CONFIDENTIAL — FOR INTERNAL COMPLIANCE RECORDS

HIPAA Security Risk Assessment

Prepared for: Riverside Pediatrics of Bergen County (fictional sample practice)

Prepared by: Practice All — Healthcare IT Services, Bergen County, NJ

Assessment period: August 4–8, 2026

Report date: August 11, 2026

Scope: 1 location · 3 providers · 8 staff · 11 workstations

Next review due: August 2027 (or upon material change)

1. Executive summary

Riverside Pediatrics operates a modern cloud EHR and a generally well-run office, but the assessment identified **2 critical, 2 high, 3 medium, and 1 low-severity findings** across the administrative, physical, and technical safeguards of the HIPAA Security Rule. The two critical findings — remote EHR access without multi-factor authentication and the absence of any ransomware-resilient backup — represented the most plausible paths to a reportable breach and were remediated during the engagement, together with the shared front-desk login.

With the included fixes applied, the practice's residual risk is concentrated in aging workstations and missing vendor agreements, both addressable within 30 days at modest cost. Completing the 30/60/90-day roadmap in Section 5 would place the practice in a defensible, attestation-ready posture ahead of the proposed Security Rule updates.

2	2	3	1
Critical	High	Medium	Low

This assessment follows the process described in NIST SP 800-30 and OCR's Guidance on Risk Analysis, mapping each observation to the implementation specifications of the HIPAA Security Rule (45 CFR Part 164, Subpart C). Evidence was gathered through a structured interview with the practice administrator, a guided questionnaire completed by the office manager, an authorized technical scan of the internal network and all workstations, a review of EHR user and audit-log configuration, and inspection of vendor contracts and policies provided by the practice.

Systems in scope: cloud EHR (vendor-hosted), practice management and billing workspace, local file server, 11 workstations and 2 laptops, network equipment, document scanner, one networked clinical device, e-fax, email, and the after-hours answering service. Out of scope: the EHR vendor's internal controls (covered by their BAA and SOC 2 report, which were verified as current).

3. Risk rating methodology

Each finding is rated by **likelihood** (the probability of the threat exploiting the vulnerability in the next 12 months, given current controls) and **impact** (effect on confidentiality, integrity, and availability of ePHI, plus operational and regulatory consequences). Severity is the product of the two:

Likelihood ↓ / Impact →	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High / Critical*
Low	Low	Low / Medium	Medium

*Elevated to Critical where the finding removes the practice's ability to recover (e.g., backup failures).

4. Findings (8)

ID	Finding	Severity	Status
F-01	Remote access to the EHR without multi-factor authentication	Critical	Remediated ✓

ID	Finding	Severity	Status
F-03	Windows 10 workstations past end of support	High	Open
F-04	Shared login used by front-desk staff	High	Remediated ✓
F-05	Business associate agreements missing for two vendors	Medium	Open
F-06	No documented security awareness training	Medium	Open
F-07	Guest Wi-Fi shares a network with clinical devices	Medium	Open
F-08	Contingency plan exists but has never been tested	Low	Open

F-01 Critical Likelihood: High · Impact: High

Remote access to the EHR without multi-factor authentication

HIPAA safeguard: §164.312(a)(2)(i) — Access Control: Unique User Identification; §164.312(d) — Person or Entity Authentication

Observation

Providers and the billing team access the cloud EHR from home using username and password only. MFA is available from the vendor but has never been enabled. Two staff passwords were found in a public credential-breach database.

Risk

A single reused or phished password gives an attacker full access to every patient chart. Credential attacks are the leading cause of reported healthcare breaches.

Recommendation

Enable vendor MFA for all user accounts (app-based, not SMS, for providers). Enforce a password manager for staff. Review EHR access logs for unfamiliar sign-in locations over the past 90 days.

Status

REMEDIATED during assessment (included fix 1 of 3)

Observation

The practice management database and shared documents are backed up nightly to a USB drive that remains permanently connected to the server. No backup has been test-restored in the last 12 months. The EHR vendor's backup covers only the hosted chart data.

Risk

Ransomware routinely encrypts connected backup drives along with the systems they protect. In that scenario the practice would lose scheduling, billing workspace, scanned documents, and HR records with no recovery path.

Recommendation

Implement a 3-2-1 backup: local copy, encrypted cloud copy with immutability/versioning, and a quarterly test restore with a written result. Document recovery time objectives in the contingency plan.

Status

REMEDIATED during assessment (included fix 2 of 3)

F-03 High Likelihood: High · Impact: Medium

Windows 10 workstations past end of support

HIPAA safeguard: §164.308(a)(1)(ii)(B) — Risk Management; §164.312(c)(1) — Integrity

Observation

Six of eleven workstations run Windows 10, which stopped receiving security updates in October 2025. Two of them are used at the front desk to access the EHR and scan patient documents.

