Meridian Healthcare Group

Healthcare Services | 450 Employees | Tampa, FL | $62M Revenue

58
RISK SCORE
MEDIUM RISK

OSINT ASSESSMENT SUMMARY

External reconnaissance identified moderate credential exposure (143 records) primarily from historical breaches with no active infostealer infections detected. Email security is partially configured but DMARC is not enforcing, creating BEC risk. Attack surface is generally well-managed with minor issues. No undisclosed breach history detected. The applicant's questionnaire responses are largely consistent with external findings, with one discrepancy regarding MFA deployment.

UNDERWRITING RECOMMENDATION

BIND WITH CONDITIONS

DMARC remediation required within 60 days. Consider BEC sublimit reduction.

143	0	0	NONE	4	1
EXPOSED CREDS	INFOSTEALERS	PRIOR INCIDENTS	DMARC	CRITICAL CVES	DISCREPANCIES

QUESTIONNAIRE VALIDATION

1 Discrepancy

MFA enabled for all remote access?	DISCREPANCY	EDR deployed on endpoints?	VERIFIED
Email security gateway in place?	VERIFIED	Regular backups with offline copy?	VERIFIED
Security awareness training?	PARTIAL	Incident response plan documented?	VERIFIED

MFA Discrepancy: Applicant stated MFA is enabled for all remote access. External scan detected VPN endpoint (vpn.meridianhcg.com) allowing password-only authentication. Recommend clarification with applicant before binding.

CREDENTIAL EXPOSURE

143 Records

SOURCE	COUNT	RISK	UNDERWRITING NOTE
Breach Databases	112	MEDIUM	Historical breaches (LinkedIn, Adobe). Passwords are hashed. No evidence of recent compromise.
Combolist Exposure	31	LOW	Aggregated lists, likely from same historical sources. Standard exposure for company size.
Infostealer Logs	0	NONE	No active infostealer infections detected. Positive indicator of endpoint security.

PREMIUM IMPACT FACTORS

No infostealer infections	-10% Premium	DMARC not enforcing	+15% Premium
Healthcare industry	+20% Premium	No prior claims/incidents	-5% Premium
MFA discrepancy	+5% Premium	EDR deployed (verified)	-5% Premium

EMAIL SECURITY ANALYSIS

SPF	CONFIGURED	Properly restrictive (-all)
DKIM	CONFIGURED	Valid signatures detected
DMARC	p=none	Monitoring only, not enforcing

BEC Risk: DMARC is configured but not enforcing (p=none). Spoofed emails will be delivered. Given healthcare industry targeting, this increases social engineering/BEC risk.

ATTACK SURFACE SUMMARY

External Assets	23 discovered
Critical CVEs	4 (patching in progress)
Exposed RDP	0 (good)
Shadow IT	8 services detected

Positive: No exposed RDP or critical remote access issues beyond VPN MFA discrepancy. Attack surface is reasonable for company size.

BREACH & INCIDENT HISTORY

No Incidents Detected

CHECK	RESULT	DETAILS
Ransomware Leak Sites	CLEAR	No appearance on known ransomware leak sites
Dark Web Monitoring	CLEAR	No company data dumps or breach announcements detected
Regulatory Filings	CLEAR	No HHS breach notifications on file
News/Media Search	CLEAR	No public breach disclosures found

Underwriting Recommendations & Coverage Notes

- **Binding Condition:** Require DMARC enforcement (p=quarantine or p=reject) within 60 days of policy inception. Provide implementation guidance.
- **BEC Coverage:** Consider $250K sublimit for social engineering/funds transfer fraud given DMARC gap. Standard limit available upon DMARC remediation.
- **MFA Clarification:** Request written confirmation from applicant regarding VPN MFA configuration before binding. If password-only confirmed, require remediation within 30 days.
- **Healthcare Considerations:** PHI exposure increases regulatory and notification costs. Ensure adequate breach response coverage ($500K+ recommended).
- **Positive Factors:** No prior incidents, no infostealer infections, EDR deployed, reasonable attack surface management. These offset some risk factors.
- **Renewal Notes:** Re-assess DMARC status and credential exposure at renewal. Expect improvement in both areas.

UNDERWRITING DECISION: APPROVE WITH CONDITIONS

This applicant presents acceptable risk for binding with the conditions noted above. The absence of infostealer infections and prior incidents, combined with verified security controls (EDR, backups, IR plan), indicates a reasonable security posture. The DMARC gap and MFA discrepancy are addressable issues that should be remediation conditions rather than binding blockers.

Suggested Premium Adjustment: +20% from base rate (net of positive and negative factors). Re-evaluate at renewal based on remediation completion.