System Categorization Report – FIPS 199
System: Electronic Health Records Portal – Midtown Regional Hospital
Prepared by: Jasmine Alexander, Cybersecurity & GRC Analyst

Overview

This report provides a system categorization based on the Federal Information Processing Standards Publication 199 (FIPS 199) for the Electronic Health Records (EHR) Portal used by Thebes Memorial Hospital. The purpose of this categorization is to determine the potential impact levels to security objectives (Confidentiality, Integrity, and Availability) in the event of a breach, compromise, or failure.

Security Objectives & Impact Levels

Security Objective	Impact Level	Justification
Confidentiality	**High**	The EHR contains Protected Health Information (PHI), personal identifiers, and sensitive patient records. A breach would cause significant harm to patients, legal liability, and regulatory penalties under HIPAA.
Integrity	**Moderate**	Inaccurate or tampered medical data could lead to misdiagnosis or incorrect treatment, but compensating controls (e.g., medical verification procedures) are in place.
Availability	**High**	Timely access to patient data is critical for emergency and ongoing care. Downtime could result in delayed treatment or loss of life.

System Categorization Summary

Based on the highest individual impact level across all three objectives, the overall **system impact level is categorized as HIGH** under FIPS 199.

This classification mandates heightened control measures for confidentiality and availability, along with consistent integrity protections to maintain trustworthiness of clinical data.

For internal security classification and continuous monitoring planning.