Sample Family Medicine, P.A.

Annual HIPAA Security Risk Analysis

SAMPLE REPORT (fictitious practice) · Performance year 2026 · Scope period Nov 2025 – Nov 2026

Prepared for	Prepared by	Report date	Version
Sample Family Medicine, P.A.	Independent Assessor	November 3, 2026	1.0

This report documents the security risk analysis and risk management activities Sample Family Medicine, P.A. completed for 2026.

Certification notice: This report does not certify HIPAA compliance. HHS does not issue or recognize HIPAA compliance certifications; this report records Sample Family Medicine, P.A.'s own assessment of risks to electronic protected health information (ePHI) and the actions taken to address them.

1. Executive Summary

This report records the practice's self-reported answers to a 73-question guided assessment; no safeguard is rated Met until evidence is reviewed. The analysis identified 16 scored risks under the current Security Rule (15 high, 1 medium, 0 low) drawn from 48 findings, plus 18 readiness items under HHS's proposed Security Rule update. No risks have been remediated or formally accepted yet.

Risk level	Identified	Remediated this year	Open (on POA&M)	Formally accepted
High	15	0	15	0
Medium	1	0	1	0
Low	0	0	0	0
Total	16	0	16	0

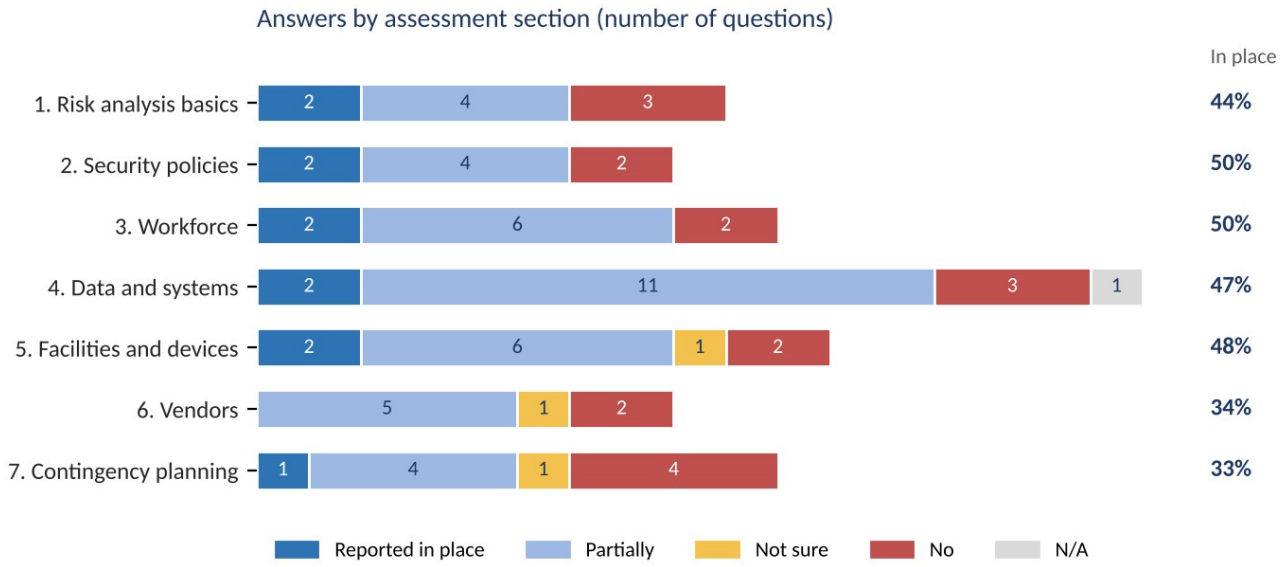
Figure 1. Risk heat map: each scored risk placed by likelihood and impact (16 risks).

Impact ↓ / Likelihood →	Unlikely (1)	Possible (2)	Probable (3)
Severe (3)	–	**3** R-002, R-004, R-009	**9** R-001, R-003, R-005, R-007, R-008, R-015, R-017, R-020, R-022
Significant (2)	–	**1** R-014	**3** R-006, R-018, R-021
Minimal (1)	–	–	–

Red cells are High (score 6–9), amber Medium (3–4), green Low (1–2), per Doc 02. Likelihood follows the assessment tool's suggestion from the practice's answers; no overrides were entered.

Safeguard area	Met	Partial	Not met
Administrative (§ 164.308)	0 (8 reported, evidence pending)	21	16
Physical (§ 164.310)	0 (2 reported, evidence pending)	8	3
Technical (§ 164.312)	0 (1 reported, evidence pending)	11	2

Figure 2. Assessment results by section.



Percentages are the tool's "safeguards in place" score: Yes counts fully, Partially counts half, Not sure counts one quarter. All answers are self-reported.

