**HIPAA Risk Assessment Report**

**Prepared by:** Adefolaji Fasanya **Date:** 04/16/2025 **Organization:** Harborview Medical Partners

**Executive Summary**

This HIPAA Risk Assessment evaluates the risks and vulnerabilities affecting the confidentiality, integrity, and availability of electronic protected health information (ePHI) at Harborview Medical Partners, a multi-site healthcare provider serving over 15,000 patients annually in the Baltimore area. This assessment is conducted in accordance with the HIPAA Security Rule and is mapped to the NIST Cybersecurity Framework (CSF).

Despite the presence of several foundational security controls, significant gaps remain — particularly in areas involving user access, email security, third-party risk, and patch management. These weaknesses introduce regulatory, reputational, and operational risks that must be addressed urgently.

**Scope**

This assessment covers Harborview’s key information systems and processes responsible for storing, transmitting, or processing ePHI, including:

* Electronic Health Records (EHR) system (MedSys EMR)
* Internal network infrastructure (LAN/WAN)
* Employee workstations and shared terminals
* Mobile devices (physician iPads, remote nursing laptops)
* Remote access portals for on-call physicians
* Third-party vendors involved in claims processing, medical imaging, and telehealth services

**Methodology**

To complete this assessment, the following methods were employed:

* Staff Interviews: Department heads, IT administrators, and compliance officers were interviewed regarding access controls, vendor management, and incident response.
* Policy Review: Security policies, password standards, and data retention procedures were analyzed for HIPAA alignment.
* Technical Scans: Vulnerability scans were conducted on internal assets using Nessus Essentials and Microsoft Baseline Security Analyzer.
* Audit Log Review: SIEM and access control logs were reviewed for anomalies and shared account usage.

**Findings & Risk Levels**

| **Risk Area** | **Description** | **Likelihood** | **Impact** | **Risk Level (L×I)** | **Controls in Place** | **Recommendations** |
| --- | --- | --- | --- | --- | --- | --- |
| *Access Control* | Shared generic login credentials on nursing stations | Medium | High | Medium-High | Password policies, MFA on admin tools | Enforce unique user IDs; apply MFA on all endpoints |
| *Data Transmission* | Use of unencrypted email for sending lab results | High | High | Critical | VPN used for remote staff | Implement email encryption and DLP tools |
| *Vendor Management* | No formal security vetting of third-party vendors | Medium | Medium | Medium | Contracts require HIPAA clauses | Introduce vendor security risk assessments |
| *Patch Management* | Lags in critical patching on imaging machines | Medium | High | Medium-High | Manual patch cycles (monthly) | Automate patching; prioritize vulnerable systems |

**Conclusion**

Harborview Medical Partners has made key investments in cybersecurity, but gaps remain that could lead to unauthorized disclosure or loss of sensitive patient data. In particular, unsecured communication channels, shared accounts, and vendor risk management pose material threats to HIPAA compliance.

Immediate remediation should focus on enforcing user accountability, encrypting communications, and formalizing vendor assessments. These measures will not only enhance patient data protection but also position Harborview more favorably during regulatory audits or cyber insurance evaluations.

**Appendix**

* Mapping of risks to NIST CSF categories
* Detailed Nessus vulnerability scan results
* Summary of interview findings
* Example vendor risk evaluation form (draft)