2026 EDITION · MIDWEST OPERATORS

Cybersecurity Readiness Guide — 2026 Edition

A practical self-assessment for Midwest businesses and clinics.

Readiness is evidence you can show — MFA enrolled, a restore you actually ran, a name on the 2 a.m. call list — not a badge you can buy. This guide is a blunt checklist for owners and operators in the Lincoln and Omaha markets. Print it. Mark it. Fix the embarrassing gaps first.

SAINT TECHNOLOGY SERVICES · HICKMAN, NEBRASKA · VETERAN-OWNED

ONCE, IN WRITING

Educational only. This is not a compliance certification, legal opinion, or insurance binder. Auditors and OCR determine HIPAA outcomes. No client names appear in this document. SAINT does not sell — and no vendor meaningfully holds — a "HIPAA certified MSP" credential.

CONTEXT FOR OPERATORS

What changed in 2026

Two clocks are running. One is a proposed federal rule. The other is the questionnaire your cyber carrier already uses to bind or renew. They are converging. Waiting for "final" is how shops stay uninsurable.

> **Still proposed — not law.** HHS published the biggest HIPAA Security Rule overhaul in 20+ years as an NPRM in January 2025. It is still a proposal. The final rule has been pushed to 2027. Nothing in this section is a claim that the NPRM is in force, that SAINT certifies you, or that OCR has pre-approved anyone's stack.

What the proposal would require

If HHS finalizes along the lines of the NPRM, covered entities and business associates would be looking at a much less optional Security Rule:

01 Mandatory encryption of ePHI at rest and in transit — not "addressable."

02 MFA required. The old "addressable" off-ramp goes away.

03 Written asset inventory and a network map you can actually produce.

04 72-hour restore and incident-reporting expectations — tested, not theoretical.

05 Annual technical testing, not a policy PDF that nobody ran.

06 Tighter business-associate oversight. Your vendors are in scope with you.

"Addressable" goes away — the 240-day window is the pain

Under today's Security Rule, "addressable" is the word shops hide behind when MFA, encryption, or a restore test feels inconvenient. The NPRM would retire that dodge. Industry commentary has pointed to a 240-day post-final-rule implementation window. That is a painful sprint. Gradual work in 2026 is cheap by comparison. Panic-buying tools in year one of a final rule is not.

Cyber insurance already asks for most of this

Carriers in 2026 are not waiting on HHS. Before bind or renewal they already want evidence of MFA, EDR, tested and preferably immutable backups, and a written incident-response plan. The proposed Security Rule and the carrier questionnaire are lining up. If you cannot screenshot the control, the honest answer on the form is "no."

TWENTY BOXES · PRINT AND MARK

Seven things that actually matter

Count a box only if you can show it — a screenshot, a dated restore, a named owner. “We have a guy” is not a control.

01 Risk analysis & asset inventory NEW

- [ ] Written risk analysis exists and was reviewed in the last 12 months — not a binder from the last time someone asked.
- [ ] Inventory covers devices, cloud apps, and where business data / ePHI actually lives.
- [ ] A current network map exists. Guessing at VLAN 1 is not an inventory.

02 Identity & email

- [ ] MFA on every mailbox and admin account — including the owner who “hates extra steps.”
- [ ] No shared-mailbox daily logins. Forwarding rules reviewed this quarter.
- [ ] Same-day offboarding: disable the account, revoke sessions, pull tokens.
- [ ] Dual-control on bank and vendor-change requests. Phishing-resistant MFA (passkeys / FIDO2) for admins and anyone who can move money — SMS is phished routinely in 2026.

03 Endpoints & detection

> *“We’ll get to it” is how ransomware starts.*

- [ ] Managed EDR with ITDR / SIEM / SAT — Huntress *or* Guardz. Pick one stack and operate it. Do not treat Huntress as the backbone of every engagement if Guardz is the better fit.
- [ ] Critical patches on a tracked cadence, including internet-facing software.
- [ ] Admin accounts separated from daily email. Least privilege — not “everyone is a local admin.”

