SENTINEL

COMPLIANCE COMMAND

Security Risk Analysis

STANDALONE ENGAGEMENT

Cedar Park Family Practice — SAMPLE (Fictional Practice)

45 CFR 164.308(a)(1)(ii)(A) · Finalized 2026-03-04

This document is a risk analysis. It records what was assessed, what was found, and the resulting risk levels. It is not a certification, not an attestation of any compliance status, and not a guarantee of any outcome or result.

Scope of the Analysis

This analysis covers electronic protected health information wherever it is created, received, maintained, or transmitted by the practice: the hosted Meridian Chart EHR, six front-office and clinical workstations, two clinical laptops, the practice email system, the patient portal, the networked copier/scanner, the on-premise backup appliance and its offsite replica, staff mobile devices used for clinical messaging, and every vendor connection through which practice ePHI moves. Single location.

Locations covered: Main office — single location

The analysis covers electronic protected health information wherever it is created, received, maintained, or transmitted — systems, devices, media, and vendor connections — not a single computer system.

Methodology

This analysis follows the nine elements of the HHS Office for Civil Rights Guidance on Risk Analysis Requirements under the HIPAA Security Rule (Final Guidance, posted July 14, 2010), implementing 45 CFR 164.308(a)(1)(ii)(A). Framework verified against the published guidance August 14, 2026.

- 1. Scope of the Analysis
- 2. Data Collection
- 3. Identify and Document Potential Threats and Vulnerabilities
- 4. Assess Current Security Measures
- 5. Determine the Likelihood of Threat Occurrence
- 6. Determine the Potential Impact of Threat Occurrence
- 7. Determine the Level of Risk
- 8. Finalize Documentation
- 9. Periodic Review and Updates to the Risk Assessment

HHS endorses no particular risk-analysis model; the nine elements above are the documentation structure the guidance itself sets out.

The Security Rule is scalable: it does not prescribe specific technologies, and a small practice is not held to a large organization’s methods. In deciding which security measures are reasonable and appropriate, 45 CFR 164.306(b)(2) requires four factors to be considered — the size, complexity and capabilities of the practice; its technical infrastructure, hardware and software security capabilities; the cost of security measures; and the probability and criticality of potential risks to ePHI. Cost alone is not an acceptable reason to leave a reasonable and appropriate measure unimplemented.

Risk level is derived as likelihood × impact on a 3×3 scale: 1–2 Low · 3–4 Moderate · 6 High · 9 Critical.

HHS endorses no risk-rating method. CMS describes an average-based example and expressly permits a risk level matrix; this analysis uses a documented 3×3 likelihood × impact matrix, which derives the level from two separately recorded judgments and is deliberately more conservative than averaging where impact is high.

Data collection: Structured remote intake completed by the practice; Working session with the practice administrator and the lead physician; Assessor-guided video walkthrough of the physical environment; Documents reviewed as provided through the secure portal; Vendor agreements and backup configuration reviewed directly Conducted remotely. No site visit was required.

Asset Inventory

System / Device	Category	Location	Notes
Meridian Chart EHR (hosted)	EHR	Hosted / cloud	
Front-office and clinical workstations (6)	Workstations	Reception, billing, clinical	
Clinical laptops (2)	Portable device	Exam rooms	
Practice email (Microsoft 365)	Email	Hosted / cloud	
Patient portal (EHR-integrated)	Patient access	Hosted / cloud	
Networked copier / scanner	Office equipment	Records room	
Backup appliance + offsite replica	Backup	Server closet / offsite	
Staff mobile devices used for clinical messaging (4)	Mobile	Carried	

Data Flows

How ePHI moves, including outward to business associates. BAA status is shown as recorded in the vendor inventory at generation.

From	To	What moves	BAA status
Practice systems	Northgate Billing Services	Claims and billing data	—
Practice systems	Ironvault Backup	Encrypted nightly backup	—
Practice systems	Riverbend IT Partners	Remote support access	—
Practice systems	SecureShred Services	Paper record destruction	—
Practice systems	Meridian Chart	Hosted EHR and patient portal	—

Threats and Vulnerabilities

5 threat/vulnerability pairs identified as applicable, each with practice-specific reasoning. 26 library threats reviewed and documented as not applicable.