Top priorities for the coming year

- R-009 — Disable the two former employees' Microsoft 365 accounts now; start quarterly access reviews. Owner: Managed IT provider / Practice Manager. Target: 2026-12-03.
- R-005 — Execute BAAs with the answering service and the shredding vendor; add incident reporting terms to existing BAAs. Owner: Practice Manager. Target: 2026-12-03.
- R-003 / R-008 — Deploy monitored EDR; enable DKIM and move DMARC to quarantine/reject. Owner: Managed IT provider. Target: 2026-12-03.
- R-017 — Require certificates of destruction and confirmed wiping for all retired and re-used devices. Owner: Managed IT provider. Target: 2026-12-03.
- R-015 / R-007 — Write the contingency/DR plan with a criticality analysis and complete a first test restore. Owner: Practice Manager / Managed IT provider. Target: 2026-12-03.

Improvements since last year

- Business associate inventory compiled during this assessment (6.1). No other improvements documented.

2. Scope & Methodology

2.1 Scope

This analysis covers all systems, locations, workforce members, and business associates that create, receive, maintain, or transmit ePHI for Sample Family Medicine, P.A. during the period Nov 2025 through Nov 2026. Locations in scope: 2 (main clinic and satellite clinic). Workforce size: 18 (3 physicians, 2 NPs, 6 MAs, 4 front desk/billing, 1 office manager, 2 part-time).

2.2 Methodology

The analysis followed NIST SP 800-30 Rev. 1 and the organization's Risk Analysis & Risk Management Plan (Doc 02). For each ePHI system, reasonably anticipated threats and vulnerabilities were identified and scored for likelihood (1–3) and impact (1–3) with current controls in place. Scores of 1–2 are Low, 3–4 Medium, and 6–9 High.

In this report, findings are based on the practice's self-reported answers to the guided HIPAA Security Risk Assessment (73 questions aligned to the HHS SRA Tool sections), completed November 3, 2026. Likelihood was suggested from those answers and impact from typical healthcare consequences; no overrides were entered. Evidence review, walkthrough confirmation and technical validation are pending. A safeguard is rated Met only when supporting evidence has been reviewed; "Yes" answers are recorded as reported in place, evidence pending, and "Not sure" answers are treated as gaps.

2.3 Participants

Name	Role / title	Sessions
Practice Manager	Practice Manager / HIPAA Security Official	Pending
Office Manager	Office Manager	Pending
Independent Assessor	Assessor	Pending

2.4 Key Dates

Kickoff	Analysis completed	Read-out
Pending	November 3, 2026	Pending

3. Environment Changes Since Last Year

- Satellite clinic opened in 2024; it was not covered by the 2023 SRA and is fully in scope here.
- Microsoft 365 and mobile devices, not covered by the 2023 SRA, are now in scope.
- After-hours answering service handles ePHI; its BAA is in progress.
- Two former employees were found with active Microsoft 365 accounts during this assessment (R-009).
- New or upgraded ePHI systems, security incidents, lost devices and AI tool use since last year: none reported.

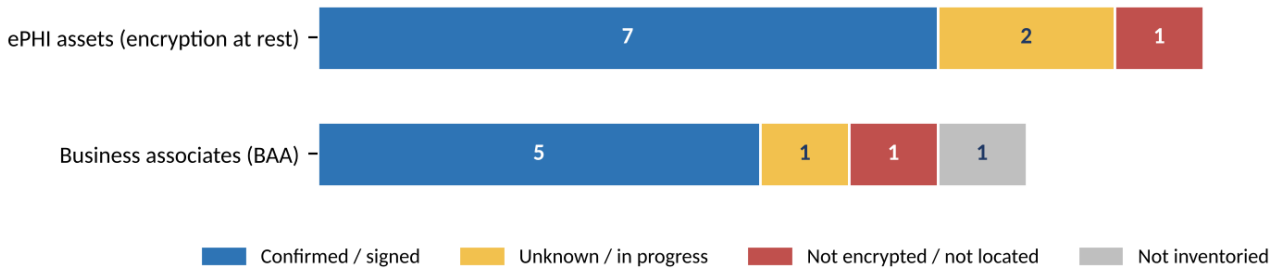
4. ePHI Inventory & Data Flow

System / location	Category	ePHI use	Hosting	BAA on file	Owner
Cloud EHR / practice management	Application / EHR	Holds ePHI; encryption: Yes	Vendor-hosted cloud	Yes (EHR vendor, 2025-03-15)	Pending

