HIPAA Compliance Audit Report

Organization: JKUAT Health Center (Simulated)

Auditor: Dickson Marienga, CISA, CISM, HIPAA Certified

Date: May 28, 2025

Scope: Technical and administrative controls under HIPAA Security Rule

Report Type: Internal Compliance Assessment

Tools Used: Manual checklist, NIST CSF, Nessus (for vulnerability scan)

# Executive Summary

This audit assesses the organization's compliance with HIPAA Security Rule requirements related to ePHI (electronic Protected Health Information). The assessment identified 3 critical, 4 moderate, and 5 low-risk issues that require remediation.

# Objectives

- Identify gaps in HIPAA technical safeguards  
- Verify access control mechanisms  
- Assess risk management program  
- Recommend corrective actions

# Methodology

- Interviewed IT/security staff  
- Reviewed network diagram and policies  
- Ran a vulnerability scan using Nessus  
- Compared practices with HIPAA 45 CFR §164.308, §164.310, §164.312

# Findings & Recommendations

## Incomplete Risk Analysis

Issue: Risk analysis is outdated (last done 2021).  
Risk: High  
Recommendation: Conduct annual risk assessments using NIST SP 800-30 framework.

## Shared Logins on EMR

Issue: Multiple nurses use one login.  
Risk: Medium  
Recommendation: Enforce unique user credentials and enable audit logs.

## Lack of Audit Logging

Issue: No log monitoring or centralized logging.  
Risk: High  
Recommendation: Implement centralized SIEM (e.g., Wazuh, Splunk Free) and retain logs for 6 years.

# Conclusion

The simulated audit has revealed compliance gaps that can expose the organization to regulatory and security risks. Immediate remediation is advised for high-risk issues. A follow-up audit is recommended in Q4 2025.