Identified threats

Threat	Category	Vulnerability	Why it applies here
Phishing / social engineering	Human	Workforce members can be induced to reveal credentials or open malicious attachments on systems that access ePHI.	Staff email is the primary channel for referrals and payer correspondence, and no simulated phishing or structured awareness training has been run.
Lost or stolen portable device	Human	Laptops, phones, tablets or portable media holding or accessing ePHI can leave the facility and be lost or stolen.	Three former staff accounts remained enabled in the EHR at the time of the assessment.
Insider	Human	Workforce members with legitimate	Riverbend IT Partners holds standing remote

Threat	Category	Vulnerability	Why it applies here
misuse / snooping		access can view records beyond their role without detection.	access to every workstation and no executed business associate agreement could be located.
Malware / ransomware	Technical	Malicious code can encrypt, destroy or exfiltrate ePHI and halt operations.	A single on-premise backup appliance with an offsite replica; restoration has never been tested, so recovery time is unknown.
Business associate breach	Third-Party	A vendor holding or accessing ePHI can suffer its own breach; obligations and notification depend on the BAA.	Riverbend IT Partners holds standing remote access to every workstation and no executed business associate agreement could be located.

Threats Reviewed and Not Applicable

Documented so the review is visible — a rejected threat is a decision, not an omission.

Threat	Reasoning
Misdirected email / fax disclosure	Not applicable to this environment.
Improper disposal of media or paper	Not applicable to this environment.
Shared or weak login credentials	Not applicable to this environment.
Departed-workforce access not terminated	Not applicable to this environment.
Physical access surviving departure (keys, badges, codes)	Not applicable to this environment.
Off-site and home use of ePHI systems	Not applicable to this environment.
Visitor and business-hours physical access	Not applicable to this environment.
Screen visible to unauthorized persons	Not applicable to this environment.
Unpatched or end-of-life software	Not applicable to this environment.
Absent encryption at rest	Not applicable to this environment.
Unencrypted transmission (email / texting ePHI)	Not applicable to this environment.
Absent or unreviewed audit logging	Not applicable to this environment.
No automatic logoff / unattended sessions	Not applicable to this environment.
No usable data backup / untested restore	Not applicable to this environment.
Misconfigured cloud storage or sharing	Not applicable to this environment.
Copier / printer / scanner storage	Not applicable to this environment.
Residual ePHI on re-used or donated equipment	Not applicable to this environment.
Undetected alteration or corruption of ePHI	Not applicable to this environment.
No emergency access path to ePHI	Not applicable to this environment.
Fire	Not applicable to this environment.
Flood / water damage	Not applicable to this environment.
Extended power failure	Not applicable to this environment.
Break-in / physical theft	Not applicable to this environment.

Threat	Reasoning
Vendor access without a BAA	Not applicable to this environment.
EHR / hosting provider outage	Not applicable to this environment.
Vendor remote-access compromise	Not applicable to this environment.

Current Security Measures — Administrative

Where a safeguard below is recorded as Not in place or Not applicable, the reason is recorded with it. An addressable implementation specification is not optional: where it is not a reasonable and appropriate safeguard, the practice must document why and adopt an equivalent alternative measure where that is reasonable and appropriate (45 CFR 164.306(d)(3)).

Safeguard	Standard	Rule	Status	Evidence	Basis / rationale
Risk management process (acting on identified risks)	164.308(a)(1)(ii)(B)	Required	—	Reported	Described in the working session; not evidenced
Sanction policy for workforce violations	164.308(a)(1)(ii)(C)	Required	—	Documented	Reviewed the executed agreement
Information system activity review	164.308(a)(1)(ii)(D)	Required	Partially in place	Reported	The practice states this is in place; no supporting document was available — Partially in place — see the register.
Designated security official responsible for security policies and procedures	164.308(a)(2)	Required	—	Reported	The practice states this is in place; no supporting document was available
Workforce security — authorization and clearance procedures	164.308(a)(3)	Required standard · addressable specifications	—	Documented	Reviewed the configuration directly
Access termination on workforce departure	164.308(a)(3)(ii)(C)	Addressable	—	Documented	Reviewed the executed agreement
Information access management (granting, establishing, reviewing and modifying access to ePHI)	164.308(a)(4)	Required standard · addressable specifications	Not in place	Not identified	Not in place at the time of the assessment.
Security awareness and training program	164.308(a)(5)	Required standard · addressable specifications	—	Reported	The practice states this is in place; no supporting document was available
Security incident procedures and response	164.308(a)(6)	Required	—	Documented	Reviewed the configuration directly
Contingency plan (backup, disaster recovery, emergency mode)	164.308(a)(7)	Required	Partially in place	Reported	Described in the working session; not evidenced — Partially in place — see the register.
Contingency plan testing and revision procedures	164.308(a)(7)(ii)(D)	Addressable	—	Reported	Described in the working session; not evidenced
Applications and data criticality analysis	164.308(a)(7)(ii)(E)	Addressable	—	Documented	Reviewed the written policy, dated and adopted