System / location	Category	ePHI use	Hosting	BAA on file	Owner
Microsoft 365 (Exchange Online, OneDrive, Teams)	Cloud service	Holds ePHI; encryption: Yes	Cloud	Yes (Microsoft, 2024-01-10)	Pending
Front desk workstations (4)	Workstation	Holds ePHI; encryption: Yes	Main clinic	N/A (practice-owned)	Pending
Front desk workstations (2)	Workstation	Holds ePHI; encryption: Unknown	Satellite clinic	N/A (practice-owned)	Pending
Exam room workstations (8)	Workstation	Holds ePHI; encryption: Yes	Both clinics	N/A (practice-owned)	Pending
Physician / NP laptops (5)	Laptop	Holds ePHI; encryption: Yes	Mobile / home	N/A (practice-owned)	Pending
Practice-issued iPhones (3) for on-call	Mobile device	Holds ePHI; encryption: Yes	Mobile	N/A (practice-owned)	Pending
Multifunction printer / scanner / fax	Printer / copier	Holds ePHI; encryption: No	Main clinic	N/A (practice-owned)	Pending
ECG machine (network-connected)	Medical device	Holds ePHI; encryption: Unknown	Main clinic	N/A (practice-owned)	Pending
Cloud backup of local scanned documents	Cloud service	Holds ePHI; encryption: Yes	Cloud	Yes (backup vendor, 2025-02-01)	Pending
Managed IT provider	Business associate	Access to PHI/ePHI (Managed IT support, remote access)	Vendor	Yes (2025-06-01)	Pending
Billing company	Business associate	Access to PHI/ePHI (Outsourced medical billing and claims)	Vendor	Yes (2024-09-20)	Pending
Answering service	Business associate	Access to PHI/ePHI (After-hours answering service)	Vendor	In progress	Pending
Shredding vendor	Business associate	Access to PHI/ePHI (On-site paper shredding)	Vendor	Unknown	Pending
Claims clearinghouse (not in vendor list)	Business associate	Claims transmission (4.9, 4.17)	Vendor	Pending	Pending

No network or ePHI data-flow diagram exists (item 1.7, proposed-rule readiness). Doc 08 System Security Plan, §2, should be completed with one. Firewall and Wi-Fi equipment at both sites hold no ePHI and are omitted from the table.

Figure 3. Encryption and BAA status across the inventory.



Counts are ePHI-holding assets and business associates with access to PHI, as reported. Unencrypted or unconfirmed assets are proposed-rule readiness items; vendors without a signed BAA fall under R-005. The claims clearinghouse referenced in question 4.17 does not appear in the vendor list.

5. Safeguard Findings

ID	Question area	Finding	Status	Risk ID
1.1	Risk analysis basics	Last SRA was performed in 2023 by the prior IT vendor; not repeated since. This assessment is the refresh.	Partial	R-020
1.2	Risk analysis basics	2023 SRA covered the EHR and main clinic only; satellite clinic (opened 2024), M365 and mobile devices were not in scope.	Partial	R-020
1.5	Risk analysis basics	Findings from 2023 were tracked informally in email; no written risk management plan.	Not met	R-020
1.8	Risk analysis basics	EHR access reports reviewed ad hoc when a concern arises; M365 audit logs not reviewed.	Partial	R-004

ID	Question area	Finding	Status	Risk ID
2.2	Security policies	Policy set purchased from a template vendor in 2022; several standards (device/media controls, contingency) not customized to the practice.	Partial	R-021
2.3	Security policies	Policies have not been reviewed since adoption in 2022.	Not met	R-021
2.5	Security policies	Policies retained; training logs and access reviews not consistently retained.	Partial	R-021
2.8	Security policies	Breach notification policy exists in template set; staff unfamiliar with the four-factor assessment.	Partial	R-022
3.4	Security and your workforce	Training at onboarding; annual refresher skipped in 2025.	Partial	R-008
3.5	Security and your workforce	No periodic reminders sent.	Not met	R-008
3.6	Security and your workforce	Endpoint antivirus managed by the managed IT provider; staff have not been trained on reporting suspected malware.	Partial	R-008
3.7	Security and your workforce	M365 sign-in alerts enabled but go to IT vendor; not reviewed by practice.	Partial	R-004
3.8	Security and your workforce	Password policy exists; shared front-desk login on satellite clinic check-in PC.	Partial	R-001

ID	Question area	Finding	Status	Risk ID
3.9	Security and your workforce	No phishing simulations performed.	Not met	R-008
3.10	Security and your workforce	Onboarding training signed; no records of annual completion.	Partial	R-021
4.1	Security and your data	Unique IDs in EHR and M365; shared Windows login on satellite check-in PC.	Partial	R-001
4.2	Security and your data	No documented emergency access procedure.	Not met	R-015
4.3	Security and your data	EHR times out after 15 minutes; Windows screen lock set via policy on main clinic PCs only.	Partial	R-001
4.7	Security and your data	EHR and M365 retain audit logs; workstations do not forward logs.	Partial	R-004
4.8	Security and your data	EHR vendor maintains integrity controls; nothing practice-side.	Partial	R-004
4.11	Security and your data	No periodic user access review; two former employees found with active M365 accounts during this assessment.	Not met	R-009
4.14	Security and your data	Microsoft Defender AV on all PCs; not centrally monitored, no EDR.	Partial	R-003
4.15	Security and your data	M365 Defender filtering on; SPF configured, DKIM not enabled, DMARC p=none.	Partial	R-008

