



ENDPOINT SOLUTIONS

Technology Leadership Assessment — Delivery Report



Client: Cedar Valley Family Medicine

Date: June 3, 2026

Prepared by: Michael-Paul Hart, Endpoint Solutions

Confidential — prepared for Cedar Valley Family Medicine leadership. Not for distribution.

ENDPOINT SOLUTIONS

Technology Leadership Assessment — Delivery Report

Client: Cedar Valley Family Medicine · Date: June 3, 2026 · Prepared by: Michael-Paul Hart

OVERALL MATURITY

44**Developing**

Combined maturity across the assessed stages.

ENGAGEMENT

Industry: Healthcare — Primary Care Clinic (2 locations)

Primary sponsor: Dr. Priya Nair — Physician Owner

Executive summary

Cedar Valley Family Medicine delivers strong patient care across two locations, and HIPAA obligations have pushed the practice to adopt some good habits — a cloud EHR, business-associate agreements with major vendors, and periodic leadership attention to compliance. But technology has been managed reactively, there is no internal owner, and the practice's continuity and vendor oversight have real gaps that matter when patient care depends on systems being up.

The most serious exposures are continuity (the EHR is vendor-hosted, but on-site systems — imaging, documents, and the local network — depend on backups that have not been tested) and unmanaged risk around staff use of new tools with patient information. HIPAA raises the stakes on both. This report gives leadership a prioritized plan to shore up continuity and governance first, then reduce day-to-day friction, without disrupting the schedule.

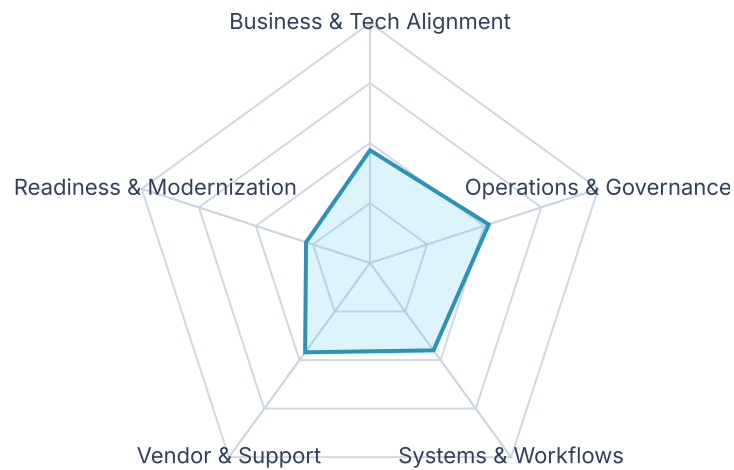
Current-state overview

The practice runs a cloud-hosted EHR/practice-management system (vendor-managed, with a signed BAA), Microsoft 365 for email and documents, an on-site imaging/document system at the main location, and a local network across two sites connected by a business ISP. A managed IT provider supports the network and endpoints. HIPAA has driven baseline discipline — BAAs, some security awareness, periodic compliance review — but there is no internal technology owner, MFA is uneven on non-EHR systems, and continuity is unproven for the on-site systems and local files. Vendor coverage and spend across the EHR, IT provider, imaging, and connectivity are not centrally tracked.

Maturity scorecard

STAGE		SCORE	INTERPRETATION
01	Business & Tech Alignment	47%	Developing
02	Operations & Governance	52%	Developing
03	Systems & Workflows	45%	Developing
04	Vendor & Support	46%	Developing
05	AI Readiness & Modernization	28%	Reactive

Maturity profile



Top findings & business implications

1. **On-site systems and local files depend on backups that have never been test-restored.** — A ransomware event or hardware failure could disrupt patient care and imaging with an unproven path to recovery — a patient-safety and HIPAA continuity risk.
2. **No internal owner for technology, security, or HIPAA-related IT controls.** — Security and continuity decisions default to vendors; leadership lacks a single accountable point and consolidated visibility.
3. **Multi-factor authentication is uneven outside the EHR.** — Email and file accounts holding patient information are more exposed to compromise and phishing, a common healthcare breach vector.
4. **No policy on staff use of AI or new tools with patient information.** — Protected health information could be entered into unapproved tools, creating HIPAA exposure the practice cannot currently see.
5. **Vendor coverage and spend across EHR, IT, imaging, and connectivity are not tracked centrally.** — Gaps in who-covers-what surface during incidents, and leadership cannot see total cost or renewal timing.