Safeguard	Standard	Rule	Status	Evidence	Basis / rationale
Periodic technical and nontechnical evaluation of security policies and procedures	164.308(a)(8)	Required	—	Documented	Reviewed the configuration directly
Business associate agreements for vendors touching ePHI	164.308(b)(1)	Required	Not in place	Not identified	Not in place at the time of the assessment.

Current Security Measures — Physical

Safeguard	Standard	Rule	Status	Evidence	Basis / rationale
Facility access controls (contingency operations, security plan, access validation, maintenance records)	164.310(a)(1)	Required standard · addressable specifications	—	Reported	Described in the working session; not evidenced
Workstation use policies (proper functions, manner of performance, surroundings, off-site use)	164.310(b)	Required	—	Documented	Reviewed the written policy, dated and adopted
Workstation security (physical protection from unauthorized access)	164.310(c)	Required	Partially in place	Reported	The practice states this is in place; no supporting document was available — Partially in place — see the register.
Device and media controls (receipt and movement of hardware and media)	164.310(d)(1)	Required standard · addressable specifications	—	Reported	The practice states this is in place; no supporting document was available
Media disposal and sanitization	164.310(d)(2)(i)	Required	—	Documented	Reviewed the system export
ePHI removal from media before re-use	164.310(d)(2)(ii)	Required	—	Documented	Reviewed the written policy, dated and adopted
Movement log for hardware and media (person responsible)	164.310(d)(2)(iii)	Addressable	Not in place	Not identified	Not in place at the time of the assessment.
Exact-copy backup before equipment movement	164.310(d)(2)(iv)	Addressable	—	Reported	The practice states this is in place; no supporting document was available

Current Security Measures — Technical

Safeguard	Standard	Rule	Status	Evidence	Basis / rationale
Unique user identification for each person with ePHI access	164.312(a)(2)(i)	Required	—	Documented	Reviewed the system export
Emergency access procedure for obtaining ePHI during an emergency	164.312(a)(2)(ii)	Required	Partially in place	Reported	Described in the working session; not evidenced — Partially in place — see the register.
Automatic logoff	164.312(a)(2)(iii)	Addressable	—	Reported	Described in the working session; not evidenced
Encryption and decryption mechanism for stored ePHI	164.312(a)(2)(iv)	Addressable	—	Documented	Reviewed the executed agreement
Audit controls (activity recording on ePHI systems)	164.312(b)	Required	—	Documented	Reviewed the system export
Integrity (protection of ePHI from improper alteration or destruction)	164.312(c)(1)	Required standard · addressable specifications	Not in place	Not identified	Not in place at the time of the assessment.
Person or entity authentication	164.312(d)	Required	—	Reported	Described in the working session; not evidenced
Transmission integrity controls (modification detection in transit)	164.312(e)(2)(i)	Addressable	—	Documented	Reviewed the executed agreement
Encryption of ePHI in transit	164.312(e)(2)(ii)	Addressable	Partially in place	Reported	The practice states this is in place; no supporting document was available — Partially in place — see the register.

Evidence Reviewed

This analysis distinguishes what Sentinel reviewed from what the practice reported. The distinction is recorded against every safeguard and finding, and is stated here so that no item in this document is read as verified unless it was.

Documented — Sentinel reviewed supporting evidence.

Reported — The practice states this is in place; supporting evidence was not reviewed, or was insufficient to record as Documented.

Not identified — The control, process, or supporting evidence was not identified during the assessment.

