

THREAT SENTRY
SECURITY

GRC AUDIT REPORT

THREAT SENTRY SECURITY

GRC Audit Report

HIPAA Security Rule Gap Assessment

Item	Detail
Client	Meridian Health Partners (fictional)
Engagement	GRC compliance audit
Assessment dates	5-23 May 2025
Report date	30 May 2025
Version	1.0 (Sample)
Prepared by	Threat Sentry Security

SAMPLE DOCUMENT. Meridian Health Partners is a fictional organization. All hosts, IP addresses, people, findings and scores are invented for demonstration and do not describe any real engagement, system or company.

CONFIDENTIAL - Client use only (sample)

1. Executive Summary

TSS assessed Meridian Health Partners' security program against the HIPAA Security Rule safeguards and mapped results to NIST CSF 2.0. Interviews, policy review and evidence sampling took place between 5 and 23 May 2025.

Overall compliance: 68% (Partially Compliant). MHP has strong physical safeguards and documented policies, but gaps in risk analysis, access reviews, vendor oversight and incident response testing must be closed before an external audit.

Safeguard area	Controls	Compliant	Partial	Gap	Score
Administrative	22	11	6	5	64%
Physical	10	8	2	0	90%
Technical	14	7	4	3	64%
Organizational / vendor	8	3	2	3	50%
Total	**54**	**29**	**14**	**11**	**68%**

2. Scope and Approach

Item	Detail
Frameworks	HIPAA Security Rule (45 CFR 164.308-316); NIST CSF 2.0 mapping
Scope	MHP corporate office, patient portal, scheduling system, 3 key vendors
Evidence	14 policies, 22 interviews, 40 evidence samples, access and log extracts
Rating scale	Compliant / Partial / Gap, plus maturity 1 (Initial) to 5 (Optimized)

3. Maturity by NIST CSF Function

Function	Current maturity	Target	Observation
Govern	2.5	3.5	Policies exist; risk ownership unclear
Identify	2.0	3.5	Asset inventory incomplete; no recent risk analysis
Protect	3.0	4.0	Good physical/technical controls; MFA partial
Detect	2.5	3.5	Logging present but not centrally reviewed
Respond	2.0	3.5	IR plan not tested in 18 months
Recover	2.5	3.5	Backups run; restores untested

4. Gap Register

ID	Control	Gap	Risk	Owner
G-01	Risk analysis (164.308(a)(1))	No enterprise risk analysis performed in 24 months	**High**	CISO
G-02	Access review (164.308(a)(4))	User access not reviewed; 14 terminated users still active	**High**	IT Director
G-03	Vendor management (164.308(b))	2 of 3 vendors lack signed BAAs	**High**	Compliance
G-04	Incident response (164.308(a)(6))	Plan not tested; no tabletop exercise	**Medium**	CISO
G-05	Audit controls (164.312(b))	Logs not centrally monitored	**Medium**	IT Director
G-06	Authentication (164.312(d))	MFA not enforced for remote admin	**Medium**	IT Director
G-07	Contingency plan (164.308(a)(7))	Backup restores not tested	**Medium**	Ops
G-08	Security awareness (164.308(a)(5))	Training completion at 71%	**Low**	HR

5. Key Observations

• **Strengths:** Clear policy library, effective physical access controls, encrypted laptops, engaged leadership.

• **Weaknesses:** Risk management is not a recurring process; vendor and access governance rely on manual, ad-hoc effort.

• **Audit exposure:** G-01, G-02 and G-03 would likely be cited as findings in a regulatory review.

6. Remediation Plan

Phase	Actions	Timeline
Phase 1: Quick wins	Sign missing BAAs; disable stale accounts; enforce MFA for remote admin (G-02, G-03, G-06)	0-30 days
Phase 2: Foundations	Conduct enterprise risk analysis; centralize log review; complete training (G-01, G-05, G-08)	30-90 days

Phase	Actions	Timeline
Phase 3: Resilience	Run IR tabletop; test backup restores; establish quarterly access reviews (G-04, G-07)	90-150 days

7. Audit-Readiness Notes

• Retain evidence of each remediation action with dates and approvers.

• Document the risk analysis methodology and risk register updates.

• Maintain a controls-to-evidence matrix for auditors.

• TSS recommends a follow-up readiness review after Phase 2.

8. Conclusion

MHP is positioned to reach substantial compliance within five months. Prioritizing risk analysis, access governance and vendor agreements will address the highest regulatory exposure and create a repeatable program.