04 Backups & recovery

> *"OneDrive exists" is not a contingency plan.*

- [ ] 3-2-1 backups with an immutable or offline copy the same ransomware cannot encrypt.
- [ ] A restore has been tested in the last 90 days. A backup you have never restored is a rumor.
- [ ] Written RTO per system. Email, line-of-business, and cameras are not the same number.

05 Incident response NEW

- [ ] Written IR plan: roles, after-hours contacts, who calls the carrier and counsel.
- [ ] First-hour playbook (isolate, reset identity, check mailbox rules) that someone has actually opened.

06 Physical security

- [ ] Physical assessment completed *before* buying cameras or locks. Design the door someone will actually try.
- [ ] Cameras and access designed with IT — waiting rooms usually yes; counseling rooms and resident bedrooms usually no.
- [ ] Platform chosen to fit (Verkada, UniFi, or other). SAINT leads as consulting and project management, not box-pushing.

07 AI & automation · shadow-AI governance

- [ ] Shadow-AI inventory and an acceptable-use policy: Copilot, ChatGPT, browser extensions — what staff actually use.
- [ ] DLP / sharing baselines before anyone enables Copilot or Workspace AI on real data. A public chatbot on a leaky tenant is not "automation."

TWENTY CHECKBOXES

How to read your score

Count only the boxes you can evidence this week. Honesty here is cheaper than a claim file.

17–20 DEFENSIBLE	You can sit across from a carrier or an auditor without improvising. Keep testing restores and reviewing forwarding rules. Readiness decays.
10–16 GAPS	A carrier or OCR investigator would find these. Pick the gap that would embarrass you on a recorded call. Fix that first — usually MFA, EDR, or a restore you have never run.
0–9 EXPOSED	Ransomware groups are counting on you. Call before the incident — not after the mailbox rules have been forwarding for three weeks.

HIPAA-readiness (clinics and PHI-adjacent work)

Independent therapy practices, dental and chiropractic offices, and senior-living operators live under the HIPAA Security Rule with a fraction of a hospital IT staff. SAINT's language is deliberate:

- We implement HIPAA-aligned technical and administrative safeguards sized to the practice — not a hospital binder dropped on a three-provider clinic.
- A Business Associate Agreement (BAA) is required before we touch PHI-adjacent systems. That is standard, not a premium add-on.
- We package evidence (access reviews, MFA posture, backup tests, vendor list) you can hand an auditor or a carrier.
- No vendor is meaningfully "HIPAA certified" the way that phrase gets sold. OCR and your auditor decide outcomes — not a PDF watermark.

> **If a salesperson offers a "HIPAA certified MSP" sticker, treat it as marketing.** Ask for a BAA, MFA on email, a restore tested in the last 90 days, and who watches alerts at 2 a.m. Alignment is work. A certificate is a slide.

TALK TO SAINT

One team. Fixed monthly rate.

SAINT Management Group LLC, doing business as SAINT Technology Services. Veteran-owned. One team for IT, cybersecurity, physical security, and intelligent operations — not four vendors who do not talk to each other.

Headquarters is Hickman, Nebraska (city-level only — no street address in this guide). Lincoln and Omaha are service markets. There is no retail storefront. Remote coverage extends further; on-site work is scoped honestly.

Managed accounts get a **15-minute first-response target**. Assessments are a conversation, not a contract. If you want a second set of eyes on the boxes you could not check, start there.

Urgent: **531-625-2111**
Email: clientcare@saintsecured.com
Web: saintsecured.com
Book: calendly.com/colton-saintsecured

15 MINUTES

Book a 15-minute readiness conversation.

Open Calendly

LEGAL
SAINT Management Group LLC d/b/a SAINT Technology Services

OWNERSHIP
Veteran-owned. Founder-operated. No private-equity roll-up story.

MARKETS
Hickman HQ · Lincoln & Omaha service · no storefront

URGENT
Compromise, mailbox takeover, facility incident: 531-625-2111. Do not wait for a form.