM	Site-to-site VPN to the largest vendor still offers IKEv1 with 3DES in its transform set, unused but negotiable. Evidence E-20.	IR 8547; vendor oversight
F-09	LOW	Internal tooling pins an EOL TLS library (two CVEs patched upstream); no exploit path identified, upgrade is hygiene. Evidence E-22.	Supply chain hygiene

The deadline picture

Already due	2030	2035	Target
SHA-1, TLS 1.0/1.1, PCI crypto inventory	RSA / ECDSA deprecated (IR 8547)	Classical PKC disallowed	Hybrid PQ on external surface

A system Riverbend's size typically needs three budget cycles to complete the 2030 work. Starting in 2027 is comfortable; starting in 2029 is an emergency program. That arithmetic, not vendor pressure, is the reason this assessment exists.

MIGRATION ROADMAP

Fourteen actions in three horizons, ordered by deadline and effort

HORIZON	ACTION	CLOSES
0–90 days	Name the crypto owner; adopt the CBOM from this report as the living inventory with a quarterly refresh	F-05
0–90 days	Disable TLS 1.0/1.1 where firmware allows; isolate the pinned imaging VLAN behind a terminating proxy	F-03
0–90 days	Encrypt the 11 cleartext HL7 routes (engine supports TLS per route today; config, not capital)	F-02
0–90 days	Strike 3DES/IKEv1 from the vendor VPN transform set; one change window	F-08
90–365 days	Retire the SHA-1 issuing CA: stand up replacement, reissue 57 leaves, decommission	F-01
90–365 days	Execute backup key rotation and put it on a 12-month clock with evidence capture	F-07
90–365 days	Require current security test evidence from both AI vendors at renewal; make evidence a contract term	F-06
90–365 days	Upgrade EOL TLS library across internal tooling	F-09
1–3 years	Move the external surface to hybrid post-quantum key exchange (portal first: terminates HNDL exposure for PHI in transit)	F-04
1–3 years	Rebuild PKI templates for algorithm agility so the 2030 swap is a template change, not a re-architecture	F-01, F-04
1–3 years	Fold crypto posture into vendor onboarding; connection-level checks replace questionnaires	F-06, F-08

Three further actions (segmentation review, HSM consolidation, insurer evidence pack) appear in the full roadmap workbook delivered alongside this report.

APPENDIX A · EVIDENCE INDEX

Every finding resolves to an artifact a reviewer can demand

ID	ARTIFACT	CONTENT HASH (SHA-256)	COLLECTED
E-01	Portal TLS handshake capture, full negotiation	9f31c7…e2ab	2026-11-03
E-04	Imaging fleet cipher enumeration, 19 endpoints	41d8a0…77c4	2026-11-04
E-07	Issuing CA certificate chain, SHA-1 signatures	b02e91…3f58	2026-11-04
E-11	Integration engine route table export, transport column	7cc3d2…91ae	2026-11-05
E-16	AI vendor connection capture, cipher suite offer	e85f44…0c12	2026-11-06
E-19	Backup KMS key metadata, creation and rotation dates	d1907b…5aa9	2026-11-06

The full index (23 artifacts) ships with the report. Artifacts are hashed at collection and stored in Riverbend's own evidence vault; Scrutari retains hashes, not PHI. A reviewer who doubts any finding requests the artifact, recomputes the hash, and reproduces the check. That is what evidence-first means, and it is the same discipline our gateway applies to every AI call it carries.

NEXT STEPS

From sample to your own numbers

The real engagement runs two weeks, fixed fee from $9,500, remote, and begins with a free CBOM scan of your external surface so you see the method on your own estate before spending anything. partnerships@scrutari.ai, or scrutari.ai/assessments.

Scrutari is the evidence layer for AI in regulated industries: a gateway that strips sensitive data at the boundary, signs every decision, and produces records anyone can verify independently, running on post-quantum rails.