YOUR MSP NAME

Executive Security & Compliance Report

Acme Healthcare Group

Report Period: April 1 – June 30, 2026

CONFIDENTIAL — Prepared exclusively for Acme Healthcare Group

Executive Summary

C+

72 / 100

▲ +8 points from last quarter

72	$1.2M	14	23
SECURITY SCORE	DOLLAR EXPOSURE	OPEN FINDINGS	REMEDIATED

Key Highlights

- ✅ MFA adoption improved from 67% to 94% across all users
- ✅ 23 remediation tasks completed since last assessment
- ✅ HIPAA readiness improved from 58% to 74%
- ⚠ 3 critical findings remain in access control category
- ⚠ 2 vendors rated high-risk require reassessment

Compliance Readiness

Framework	Readiness	Compliant	Gaps	Not Assessed	Status
HIPAA	74%	31	8	3	PARTIAL
SOC 2	68%	44	15	6	PARTIAL
PCI DSS	82%	38	6	2	GOOD
NIST CSF	71%	52	18	4	PARTIAL
CIS Controls v8	76%	28	7	2	PARTIAL

Critical Compliance Gaps

Framework	Requirement	Gap	Priority
HIPAA	Access Control (§164.312(a))	No automated access review process	CRITICAL
HIPAA	Audit Controls (§164.312(b))	Audit logs not centralized	HIGH
SOC 2	CC6.1 — Logical Access	Shared admin accounts detected	CRITICAL
SOC 2	CC7.2 — System Monitoring	No SIEM or centralized logging	HIGH
NIST	PR.AC-1 — Identity Management	No SSO for cloud applications	MEDIUM
CIS	Control 5 — Account Management	12 dormant accounts active >90 days	HIGH

Identity Security

94%	12	8	3
MFA ADOPTION	DORMANT ACCOUNTS	EXCESS ADMIN ACCOUNTS	EXTERNAL/GUEST USERS

Users Without MFA

User	Role	Last Login	Risk
j.martinez@acme.com	Finance Manager	2 days ago	CRITICAL
r.chen@acme.com	IT Admin	Today	CRITICAL
s.patel@acme.com	HR Director	5 days ago	HIGH

Vendor Risk Assessment

18	2	14
TOTAL VENDORS	HIGH RISK	ASSESSED

High-Risk Vendors Requiring Action

Vendor	Category	Risk Score	Issue	Action
CloudPayroll Inc.	HR / Payroll	82 — HIGH	No SOC 2 report provided	Request current SOC 2
QuickStore EHR	Healthcare SaaS	71 — HIGH	Encryption policy outdated	Reassess Q3 2026

Remediation Roadmap

Prioritized action plan based on risk severity and compliance impact.

PRIORITY 1 — CRITICAL

Eliminate shared admin accounts

Impact: SOC 2 CC6.1, HIPAA §164.312(a) | Effort: 4-8 hours | Due: Immediate

PRIORITY 2 — CRITICAL

Enforce MFA on remaining 3 users

Impact: All frameworks, identity security score | Effort: 1-2 hours | Due: Within 7 days

PRIORITY 3 — HIGH

Centralize audit logging

Impact: HIPAA §164.312(b), SOC 2 CC7.2, NIST DE.CM | Effort: 8-16 hours | Due: Within 30 days

PRIORITY 4 — HIGH

Disable 12 dormant accounts

Impact: CIS Control 5, identity attack surface | Effort: 2-4 hours | Due: Within 14 days

PRIORITY 5 — HIGH

Request SOC 2 report from CloudPayroll Inc.

Impact: Vendor risk, HIPAA business associate requirements | Effort: 1 hour | Due: Within 14 days

PRIORITY 6 — MEDIUM

Implement SSO for cloud applications

Impact: NIST PR.AC-1, SOC 2 CC6.1 | Effort: 16-24 hours | Due: Within 60 days

PRIORITY 7 — MEDIUM

Establish automated access review process

Impact: HIPAA §164.312(a), SOC 2 CC6.2 | Effort: 8-12 hours | Due: Within 60 days

Evidence Checklist

Evidence Item	Status	Last Collected
MFA enrollment report	COLLECTED	May 20, 2026

User access list	COLLECTED	May 20, 2026
Admin privilege audit	COLLECTED	May 20, 2026
Vendor risk assessments	PARTIAL	Apr 15, 2026
Security awareness training logs	MISSING	—
Incident response plan	COLLECTED	Mar 1, 2026
Business continuity plan	MISSING	—
Encryption configuration proof	COLLECTED	May 18, 2026

This report was generated automatically by Nuronus.

White-labeled reports carry your MSP brand — clients never see Nuronus.
Free for 2 clients at **nuronus.com**