Vendor Risk Assessment Report
Vendor: MedPay Solutions (Mock Payment Processor)
System: Integrated Billing Module for Thebes Memorial Hospital EHR
Prepared by: Jasmine Alexander, Cybersecurity & GRC Analyst

Security Questionnaire Overview

Below is a high-level assessment of MedPay Solutions, a third-party payment processing vendor that integrates directly with the hospital's electronic billing system. This vendor processes personally identifiable information (PII), protected health information (PHI), and payment card data (PCI).

Vendor Security Questionnaire Snapshot:

Category	Question	Response
Data Handling	Does the vendor encrypt PHI and PCI data at rest and in transit?	Yes, using AES-256 and TLS 1.2+
Access Control	Are user roles reviewed and access revoked upon termination?	Yes, reviewed quarterly
Incident Response	Does the vendor have an IRP and breach notification protocol?	Yes, within 48 hours of detection
Third-Party Sharing	Does the vendor share data with sub-processors?	Yes, with contractual agreements and risk assessments
Compliance	Is the vendor compliant with HIPAA and PCI-DSS?	Yes, latest audit: Q3 2024
Business Continuity	Is there a documented BCP/DRP in place?	Yes, tested bi-annually
Audit & Oversight	Are independent security assessments conducted?	Yes, annual SOC 2 Type II audit

Risk Summary & Recommendations

Overall Risk Level: *Moderate*
While MedPay meets most standard requirements, there are two areas that require improvement:

1. **Sub-Processor Transparency:** Contracts exist, but full audit logs for sub-processors are not currently shared.

2. **IR Notification Window:** A 48-hour breach notification SLA is acceptable but should ideally align with internal 24-hour expectations.

Recommendations:

- Request annual sub-processor transparency reports or SOC 2 summaries.
- Amend service-level agreement (SLA) to include a 24-hour initial breach notification for critical data.

This assessment supports vendor onboarding, risk classification, and compliance planning.