ID	Question area	Finding	Status	Risk ID
5.1	Security and the practice	Main clinic network closet locked; satellite clinic firewall and switch sit in an unlocked supply room.	Partial	R-006
5.2	Security and the practice	Alarm and keyed locks at both sites; cameras at main clinic only; no written facility security plan.	Partial	R-006
5.3	Security and the practice	Visitors sign in at front desk; no badges and vendors not escorted consistently.	Partial	R-006
5.4	Security and the practice	No maintenance log for locks/alarm changes.	Not met	R-006
5.6	Security and the practice	Exam room PCs not cable-locked; laptops go home with providers.	Partial	R-014
5.7	Security and the practice	Paper shredded by the shredding vendor (certificates on file); retired PCs taken by IT vendor without certificates of destruction.	Partial	R-017
5.8	Security and the practice	Unknown whether IT vendor wipes drives before redeploying PCs.	Not verified (gap)	R-017
5.9	Security and the practice	No hardware/media movement log.	Not met	R-017
5.11	Security and the practice	Practice iPhones enrolled in Intune with remote wipe; providers also access M365 email on personal phones without MDM.	Partial	R-002

ID	Question area	Finding	Status	Risk ID
6.1	Security and your vendors	List compiled during this assessment; previously no maintained list.	Partial	R-005
6.2	Security and your vendors	BAAs signed with EHR, Microsoft, IT, billing and backup vendors; answering service BAA in progress; no BAA located for the shredding vendor.	Partial	R-005
6.3	Security and your vendors	Vendor-supplied BAAs accepted as-is; incident reporting timeframes missing in two.	Partial	R-005
6.4	Security and your vendors	No vendor security review before onboarding.	Not met	R-005
6.5	Security and your vendors	EHR and billing BAAs specify 10-day reporting; others silent.	Partial	R-005
6.6	Security and your vendors	No vendor offboarding has occurred recently; no documented procedure.	Not verified (gap)	R-005
6.7	Security and your vendors	M365 Secure Score 52%; shared responsibility not documented.	Partial	R-005
7.1	Contingency planning	Hurricane checklist exists; no ransomware or extended-outage scenarios documented.	Partial	R-015
7.3	Contingency planning	Backups encrypted and offsite; immutability not confirmed for M365 backup.	Partial	R-007
7.4	Contingency planning	No written disaster recovery plan; relies on EHR vendor.	Not met	R-015

ID	Question area	Finding	Status	Risk ID
7.5	Contingency planning	Paper downtime forms for EHR outage at main clinic only.	Partial	R-015
7.7	Contingency planning	No criticality analysis performed.	Not met	R-015
7.8	Contingency planning	No documented restore tests.	Not met	R-007
7.10	Contingency planning	UPS on main clinic firewall and switch; none at satellite clinic. Hurricane shutters at main clinic.	Partial	R-018
BA	Vendors	Answering service has access to ePHI without a confirmed BAA (In progress).	Not met	R-005
BA	Vendors	Shredding vendor has access to ePHI without a confirmed BAA (Unknown).	Not met	R-005

5.1 Proposed Security Rule Readiness

These items reflect requirements in HHS's pending Security Rule update and are tracked separately from current-rule findings. The current rule remains in force until a final rule is published. Several also relate to current Required or Addressable specifications (2.7, 4.6, 4.4).

ID	Question area	Finding	Status	Priority
1.4	Risk analysis basics	No annual review occurred; not updated when satellite clinic opened.	Not met	High
1.6	Risk analysis basics	Spreadsheet inventory kept by the managed IT provider; medical devices and printers not included.	Partial	High
1.7	Risk analysis basics	No network or data-flow diagram exists.	Not met	High
2.6	Security policies	No periodic evaluation performed other than the 2023 SRA.	Not met	High

ID	Question area	Finding	Status	Priority
2.7	Security policies	Incident reporting form exists; no response playbook or incident log.	Partial	High
3.3	Security and your workforce	EHR access removed same day; M365 account disablement depends on IT ticket and has lagged up to a week. No offboarding checklist for keys/badges.	Partial	High
4.4	Security and your data	BitLocker on main clinic PCs and laptops; satellite clinic PCs, ECG and MFP hard drive unverified/unencrypted.	Partial	High
4.5	Security and your data	EHR and M365 use TLS; Office 365 Message Encryption licensed but staff rarely use it for external email.	Partial	Medium
4.6	Security and your data	MFA enforced for M365 and EHR; not enforced on IT vendor remote access tool or local admin accounts.	Partial	High
4.12	Security and your data	Windows Update automatic; firmware on firewall and MFP not patched on a schedule.	Partial	High
4.13	Security and your data	No vulnerability scanning or penetration testing performed.	Not met	High
4.16	Security and your data	Business firewall at each site; guest Wi-Fi isolated but clinical PCs and ECG on same flat network.	Partial	High

