

MediCore Health Technologies

Enterprise Risk Assessment

A comprehensive security risk assessment covering 10 critical risks across five control domains, scored using NIST 800-30 methodology, mapped to NIST 800-53 and HIPAA requirements, and prioritized for executive action.

CONFIDENTIAL – EXECUTIVE DISTRIBUTION

FISCAL YEAR 2024



Made with GAMMA

Executive Summary

MediCore Health Technologies manages protected health information (PHI) for over 2 million patients across a distributed cloud and on-premises infrastructure. This assessment identifies **10 significant risks** spanning Access Control, Data Handling, Vendor Management, and Incident Response. Three risks are rated **Critical** and require immediate remediation to maintain HIPAA compliance and protect patient data.

10

Risks Identified

Across 5 control domains

3

Critical Severity

Requiring immediate action

5

High Severity

90-day remediation window

2

Moderate Severity

180-day remediation window

System Categorization — FIPS 199

Per FIPS 199 and NIST SP 800-60, MediCore's primary information systems are categorized based on the potential impact of a security breach on **confidentiality**, **integrity**, and **availability**. PHI systems are classified **HIGH** across all three security objectives, triggering the most stringent control baselines under NIST 800-53.

Information System	Confidentiality	Integrity	Availability	Overall Impact
Electronic Health Records (EHR)	HIGH	HIGH	HIGH	HIGH
Patient Portal & Telehealth	HIGH	HIGH	MEDIUM	HIGH
Billing & Claims Processing	MEDIUM	HIGH	MEDIUM	HIGH
HR & Workforce Systems	MEDIUM	MEDIUM	LOW	MEDIUM

 All HIGH-impact systems require NIST 800-53 High Baseline controls and are subject to HIPAA Security Rule requirements under 45 CFR §164.308 - 314.

Risk Scoring Methodology — NIST 800-30

Risks are scored using the NIST SP 800-30 **Likelihood × Impact** matrix. Likelihood reflects threat probability and vulnerability exposure; Impact measures harm to confidentiality, integrity, and availability. Composite scores determine prioritization for remediation.

Likelihood Scale

- **Very High (5):** Exploitable now, active threat
- **High (4):** Likely within 6 months
- **Moderate (3):** Possible within 1 year
- **Low (2):** Unlikely but plausible
- **Very Low (1):** Rare under current conditions

Impact Scale

- **Very High (5):** Catastrophic – regulatory action, major breach
- **High (4):** Severe – significant PHI exposure, fines
- **Moderate (3):** Noticeable – limited breach, reputational harm
- **Low (2):** Minor – contained, minimal patient impact
- **Very Low (1):** Negligible – no PHI exposure

Critical: 20–25

Immediate action required

High: 12–19

90-day remediation

Moderate: 5–11

180-day remediation

Low: 1–4

Accept or monitor

Enterprise Risk Register

All 10 identified risks scored and ranked by composite risk score. Critical and High-severity items require executive attention and documented remediation plans within defined timelines.

ID	Risk Description	Domain	Like.	Impact	Score	Severity
R-01	Privileged access without MFA	Access Control	4	5	20	Critical
R-02	PHI unencrypted at rest	Data Handling	3	5	15	Critical
R-03	No centralized SIEM / log monitoring	Incident Response	4	4	16	Critical
R-04	Vendor BAAs incomplete or expired	Vendor Mgmt	3	4	12	High
R-05	Legacy systems unpatched (90+ days)	Vulnerability Mgmt	4	3	12	High
R-06	Excessive user access privileges	Access Control	3	4	12	High
R-07	PHI transmitted over unencrypted channels	Data Handling	2	5	10	High
R-08	No tested incident response plan	Incident Response	3	3	9	High
R-09	Insecure mobile device access to EHR	Endpoint Security	3	3	9	High
R-10	Insufficient security awareness training	Workforce	3	2	6	Moderate

Access Control Risks

R-01

R-06

R-01: Privileged Access Without MFA

Score: 20 — Critical

Administrative and clinical users access EHR and network infrastructure without multi-factor authentication, exposing the environment to credential theft and lateral movement.

- **NIST 800-53:** IA-2, IA-3, AC-2
- **HIPAA:** §164.312(a)(2), §164.308(a)(5)
- **Remediation:** Enforce MFA for all privileged accounts within 30 days

R-06: Excessive User Access Privileges

Score: 12 — High

Role-based access controls are not enforced. Staff retain access beyond job function requirements, increasing insider threat and data exposure risk.

- **NIST 800-53:** AC-6, AC-3, AC-17
- **HIPAA:** §164.312(a)(1), §164.308(a)(4)
- **Remediation:** Implement least-privilege RBAC; quarterly access reviews



Data Handling Risks

R-02

R-07

R-02: PHI Unencrypted at Rest

Score: 15 — Critical

Multiple database instances storing PHI lack encryption at rest. A breach or theft would constitute a reportable HIPAA breach under the Breach Notification Rule.

- **NIST 800-53:** SC-28, SC-13
- **HIPAA:** §164.312(e)(2)(ii), §164.402-404
- **Remediation:** Enable AES-256 encryption on all PHI repositories within 60 days

R-07: PHI Transmitted Over Unencrypted Channels

Score: 10 — High

Internal APIs and legacy integrations transmit PHI over unencrypted HTTP. Network sniffing or man-in-the-middle attacks could expose patient records in transit.