Not applicable — Not applicable based on the documented scope and rationale.

Classification	Items
Documented	13
Reported	14
Not identified	9
Not applicable	0
Unclassified	0

Risk Determinations

Risk level is derived as likelihood × impact on a 3×3 scale: 1–2 Low · 3–4 Moderate · 6 High · 9 Critical. Likelihood and impact are recorded judgments with rationale; the level is derived, never assigned by hand.

Threat	Likelihood	Impact	Level	Rationale
Phishing / social engineering	High	High	Critical	Likelihood: Based on the practice's current controls and the conditions observed during the assessment. Impact: Reflects the volume of ePHI reachable through this path and the practice's ability to detect and recover.
Lost or stolen portable device	High	Medium	High	Likelihood: Based on the practice's current controls and the conditions observed during the assessment. Impact: Reflects the volume of ePHI reachable through this path and the practice's ability to detect and recover.
Insider misuse / snooping	Medium	High	High	Likelihood: Based on the practice's current controls and the conditions observed during the assessment. Impact: Reflects the volume of ePHI reachable through this path and the practice's ability to detect and recover.
Malware / ransomware	Medium	Medium	Moderate	Likelihood: Based on the practice's current controls and the conditions observed during the assessment. Impact: Reflects the volume of ePHI reachable through this path and the practice's ability to detect and recover.
Business associate breach	Medium	High	High	Likelihood: Based on the practice's current controls and the conditions observed during the assessment. Impact: Reflects the volume of ePHI reachable through this path and the practice's ability to detect and recover.

Remediation Register

Every finding ranked, owned, and dated. Open items remain open here — the register states reality.

Sentinel structures and documents remediation; implementing the corrective actions remains the practice's responsibility. A closed entry records that the finding was closed and the evidence that documents it.

Finding	Level	Owner	Target date	Evidence required to close	Status
No executed business associate agreement for the IT provider holding standing remote access	Critical	Practice Owner	2026-04-15	Executed BAA countersigned by both parties	Open
Device encryption not confirmed on clinical laptops	High	IT Provider	2026-04-30	Encryption status report or configuration screenshot for each laptop	Open
Backup restoration has never been tested	High	IT Provider	2026-05-29	Dated restoration test record showing a file recovered and verified	Open
Three former workforce members retained active EHR accounts	High	Practice Administrator	2026-03-20	EHR user list showing the accounts disabled, plus a termination checklist	Open
No security awareness training programme in place	Moderate	Practice Administrator	2026-06-30	Training completion record for all workforce members	Open

Findings Closed Since the Prior Analysis

This is the first analysis of record — there is no prior register to close against.

Periodic Review

The Security Rule names no fixed interval for risk analysis, but expects periodic review and updates as the environment changes. This engagement includes a six-month remediation review, which Sentinel schedules and conducts. Sentinel recommends annual reassessment pacing as a professional operating standard — not a legal deadline — and scheduling any analysis beyond the deliverables of this engagement is the practice's responsibility.

Statement of Preparation

Conducted by Kevin Jones, Sentinel Compliance Command. Started 2026-03-04; finalized 2026-03-04.

This document is a risk analysis. It records what was assessed, what was found, and the resulting risk levels. It is not a certification, not an attestation of any compliance status, and not a guarantee of any outcome or result.

No license, credential, or certification is required by law to conduct a HIPAA security risk analysis, and the U.S. Department of Health and Human Services does not recognize any private HIPAA credential. Sentinel Compliance Command does not represent this analysis as a legal determination; questions of legal sufficiency belong with the practice's counsel.

This analysis is part of the practice's Security Rule documentation. 45 CFR 164.316(b)(2) requires such documentation to be retained for six years from the date of its creation or the date it was last in effect, whichever is later; to be made available to the persons responsible for implementing the procedures it describes; and to be reviewed periodically and updated as needed in response to environmental or operational change. Written form may be electronic.

This engagement is a bounded, point-in-time security risk analysis. It reflects the practice as assessed on the dates stated, and the findings in the Remediation Register remain the practice's to remediate. The engagement includes one further scheduled deliverable — a six-month remediation review documenting what evidence of closure Sentinel was able to review. Beyond the deliverables defined in the engagement, this document does not establish or imply continuous monitoring or an ongoing advisory relationship.