ID	Question area	Finding	Status	Priority
6.8	Security and your vendors	No periodic written verification obtained.	Not met	High
7.6	Contingency planning	Plans never tested.	Not met	High
7.9	Contingency planning	EHR vendor SLA states 24h RTO; local workstation rebuild time unknown.	Not verified (gap)	High
Asset	Inventory	Front desk workstations (2) stores or accesses ePHI and is not confirmed encrypted (Unknown).	Not met	High
Asset	Inventory	ECG machine (network-connected) stores or accesses ePHI and is not confirmed encrypted (Unknown).	Not met	High
Asset	Inventory	Multifunction printer / scanner / fax stores or accesses ePHI and is not confirmed encrypted (No).	Not met	High

6. Technical Validation Results

Check	Result	Date	Notes / risk ID
Orphaned accounts	Not run	—	Reported: 2 enabled M365 accounts for former staff (R-009)
MFA coverage	Not run	—	Reported: not on IT vendor remote tool or local admins (4.6)
Privileged accounts	Not run	—	No data
Encryption coverage	Not run	—	Reported: 3 ePHI assets not confirmed encrypted (4.4)

Check	Result	Date	Notes / risk ID
EDR and patch coverage	Not run	—	Reported: no EDR; firmware not patched on schedule (R-003, 4.12)
External exposure	Not run	—	No scanning performed (4.13)
Internal vulnerabilities	Not run	—	No scanning performed (4.13)
Email authentication	Not run	—	Reported: SPF yes, DKIM no, DMARC p=none (R-008)
Backup integrity	Not run	—	Reported: no restore tests (R-007)
Screen lock	Not run	—	Reported: EHR 15 min; Windows lock main clinic only (R-001)
Log retention	Not run	—	Reported: workstations do not forward logs (R-004)

Technical validation has not been performed. Notes show what the practice reported; each check must be run before the related safeguards can be rated.

7. Risk Register

Risk ID	Threat / vulnerability	Level	Planned mitigation	Owner	Status	Residual
R-001	All ePHI systems: Unauthorized access to ePHI via stolen credentials. Practice detail: shared Windows login on the satellite check-in PC; screen lock enforced on main clinic PCs only.	High (3×3=9)	Remove the shared satellite login; enforce a password standard and screen lock by policy on every PC at both sites.	Managed IT provider / Practice Manager	Open	Pending remediation
R-002	Laptops, mobile devices, removable media: Unencrypted ePHI on portable devices. Practice detail: providers read M365 email on personal phones without MDM.	High (2×3=6)	Require Intune app protection or MDM for any personal device accessing M365, with a signed BYOD agreement (Doc 10).	Managed IT provider / Practice Manager	Open	Pending remediation
R-003	EHR, file servers, endpoints: Ransomware / malware attack on ePHI systems. Practice detail: antivirus not centrally monitored; no EDR.	High (3×3=9)	Deploy managed EDR on all endpoints with alert monitoring.	Managed IT provider / Practice Manager	Open	Pending remediation

Risk ID	Threat / vulnerability	Level	Planned mitigation	Owner	Status	Residual
R-004	EHR / PM system: Insider threat — workforce misuse. Practice detail: EHR access reports reviewed ad hoc; M365 audit logs and sign-in alerts not reviewed by the practice; no practice-side integrity controls.	High (2×3=6)	Monthly documented log review (EHR access reports, M365 audit and sign-in alerts) with alerts routed to the practice; document integrity controls (Docs 06, 08).	Managed IT provider / Practice Manager	Open	Pending remediation
R-005	Business associate systems: Business associate data breach. Practice detail: no signed BAA with the answering service or the shredding vendor; BAAs lack incident reporting terms; no vendor reviews or offboarding procedure; M365 Secure Score 52%.	High (3×3=9)	Execute the two missing BAAs; amend BAAs for reporting timelines; adopt vendor review and offboarding steps; raise M365 Secure Score against a baseline (Doc 05).	Practice Manager	Open	Pending remediation
R-006	Server room / IT closet: Unauthorized entry to server room. Practice detail: satellite firewall and switch in an unlocked supply room; no facility security plan, vendor escorts or maintenance log.	High (3×2=6)	Lock the satellite network equipment; write a facility security plan per site; badge and escort vendors; keep a lock/alarm maintenance log (Doc 11).	Practice Manager	Open	Pending remediation
R-007	Backup platform: Failure of backup/recovery systems. Practice detail: no documented restore tests; M365 backup immutability unconfirmed.	High (3×3=9)	Confirm immutable or offline backup copy; perform and document quarterly test restores (Doc 09).	Managed IT provider / Practice Manager	Open	Pending remediation