Risk

Unpatched operating systems accumulate publicly known vulnerabilities that commodity malware exploits automatically — no targeted attack required.

Recommendation

Replace or upgrade all six devices within 60 days (four support Windows 11; two require replacement). Until then, restrict those machines from email and web browsing.

Status

Open — scheduled in roadmap (30-day items)

F–04 High Likelihood: Medium · Impact: Medium

Shared login used by front-desk staff

HIPAA safeguard: §164.312(a)(2)(i) — Unique User Identification; §164.308(a)(5)(ii)(C) — Log-in Monitoring

Observation

Three front-desk employees share a single "FrontDesk" Windows and EHR account. Individual activity cannot be attributed to a specific person.

Risk

Without unique identification, the practice cannot investigate suspicious chart access, satisfy an OCR audit request, or cleanly terminate access when an employee leaves.

Recommendation

Create individual accounts for each employee, remove the shared account, and enable automatic logoff on front-desk machines (§164.312(a)(2)(iii)).

Status

REMEDIATED during assessment (included fix 3 of 3)

F–05 Medium Likelihood: Low · Impact: High

Business associate agreements missing for two vendors

HIPAA safeguard: §164.308(b)(1) — Business Associate Contracts; §164.314(a) — Organizational Requirements

Observation

The practice could not produce BAAs for its e-fax provider or its after-hours answering service, both of which handle PHI. BAAs are in place for the EHR, clearinghouse, and email provider.

Risk

Sharing PHI with a vendor without a BAA is itself a HIPAA violation, independent of any breach, and has been the basis of OCR enforcement actions against small practices.

Recommendation

Execute BAAs with both vendors within 30 days or migrate to equivalents that will sign one. Add a BAA checklist step to the new-vendor process.

Status

F–06 **Medium** Likelihood: Medium · Impact: Medium

No documented security awareness training

HIPAA safeguard: §164.308(a)(5)(i) — Security Awareness and Training

Observation

Staff receive informal guidance at hire but no recurring security training, and no training records are kept. Two of five staff clicked a simulated phishing link during the assessment.

Risk

Phishing remains the most common initial access vector in healthcare incidents. Undocumented training also weakens the practice's defensibility in an audit.

Recommendation

Adopt brief quarterly training with phishing simulation and automatic record-keeping. Include it in onboarding for new hires.

Status

Open — scheduled in roadmap (60-day items)

F–07 **Medium** Likelihood: Low · Impact: Medium

Guest Wi-Fi shares a network with clinical devices

HIPAA safeguard: §164.312(e)(1) — Transmission Security

Observation

The waiting-room guest Wi-Fi is served from the same flat network as workstations, the document scanner, and a networked spirometer. Patient devices can see clinical devices on the LAN.

Risk

Any compromised or malicious patient device gains a network path to clinical systems, bypassing the firewall entirely.

Recommendation

Segment guest traffic onto an isolated VLAN with client isolation. Inventory all networked clinical devices while segmenting (supports the proposed Security Rule asset-inventory requirement).

F–08 Low Likelihood: Low · Impact: Medium

Contingency plan exists but has never been tested

HIPAA safeguard: §164.308(a)(7)(ii)(D) — Testing and Revision Procedures

Observation

A written contingency plan from 2022 names a former employee as the emergency contact and references a server that has since been retired. It has never been exercised.

Risk

In a real outage the plan would misdirect staff during the hours that matter most, extending downtime and potentially patient-care disruption.

Recommendation

Update roles and systems, then run a 60-minute tabletop exercise annually. Keep a printed copy accessible without network access.

Status

Open — scheduled in roadmap (90-day items)

5. Remediation roadmap

Within 30 days

- Replace/upgrade the six end-of-support workstations (F-03)
- Execute BAAs with e-fax and answering-service vendors (F-05)
- Enable automatic screen lock (10 min) on all workstations
- Review EHR audit logs for the past 90 days of remote sign-ins

Within 60 days

- Launch quarterly security awareness training with phishing simulation (F-06)
- Segment guest Wi-Fi onto an isolated VLAN; inventory clinical devices (F-07)
- Enable full-disk encryption on the two laptops used for home charting

Within 90 days

- Update and tabletop-test the contingency plan (F-08)
- Adopt a sanction policy and access-review calendar (annual)
- Schedule the next risk assessment review (12 months)

6. Attestation record

This document records that Riverside Pediatrics of Bergen County conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the practice, as required by 45 CFR §164.308(a)(1)(ii)(A), for the period noted on the cover. Findings and remediation status are documented herein; the remediation roadmap constitutes the practice's risk management plan under §164.308(a)(1)(ii)(B).

Practice representative — signature / date

Assessor, Practice All — signature / date