Domain observations

01 • BUSINESS & TECH ALIGNMENT — 47%

Leadership recognizes that reliable systems are part of patient care and compliance, but technology decisions are made case by case rather than against a plan. There is no roadmap tying technology to the practice's growth (a possible third location) or to its compliance calendar.

02 • OPERATIONS & GOVERNANCE — 52%

HIPAA has produced some governance — BAAs, periodic compliance attention, occasional leadership discussion — which is a relative strength versus other SMBs. But there is no internal technology or security owner, IT-side HIPAA controls aren't documented against a standard, and reporting is inconsistent. Formalizing ownership and control documentation is the priority.

03 • SYSTEMS & WORKFLOWS — 45%

The cloud EHR is vendor-managed and generally reliable, but the on-site imaging/document system and local network are where continuity risk lives — backups exist but have never been test-restored, and there are no documented recovery targets. Microsoft 365 is used mainly for email. Some workflow friction exists between the EHR, documents, and scheduling.

04 • VENDOR & SUPPORT — 46%

The practice depends on several critical vendors — EHR, managed IT, imaging, connectivity — but coverage boundaries are only partly clear and there is no central view of spend or renewals. During an incident it is not always obvious who is responsible. A consolidated vendor and BAA inventory would reduce both risk and cost.

05 • AI READINESS & MODERNIZATION — 28%

AI readiness is early and, importantly, unmeasured: leadership is unsure whether staff are using AI tools with patient information, and there is no acceptable-use policy. Given HIPAA, the first step is visibility and a clear policy, not adoption. There are longer-term automation opportunities in documentation and scheduling once guardrails exist.

Risk register

RISK	AREA	SEVERITY	OWNER
Untested backups of on-site imaging/documents and local files — recovery unproven	Systems & Workflows	Critical	Managed IT + Physician Owner
Possible PHI entered into unapproved AI or consumer tools, with no policy	AI Readiness & Modernization	High	Physician Owner + Compliance
Uneven MFA on email/file accounts holding patient information	Operations & Governance	High	Managed IT
No internal owner or documented IT-side HIPAA controls	Operations & Governance	Medium	Practice Manager
Unclear vendor coverage boundaries during an incident	Vendor & Support	Medium	Practice Manager

Recommended priorities

03 • SYSTEMS & WORKFLOWS

Prove continuity for on-site systems and local files

Test-restore imaging, documents, and local file backups, document recovery targets, and close gaps — so a failure or ransomware event does not put patient care or compliance at risk.

02 • OPERATIONS & GOVERNANCE

Enforce MFA and document IT-side HIPAA controls

Turn on multi-factor authentication across email and files, and document the practice's technical safeguards against a recognized standard the practice can show auditors and insurers.

05 • AI READINESS & MODERNIZATION

Get visibility and a policy on AI and new-tool use with PHI

Determine whether staff are using AI tools with patient information and publish a clear acceptable-use policy before any adoption.

04 • VENDOR & SUPPORT

Consolidate vendors, BAAs, coverage, and spend

Build one view of critical vendors, business-associate agreements, coverage boundaries, and renewals so responsibility is clear and cost is visible.

Technology leadership roadmap

0–30 days

ACTION	OWNER	PRIORITY	EFFORT
Test-restore on-site imaging, documents, and local file backups Outcome: Proven recovery for care-critical on-site systems · Vendor: MedTech Managed IT · Depends on: Backup access	Managed IT	High	Medium
Enforce multi-factor authentication on all email and file accounts Outcome: Reduced phishing and account-compromise risk · Vendor: MedTech Managed IT	Managed IT	High	Low
Assess AI/tool use with PHI and publish an acceptable-use policy Outcome: Visibility and guardrails for HIPAA compliance · Vendor: Endpoint Solutions	Physician Owner	High	Low

31–90 days

ACTION	OWNER	PRIORITY	EFFORT
Document IT-side HIPAA technical safeguards against a standard Outcome: Audit- and insurer-ready control documentation · Vendor: Endpoint Solutions	Practice Manager	High	Medium
Build a vendor, BAA, coverage, and renewal inventory Outcome: Clear responsibility and cost visibility · Vendor: Endpoint Solutions · Depends on: Contracts gathered	Practice Manager	Medium	Medium
Name an internal technology & security point of contact Outcome: A single accountable owner for technology and risk	Physician Owner	Medium	Low