Risk ID	Threat / vulnerability	Level	Planned mitigation	Owner	Status	Residual
R-008	Email platform: Phishing leads to email account takeover and mailbox ePHI exposure. Practice detail: annual training skipped in 2025; no reminders or phishing simulations; DKIM off, DMARC p=none.	High (3×3=9)	Annual training for all staff, quarterly reminders and phishing simulations; enable DKIM and move DMARC to quarantine, then reject.	Practice Manager	Open	Pending remediation
R-009	All ePHI systems: Former workforce member retains access. Practice detail: no periodic access review; two former employees found with active M365 accounts.	High (2×3=6)	Disable the two accounts immediately; quarterly documented access reviews for EHR and M365.	Managed IT provider / Practice Manager	Open	Pending remediation
R-014	Laptops, mobile devices: Lost or stolen unencrypted device. Practice detail: exam room PCs not cable-locked; laptops go home with providers.	Medium (2×2=4)	Cable-lock exam room PCs and set rules for laptops taken home (Doc 10).	Practice Manager	Open	Pending remediation
R-015	Hosted EHR / cloud services: Extended EHR or cloud vendor outage. Practice detail: no DR plan, criticality analysis or emergency access procedure; downtime forms at main clinic only.	High (3×3=9)	Write a contingency and DR plan with a criticality analysis and break-glass procedure; extend downtime forms to the satellite clinic (Docs 06, 09).	Practice Manager	Open	Pending remediation
R-017	Copiers, retired devices: Improper disposal of copier drives or retired devices. Practice detail: retired PCs left with IT vendor without certificates; drive wiping unknown; no media movement log.	High (3×3=9)	Require NIST 800-88 sanitization or certified destruction with certificates; confirm wiping before re-use; log device movement (Doc 07).	Managed IT provider / Practice Manager	Open	Pending remediation
R-018	Server location: Fire, flood, or power loss at server location. Practice detail: no UPS at the satellite clinic.	High (3×2=6)	Install UPS and surge protection for satellite network equipment.	Managed IT provider / Practice Manager	Open	Pending remediation

Risk ID	Threat / vulnerability	Level	Planned mitigation	Owner	Status	Residual
R-020	Security program (all ePHI): Risk analysis lapsed since 2023 and covered only the EHR and main clinic; no written risk management plan.	High (3×3=9)	Complete the enterprise-wide risk analysis for both sites, M365 and mobile devices; adopt a written risk management plan with owners and dates (Doc 02).	Practice Manager	Open	Pending remediation
R-021	Security policies and records: Policies not reviewed since 2022 or tailored to the practice; training logs and access reviews not retained.	High (3×2=6)	Review, tailor and re-sign Docs 01–12; set an annual review; keep training and review records for six years.	Practice Manager	Open	Pending remediation
R-022	Breach response: Late or missed breach notification: staff unfamiliar with the four-factor breach risk assessment.	High (3×3=9)	Train leadership on the four-factor assessment; adopt notification timelines, templates and decision records (Doc 04).	Practice Manager	Open	Pending remediation

Risk IDs follow the engagement workbook catalog. Catalog risks not scored in this report: R-010 Unpatched or unsupported systems exploited (Related readiness items 4.12, 4.13; not scored); R-011 Remote access exposed without MFA (RDP, VPN) (Related readiness item 4.6 (IT vendor remote tool lacks MFA); not scored); R-012 Flat network lets one infected device reach EHR or backups (Related readiness item 4.16 (clinical PCs and ECG on flat network); not scored); R-013 Misdirected email, fax, or portal message (Related readiness item 4.5; no incident data); R-016 ePHI entered into unapproved AI or consumer apps (Not covered by the assessment); R-019 Paper PHI left accessible or disposed of improperly (Shredding vendor certificates reported (5.7); walkthrough P5 pending). R-020 to R-022 were added for program-level findings.

8. Risk Management Activities Completed

Date completed	Risk ID	Action completed	Verified by
—	—	None recorded for this period	—

