MIS582-Module 3: Case Study Assignment

Loyal improves data protection, platform performance with Always Encrypted with secure enclaves for Azure SQL Database

[redacted]

DeVry University, Keller Grad

Prof. Dr. Anas Bayan

Due Date

Introduction

In a healthcare landscape increasingly dominated by data, protecting patient information is not only a legal requirement under the Health Insurance Portability and Accountability Act (HIPAA) it's also essential to keeping trust with the public. As I dug into Loyal, the case study on their work with Microsoft Azure, I began to appreciate even more how strategic database design and architecture can drive not just compliance but real operational benefit. Loyal's use of FHIR demonstrates how a well-architected data infrastructure with a foundation of encryption, secure enclaves, and cloud-native technologies can safeguard sensitive health information while allowing real-time engagement and analytics. In this article, we'll look at what Loyal has done to implement their database, start with the constraints and parameters for compliance, move along to understand and review the architecture and data flow, and finally evaluate security requirements to ensure that we are aware what it takes to keep the system secure.

1. Identify and analyze the database implementation

When I looked at Loyal's approach to implementing a database, I found I liked Azure SQL Database with Always Encrypted with secure enclaves. This solution is a good indication of moving towards a more modern, cloud-native architecture that values scalability and extremely rigorous data protection. As Loyal is in the healthcare space, and therefore needs to