91–180 days

ACTION	OWNER	PRIORITY	EFFORT
Reduce friction between the EHR, documents, and scheduling Outcome: Less staff time lost to workarounds · Vendor: EHR vendor	Practice Manager	Medium	Medium
Formalize a security-awareness and phishing-training cadence Outcome: Fewer successful phishing attempts · Vendor: MedTech Managed IT	Managed IT	Medium	Low

181–365 days

ACTION	OWNER	PRIORITY	EFFORT
Develop a two-site continuity plan and annual test Outcome: Care continues if one location or system is down · Vendor: Endpoint Solutions · Depends on: Restore tests complete	Physician Owner	Medium	Medium
Evaluate approved automation for documentation and scheduling Outcome: Provider time back for patient care · Vendor: Endpoint Solutions · Depends on: AI policy in place	Technology owner	Low	Medium

Vendor & support ecosystem

VENDOR	ROLE / COVERAGE	RENEWAL / NOTES
CareChart EHR (cloud, BAA signed)	EHR & practice management	Annual 02/2027
MedTech Managed IT	Network, endpoint & help-desk support (BAA signed)	07/2026
Microsoft 365 (Business Standard, BAA signed)	Email, files, identity — 70 licenses	04/2027
ClearImage PACS (on-site)	Imaging & document storage	12/2026
TwinCity Fiber	Internet & two-site connectivity	Unknown — contract not located
ShieldCyber Insurance	Cyber liability (healthcare)	09/2026

Documentation reviewed: Vendor list & major technology invoices · MSP / IT support agreement · Microsoft 365 licensing or admin summary · Cybersecurity / cyber insurance documentation · Device count / inventory · Employee count by role or location · Known projects, issues, or planned purchases

Evidence notes: Business-associate agreements were available for major vendors — a positive. Backup & recovery documentation and IT-side HIPAA control documentation were not available and are priority gaps. Whether staff use AI tools with PHI is currently unknown and should be assessed.

Renewal & contract calendar

RENEWAL	VENDOR	ROLE / COVERAGE
07/2026	MedTech Managed IT	Network, endpoint & help-desk support (BAA signed)
09/2026	ShieldCyber Insurance	Cyber liability (healthcare)
12/2026	ClearImage PACS (on-site)	Imaging & document storage
Annual 02/2027	CareChart EHR (cloud, BAA signed)	EHR & practice management
04/2027	Microsoft 365 (Business Standard, BAA signed)	Email, files, identity — 70 licenses
Unknown — contract not located	TwinCity Fiber	Internet & two-site connectivity

Next steps

1. Review this report with leadership and confirm the priorities.
2. Assign owners and target dates to the roadmap actions.
3. Decide where ongoing technology advisory support is appropriate.

Appendix — discovery responses

01 · Business & Tech Alignment

Does technology clearly support your business strategy?	Somewhat
Leadership visibility into technology	Limited
Confidence making technology decisions	Some
Is there a technology plan tied to business goals?	Informal

02 · Operations & Governance

Is ownership of systems and risks clear?	Partly
Is IT reactive or governed?	Mostly reactive
How are tech decisions made?	Informal
Leadership gets regular technology reporting?	Sometimes

03 · Systems & Workflows

How much do tools or workflows slow people down?	Somewhat
Are core systems integrated?	Some
Microsoft 365 used to its potential?	Basics only
Confidence in continuity if a key system fails	Low

04 · Vendor & Support

Is it clear who covers what for support?	Partly
Visibility into total technology spend	Limited
Are vendors aligned to business needs?	Somewhat
Awareness of upcoming contracts or renewals	Vague

05 · AI Readiness & Modernization

Are employees using AI tools today?	Unknown
AI acceptable-use policy?	None
Identified automation opportunities?	None
Is your data ready to support AI?	Some

How scoring works

Each answer maps to a 0–100 maturity value based on what it signals. Stage scores are the average of the answered, scored questions in that stage; the overall score is the average of assessed stages. Some questions are informational context and are not scored. Bands: Strategic 80+ · Governed 60+ · Developing 40+ · Reactive 20+ · Ad-hoc 0+.

Prepared by Endpoint Solutions for client leadership review. For the cleanest PDF, turn browser print dialog **Headers and footers** off.