SENTINEL

COMPLIANCE COMMAND

Security Risk Analysis

STANDALONE ENGAGEMENT

Willow Creek Family Medicine — SAMPLE (Fictional Practice)

45 CFR 164.308(a)(1)(ii)(A) · Finalized 2026-08-16

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 the hosted ClearChart Health EHR, four front-office and clinical workstations, the practice email system, the patient portal, the networked copier/scanner, local and offsite backups held with SecureVault Data Backup, and every vendor connection where Willow Creek Family Medicine ePHI is created, received, maintained, or transmitted.

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.

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

Data collection: On-site walkthrough

Asset Inventory

System / Device	Category	Location	Notes
ClearChart Health EHR (hosted)	EHR	Hosted / cloud	
Front-office workstations (4)	Workstations	Reception & billing office	
Clinical laptop (exam rooms)	Portable device	Exam rooms	
Networked copier/scanner	Office equipment	Records room	

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	BrightPath Billing Partners	Claims and billing data	Executed
Practice systems	SecureVault Data Backup	Encrypted nightly backup	Executed
Practice systems	Bluestem IT Services	Remote support access	Pending
Practice systems	TidyShred Document Destruction	Paper records destruction	Executed

Threats and Vulnerabilities

3 threat/vulnerability pairs identified as applicable, each with practice-specific reasoning. 21 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 handle inbound patient email daily on accounts that also open the EHR; one phishing attempt is already on the incident log.
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.	A clinical laptop moves between exam rooms daily and occasionally leaves the building for home charting; disk encryption has not been verified on it.
No usable data backup / untested restore	Technical	ePHI cannot be recovered after loss, corruption or ransomware if backups are absent or never test-restored.	A restore from the SecureVault offsite backup has never been test-performed at this practice.

Threats Reviewed and Not Applicable

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

Threat	Reasoning
Insider misuse / snooping	Not applicable to this environment.
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.
Unpatched or end-of-life software	Not applicable to this environment.
Absent encryption at rest	Not applicable to this environment.

Threat	Reasoning
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.
Malware / ransomware	Not applicable to this environment.
Misconfigured cloud storage or sharing	Not applicable to this environment.
Copier / printer / scanner storage	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.
Business associate breach	Not applicable to this environment.
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

Safeguard	Standard	Status	Evidence / note
Risk management process (acting on identified risks)	164.308(a)(1)(ii)(B)	In place	
Sanction policy for workforce violations	164.308(a)(1)(ii)(C)	In place	
Information system activity review	164.308(a)(1)(ii)(D)	In place	
Workforce authorization and clearance procedures	164.308(a)(3)	In place	
Access termination on workforce departure	164.308(a)(3)(ii)(C)	In place	
Security awareness and training program	164.308(a)(5)	In place	
Security incident procedures and response	164.308(a)(6)	In place	
Contingency plan (backup, disaster recovery, emergency mode)	164.308(a)(7)	In place	
Business associate agreements for vendors touching ePHI	164.308(b)(1)	In place	

Current Security Measures — Physical

Safeguard	Standard	Status	Evidence / note
Facility access controls	164.310(a)	In place	
Workstation use and workstation security	164.310(b)-(c)	In place	
Device and media controls (receipt, movement, reuse)	164.310(d)	In place	
Media disposal and sanitization	164.310(d)(2)(i)	In place	

Current Security Measures — Technical

Safeguard	Standard	Status	Evidence / note
Access control with unique user identification	164.312(a)	In place	
Automatic logoff	164.312(a)(2)(iii)	Partially in place	
Encryption of ePHI at rest	164.312(a)(2)(iv)	Not in place	
Audit controls (activity recording on ePHI systems)	164.312(b)	In place	
Integrity controls (protection from improper alteration)	164.312(c)	In place	
Person or entity authentication	164.312(d)	In place	
Transmission security (encryption in transit)	164.312(e)	In place	

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	Medium	High	Likelihood: Daily inbound email volume across the workforce; one attempt already on the log. Impact: A phished credential opens the hosted EHR.
Lost or stolen portable device	Medium	High	High	Likelihood: Restore has never been exercised; failure would be discovered only during an emergency. Impact: Ransomware without a proven restore risks total loss of the practice record.
No usable data backup / untested restore	Medium	High	High	Likelihood: The laptop leaves the building; loss or theft is a recognized exposure for portable devices. Impact: An unencrypted lost laptop is a reportable exposure of every chart it can reach.

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	Status
Address: Phishing / social engineering exposure across staff email	High	J. Tran, Office Manager	2026-09-30	In Progress
Perform and document a test restore of the SecureVault offsite backup	High	Bluestem IT Services (vendor) — sponsored by J. Tran	2026-09-15	In Progress
Verify or enable full-disk encryption on the clinical laptop	High	Bluestem IT Services (vendor) — sponsored by Dr. A. Whitfield	2026-09-06	Open
Safeguard not in place: encryption of ePHI at rest on front-office workstations (164.312(a)(2)(iv))	Moderate	Bluestem IT Services (vendor)	2026-10-15	Open
Execute the pending BAA with Bluestem IT Services	Moderate	J. Tran, Office Manager	2026-09-06	In Progress
Standardize workstation auto-logoff to a single documented interval	Moderate	J. Tran, Office Manager	2026-10-30	Open
Shared login retired on the networked copier/scanner console	High	Bluestem IT Services (vendor)	2026-07-07	Closed 2026-07-12 — Per-user access codes issued; configuration change record dated and filed to the practice record
Sanction-policy acknowledgment collected from all four workforce members	Low	J. Tran, Office Manager	2026-07-22	Closed 2026-07-26 — Four signed acknowledgment forms dated and filed to the practice record
Contingency-plan review completed and documented for the current cycle	Moderate	Dr. A. Whitfield	2026-07-27	Closed 2026-08-02 — Reviewed plan re-adopted; review memorandum dated and filed to the practice record

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. Scheduling and conducting future reviews is the practice's responsibility.

Statement of Preparation

Conducted by Sentinel Compliance Command. Started 2026-08-16; finalized 2026-08-16.

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 engagement was a bounded, point-in-time security risk analysis. It reflects the practice as assessed on the dates stated. The findings in the Remediation Register remain the practice's to remediate, and this document does not establish or imply any ongoing monitoring, tracking, or advisory relationship.