9. Plan of Action & Milestones

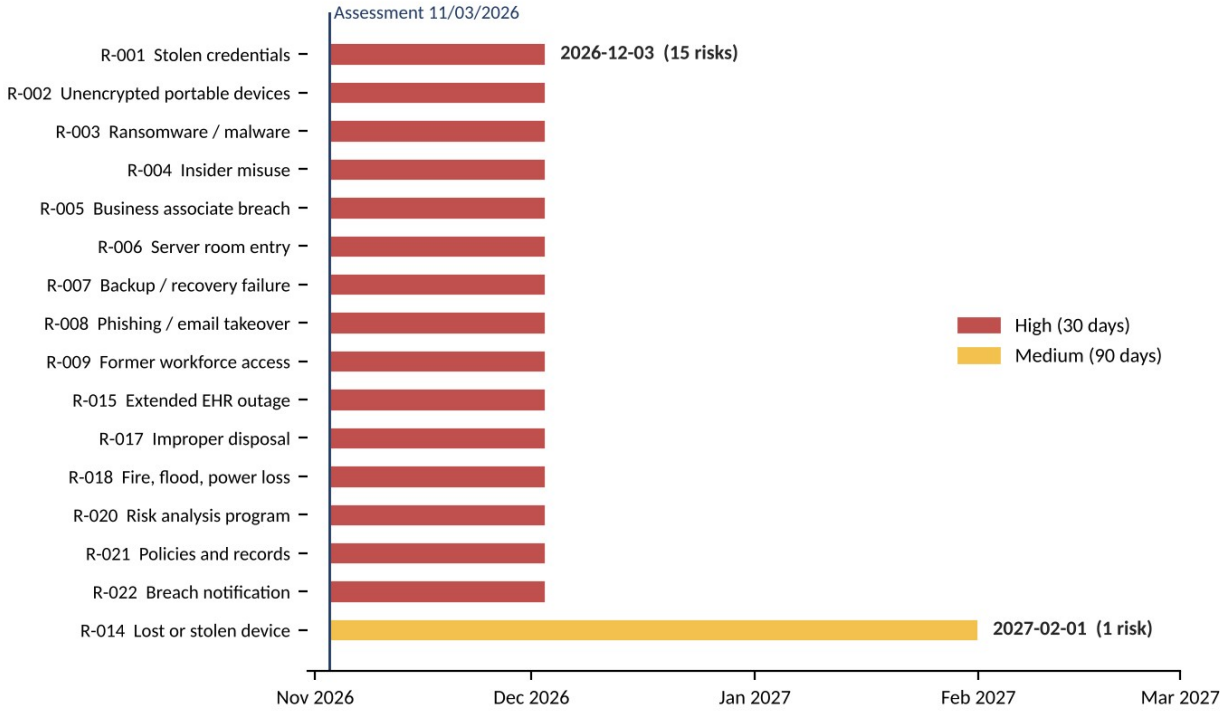
#	Risk ID	Required action	Owner	Target date	Interim control
1	R-001	Remove the shared satellite login; enforce a password standard and screen lock by policy on every PC at both sites.	Managed IT provider / Practice Manager	2026-12-03	None documented

#	Risk ID	Required action	Owner	Target date	Interim control
2	R-002	Require Intune app protection or MDM for any personal device accessing M365, with a signed BYOD agreement (Doc 10).	Managed IT provider / Practice Manager	2026-12-03	None documented
3	R-003	Deploy managed EDR on all endpoints with alert monitoring.	Managed IT provider / Practice Manager	2026-12-03	None documented
4	R-004	Monthly documented log review (EHR access reports, M365 audit and sign-in alerts) with alerts routed to the practice; document integrity controls (Docs 06, 08).	Managed IT provider / Practice Manager	2026-12-03	None documented
5	R-005	Execute the two missing BAAs; amend BAAs for reporting timelines; adopt vendor review and offboarding steps; raise M365 Secure Score against a baseline (Doc 05).	Practice Manager	2026-12-03	None documented
6	R-006	Lock the satellite network equipment; write a facility security plan per site; badge and escort vendors; keep a lock/alarm maintenance log (Doc 11).	Practice Manager	2026-12-03	None documented
7	R-007	Confirm immutable or offline backup copy; perform and document quarterly test restores (Doc 09).	Managed IT provider / Practice Manager	2026-12-03	None documented

#	Risk ID	Required action	Owner	Target date	Interim control
8	R-008	Annual training for all staff, quarterly reminders and phishing simulations; enable DKIM and move DMARC to quarantine, then reject.	Practice Manager	2026-12-03	None documented
9	R-009	Disable the two accounts immediately; quarterly documented access reviews for EHR and M365.	Managed IT provider / Practice Manager	2026-12-03	None documented
10	R-014	Cable-lock exam room PCs and set rules for laptops taken home (Doc 10).	Practice Manager	2027-02-01	None documented
11	R-015	Write a contingency and DR plan with a criticality analysis and break-glass procedure; extend downtime forms to the satellite clinic (Docs 06, 09).	Practice Manager	2026-12-03	None documented
12	R-017	Require NIST 800-88 sanitization or certified destruction with certificates; confirm wiping before re-use; log device movement (Doc 07).	Managed IT provider / Practice Manager	2026-12-03	None documented
13	R-018	Install UPS and surge protection for satellite network equipment.	Managed IT provider / Practice Manager	2026-12-03	None documented
14	R-020	Complete the enterprise-wide risk analysis for both sites, M365 and mobile devices; adopt a written risk management plan with owners and dates (Doc 02).	Practice Manager	2026-12-03	None documented

#	Risk ID	Required action	Owner	Target date	Interim control
15	R-021	Review, tailor and re-sign Docs 01–12; set an annual review; keep training and review records for six years.	Practice Manager	2026-12-03	None documented
16	R-022	Train leadership on the four-factor assessment; adopt notification timelines, templates and decision records (Doc 04).	Practice Manager	2026-12-03	None documented

Figure 4. Remediation timeline for open risks.



