POA&M: Thebes Memorial Hospital EHR Security Gaps & Remediation Plan
System: Electronic Health Records Portal – Midtown Regional Hospital
Framework: NIST 800-53 | Alignment: Moderate Impact System

Identified Control Weaknesses

1. Weak Access Control (AC-2)

Description: User provisioning and deprovisioning are handled manually, resulting in delays in revoking access for terminated employees.
Planned Remediation: Implement automated identity lifecycle management integrated with HRIS.
Milestone 1: Select IAM vendor – **May 15, 2025**
Milestone 2: Complete pilot for HR-to-IT workflow – **June 15, 2025**
Milestone 3: Org-wide rollout and deactivation testing – **July 10, 2025**

2. Insufficient Audit Logging (AU-6)

Description: Application logs are only retained for 15 days, and fail to include admin activity trails.
Planned Remediation: Extend log retention to 90 days and configure logging of privileged user actions.
Milestone 1: Update logging configuration for EHR modules – **April 25, 2025**
Milestone 2: Deploy SIEM connector for log ingestion – **May 10, 2025**
Milestone 3: Validate alerting rules for admin activity – **May 20, 2025**

3. Data-at-Rest Not Fully Encrypted (SC-12)

Description: EHR backups stored on network drives lack full disk encryption.
Planned Remediation: Encrypt all backups using FIPS 140-2 validated tools.
Milestone 1: Inventory all backup volumes – **April 22, 2025**
Milestone 2: Apply encryption policies – **May 5, 2025**
Milestone 3: Complete encryption key management review – **May 12, 2025**

Overall Risk Summary

These vulnerabilities pose a significant threat to PHI confidentiality and system trustworthiness. Remediation is prioritized over a 60–90 day window. Project overseen by the Information Security Officer (ISO) in coordination with IT and compliance.

Prepared for internal security review and stakeholder presentation. Document Owner: Jasmine Alexander, Cybersecurity & GRC Analyst