- **NIST 800-53:** SC-8, SC-13
- **HIPAA:** §164.312(e)(1), §164.312(e)(2)(ii)
- **Remediation:** Enforce TLS 1.2+ on all PHI data flows; decommission HTTP endpoints

Vendor Management & Vulnerability Risks

R-04

R-05

R-04: Vendor BAAs Incomplete or Expired

Score: 12 — High

Seven of 22 business associates lack current Business Associate Agreements, creating HIPAA liability gaps. Vendor security posture is not assessed before onboarding.

- **NIST 800-53:** SA-9, SA-4, SR-11
- **HIPAA:** §164.308(b), §164.502(e), §164.504(e)
- **Remediation:** Execute BAAs with all vendors; implement vendor risk assessment program

R-05: Legacy Systems Unpatched 90+ Days

Score: 12 — High

Three legacy servers hosting clinical applications have not been patched in over 90 days, with multiple CVEs rated CVSS 9.0+ publicly disclosed and actively exploited.

- **NIST 800-53:** SI-2, CM-8, RA-5
- **HIPAA:** §164.308(a)(5)(ii)(B), §164.308(a)(8)
- **Remediation:** Patch immediately; establish 30-day critical patch SLA

Incident Response, Endpoint & Workforce Risks

R-03

R-08

R-09

R-10

R-03: No Centralized SIEM

16 — Critical

Logs are siloed with no correlation or alerting. Threats go undetected for extended periods.

NIST: AU-2, AU-6, SI-4 / HIPAA: §164.308(a)(5)(ii)(B)

R-08: No Tested IR Plan

9 — High

Incident response plan exists but has never been tested. Staff lack defined roles during a breach.

NIST: IR-2, IR-4, IR-6 / HIPAA: §164.308(a)(6)

R-09: Insecure Mobile EHR Access

9 — High

Clinicians access EHR on personal devices without MDM enforcement or remote wipe capability.

NIST: AC-17, AC-19, SC-28 / HIPAA: §164.312(a)(2)(iv)

R-10: Insufficient Security Training

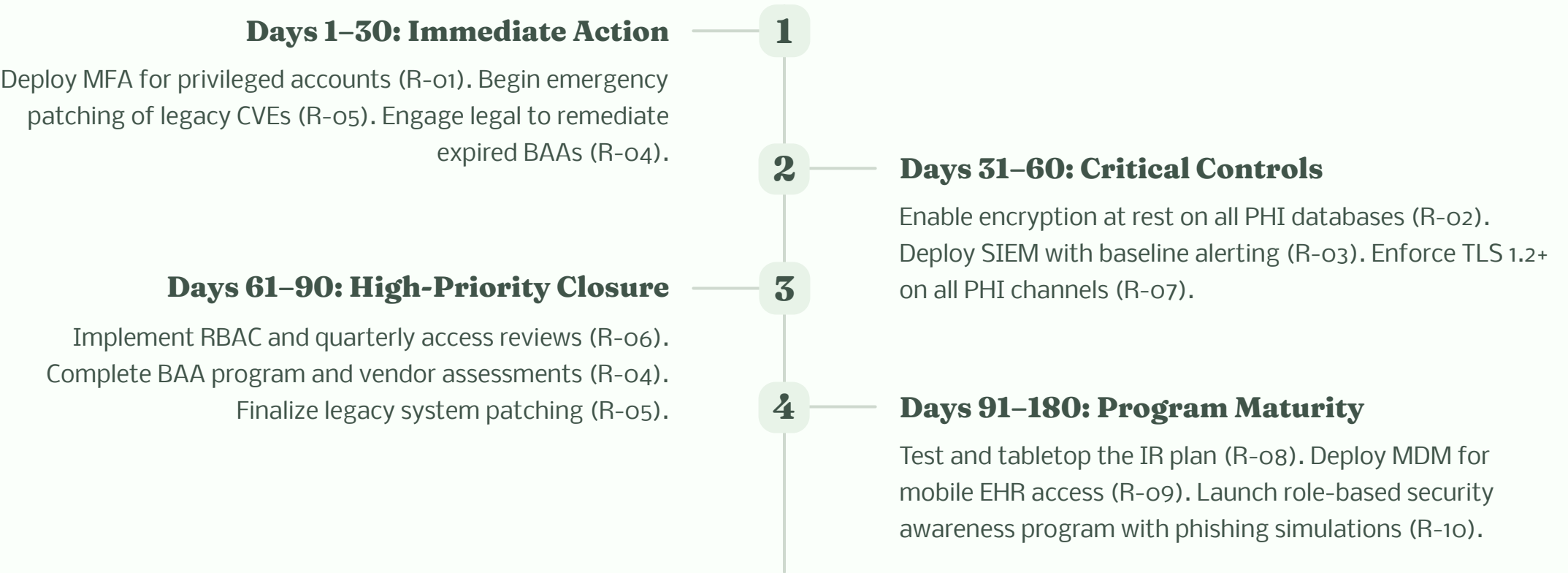
6 — Moderate

Annual training is generic and not role-based. Phishing simulation has never been conducted.

NIST: AT-2, AT-3 / HIPAA: §164.308(a)(5)(i)

Prioritized Remediation Roadmap

Remediation is sequenced by risk score, regulatory exposure, and implementation complexity. Critical items must begin immediately; all High-severity items must be resolved within 90 days.



✔ Successful completion of this roadmap will reduce MediCore's overall risk exposure by an estimated **70%** and achieve alignment with NIST 800-53 High Baseline and HIPAA Security Rule requirements.