EXECUTIVE SUMMARY

HIPAA Security Risk Assessment

Sample deliverable, redacted. Representative composite for illustration.

CLIENT

Specialty healthcare practice

Western Massachusetts

PROFILE

2 locations · ~25 workforce members

Cloud EHR, PM, imaging, email

REQUIREMENT

45 CFR § 164.308(a)(1)(ii)(A)

Security Management Process

METHOD & WINDOW

OCR SRA guidance · NIST SP 800-30

3 weeks, remote and on-site

OVERALL POSTURE

Two of the seventeen risks identified were rated critical, and both were actively exposing the practice to a reportable breach of electronic protected health information. In an Office for Civil Rights (OCR) investigation, the first document requested is the practice's risk analysis, and the cost of not having one is rarely the fine. It is the breach notification to patients and the media, and the corrective action plan that OCR monitors for years afterward. Both critical findings were resolved during this engagement through configuration changes, with no capital expenditure.

Outside those two items, the practice operates from a materially strong compliance foundation. Clinical and administrative discipline is evident in daily operations, and the systems handling ePHI, the EHR, practice management, imaging, and email, are run with care. The gaps identified are the avoidable kind that accumulate without a formal security program, not signs of a practice in trouble.

None of the findings require new spending to resolve. The majority are fixed through settings and process discipline, sequenced into a roadmap the practice can execute in a single quarter. On completion of the 30/60/90 day plan, the practice would hold a defensible risk analysis, the document OCR requests first in any audit or breach investigation, and a working security program it owns.

RISK DISTRIBUTION

Seventeen risks rated on likelihood and impact to the confidentiality, integrity, and availability of ePHI.

2	4	5	6
CRITICAL	HIGH	MEDIUM	LOW
Both resolved in engagement	Roadmap, days 1–60	Roadmap, days 31–90	Tracked, annual cycle

PRIORITY FINDINGS

Top six of seventeen identified risks. The complete report provides the full risk register, asset and ePHI flow inventory, policy gap analysis, and evidence appendix.

FINDING	RISK	HIPAA REF.	RECOMMENDATION
1 **ePHI stored on unencrypted workstations and laptops**	CRITICAL	§ 164.312(a)(2)(iv)	Deploy full-disk encryption on all endpoints. Verify enrollment and recovery-key escrow through device management.
2 **Shared EHR login credentials among front-desk staff**	CRITICAL	§ 164.312(a)(2)(i), (d)	Issue unique user IDs for every workforce member. Enable MFA on EHR and email. Disable shared accounts.
3 **No BAA inventory; three vendors handle ePHI without executed agreements**	HIGH	§ 164.308(b)(1)	Build a vendor inventory and execute BAAs with all ePHI-handling vendors. Add a BAA check to vendor onboarding.
4 **Backups never tested; no documented recovery plan**	HIGH	§ 164.308(a)(7)	Implement immutable, offsite backups. Document and test a recovery plan with defined RTO and RPO. Test quarterly.
5 **No security awareness or phishing training program**	HIGH	§ 164.308(a)(5)	Launch quarterly awareness training and phishing simulation. Track completion as a compliance record.
6 **Terminated-user access not consistently revoked across systems**	MEDIUM	§ 164.308(a)(3)(ii)(C)	Adopt an offboarding checklist tied to HR events. Run quarterly access reviews across EHR, email, and imaging.

REMEDIATION ROADMAP

Sequenced for risk reduction per dollar and per staff-hour. No major capital spend required.

DAYS 1–30

Stop the bleeding

Full-disk encryption on all endpoints. Unique logins and MFA for EHR and email. Disable shared and dormant accounts. Designate Seqora as HIPAA Security Officer under a vCISO retainer, satisfying § 164.308(a)(2).

DAYS 31–60

Build the paper trail

Execute outstanding BAAs and complete the vendor inventory. Adopt the core policy set: acceptable use, access control, incident response, sanctions. Deliver the first all-staff security training.

DAYS 61–90

Prove resilience

Immutable offsite backups with a documented recovery test. Launch the phishing simulation program. Establish quarterly access reviews and an annual risk-analysis cadence.

ABOUT SEQORA SECURITY

Seqora Security provides fractional vCISO services and HIPAA Security Risk Assessments to healthcare practices in Western Massachusetts. Led by Anthony Polo: 9+ years securing banks, insurers, and manufacturers, M.S. Cybersecurity Management, CISM candidate. Seqora can serve as your practice's designated HIPAA Security Officer under an ongoing vCISO retainer. Engagements are sized to what a practice actually needs, starting with a risk assessment you can stand behind in an audit.
tony@seqorasecurity.com · seqora.app · Springfield, MA