Bars run from the assessment date to each risk's Doc 02 target date (High 30 days, Medium 90 days). Fifteen risks share one due date; leadership may approve phased dates in the risk management plan.

10. Risk Acceptance

Risk ID	Residual level	Rationale	Accepted by	Date
None	—	No findings were marked "Risk accepted" in the assessment.	—	—

11. Policy Library Status

Doc	Policy	Coverage	Version	Signed	Changes this year
01	Information Security Policy	Pending	2022 template set	Pending	None; not reviewed since 2022 (2.3)
02	Risk Analysis & Risk Management Plan	Gap: no written risk management plan (1.5)	2022 template set	Pending	None; not reviewed since 2022 (2.3)
03	Workforce Security & Training Policy	Pending	2022 template set	Pending	None; not reviewed since 2022 (2.3)
04	Incident Response Plan	Partial: reporting form only; no playbook or incident log (2.7)	2022 template set	Pending	None; not reviewed since 2022 (2.3)
05	Business Associate Agreement	Partial: vendor BAAs accepted as-is (6.3)	2022 template set	Pending	None; not reviewed since 2022 (2.3)
06	Audit Controls & Access Management Policy	Pending	2022 template set	Pending	None; not reviewed since 2022 (2.3)
07	Media & Device Disposal Policy	Partial: 2022 template, not customized (2.2)	2022 template set	Pending	None; not reviewed since 2022 (2.3)
08	System Security Plan	Pending	2022 template set	Pending	None; not reviewed since 2022 (2.3)
09	Contingency & Data Backup Plan	Partial: 2022 template, not customized (2.2)	2022 template set	Pending	None; not reviewed since 2022 (2.3)
10	Workstation Use & Security Policy	Pending	2022 template set	Pending	None; not reviewed since 2022 (2.3)
11	Facility Access Control & Remote Work Policy	Pending	2022 template set	Pending	None; not reviewed since 2022 (2.3)

Doc	Policy	Coverage	Version	Signed	Changes this year
12	Notice of Privacy Practices	Pending	Pending	Pending	Pending

12. MIPS Promoting Interoperability

CEHRT in scope: Cloud EHR, version on file. CMS EHR Certification ID: on file.

Requirement	Completed	Date
Security risk analysis conducted or reviewed in-year, covering the full performance period (PI_PPHI_1, part 1)	Evidence review pending; scope must cover the full calendar year	—
Security risk management activities conducted (PI_PPHI_1, part 2)	No: none logged yet	—
Encryption of CEHRT data addressed	Reported encrypted (vendor-hosted); vendor documentation pending	—
2025 High Priority Practices SAFER Guide self-assessment	Pending	—

13. Attestation & Signatures

We attest that this security risk analysis was conducted for Sample Family Medicine, P.A. for the period Nov 2025 through Nov 2026, that it assessed risks to the confidentiality, integrity, and availability of ePHI, and that the risk management activities described in Section 8 were carried out. This attestation does not certify HIPAA compliance.

Name	Title	Signature & Date
Practice Manager	Security Officer	
Practice Owner	Executive / Owner	
Independent Assessor	Assessor	

Appendix A — Evidence Index

Evidence binder location:

File name	Question / check ID	Description	Date collected
None logged	—	No evidence collected yet; results are self-reported	—

Appendix B — Risk Scoring Method

Factor	Low (1)	Medium (2)	High (3)
Likelihood	Unlikely	Possible	Probable
Impact	Minimal harm	Significant harm	Severe / catastrophic
Risk level = Likelihood × Impact	Low (1–2)	Medium (3–4)	High (6–9)

Remediation targets: High within 30 days, Medium within 90 days, Low within 180 days of identification (Doc 02, §4.1).

Appendix C — MIPS Security Risk Analysis Attestation Memo

To: Sample Family Medicine, P.A. MIPS / quality reporting lead

From: Practice Manager, Security Officer

Date: November 3, 2026

Re: Security Risk Analysis measure (PI_PPHI_1), performance year 2026

This memo confirms the following for the 2026 performance period:

- A security risk analysis was conducted on November 3, 2026, within calendar year 2026, covering the full performance period (Nov 2025 through Nov 2026), in accordance with 45 CFR § 164.308(a)(1)(ii)(A).
- The analysis covered the certified EHR technology used for Promoting Interoperability reporting: Cloud EHR, version on file (CMS EHR Certification ID), including the security and encryption of ePHI it creates or maintains.
- Security risk management activities were conducted during the year in accordance with 45 CFR § 164.308(a)(1)(ii)(B). Risk management actions completed to date are, as listed in Section 8 of the SRA report.
- Supporting documentation is retained in the SRA evidence binder at.

This memo supports the MIPS attestation only. It does not certify HIPAA compliance; HHS does not issue or recognize HIPAA compliance certifications.

Name	Title	Signature & Date
Practice Manager	Security Officer	