Rafael Cervantes

01/23/2025

Developing a Cloud Security Plan

Company: HealthNet Solutions

industry : Healthcare

Size: Medium-sized company with about 500 employees

The infrastructure as a Service (IaaS) is the best suitable cloud model for the HealthNet Solutions.The Infrastructure as a Service (IaaS) lets the company take advantage of the flexibility and cost efficiency of the cloud, while having control over their operating system and software stack. This cloud model aligns with the requirement to manage sensitive healthcare data compliance with HIPAA regulations. The deployment most suitable for HealthNet Solutions is the hybrid cloud. The hybrid cloud allows HealthNet Solutions to keep sensitive records on a private cloud while using the flexibility and cost efficiency of public cloud tools for less sensitive operations.

It is critical to enforce the principle of least privilege to guarantee that only authorized personnel have access to sensitive data. Multi-Factor Authentication (MFA) helps enhance security, compliance, protects sensitive data and increases trust. Multi-Factor Authentication (MFA) requires users to provide two or more verification factors to access a system or account. Role-Based Access Control (RBAC) enforces permission based on users roles.This improves security, scalability, least privilege principle and simplifies management. Using Audit Trails helps document the activities

and events in a system or applications. Using Audit Trails helps data integrity, forensic investigation and accountability.

Using Data at Rest helps encrypt sensitive data such as patient records both in the private and public cloud. Data at Rest helps insider threats, data integrity and prevention of data breaches. Using Data in Transit, encrypts data during transmission across the networks. Data in Transit helps protect against man-in-the-middle attacks. Using Azure key Vaults helps safeguard sensitive data, certificates, passwords and encryption keys. This helps with scalability, reduces risk of data exposure, simplifies key rotation backup and recovery.

Virtual Private Cloud (VPC) is a private section of a public cloud. Google Cloud is a Virtual Private Cloud (VPC) that uses public and private subnets, security groups, VPN, and internet gateways. This helps with scalability, simplifies network management, private connections, isolation and security. Using a VPN helps secure communications between local data centers and the cloud. Google Cloud comes with a VPN, there is no need to get another VPN. Using cloud native firewalls like Azure Network Security Groups helps with security management, real time monitoring, enhanced compliance, zero trust security model, and restricting inbound and outbound traffic to only trusted sources.

Incident Response Plan (IRP) is a plan outlining the procedure for detecting, responding and recovering from a security incident. HealthNet Solutions should use both Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Intrusion Detection System (IDS) monitors network traffic and system activities for suspicious

behavior and alerts the security teams. Intrusion Detection System (IDS) helps with early threat detection, and non intrusive monitoring. Intrusion Prevention System (IPS) detects suspicious activity and blocks it to prevent threats in real time. This helps with compliance, real time blocking, prevention of ransomware and malware. Containment helps with isolating any compromised systems and preventing attackers from advancing. Once the incident is eradicated the recovery plan starts and systems are restored from clean backups. The company should communicate the incident to stakeholders, media and regulatory bodies like HIPAA.

Ensuring that all cloud services used are HIPAA compliant and provide the protection for Protected Health Information (PHI). Data residency should comply with the regulatory requirements within the geographic location. Proving audits and reports on the cloud environments to ensure ongoing compliance with HIPAA and other healthcare regulations.

Azure Monitoring collects logs from all cloud resources and applications. Azure Monitoring helps with comprehensive visibility, issue detection, alerts, end to end monitoring, security and compliance. Setting up a 24/7 monitoring system like Azure Security center that helps with threat protection, detection advance data security, in real time. Splunk is a Security information and event Management (SIEM) that is designed to collect, and analyze big data in real time. Splunk has machine learning tools for detection, analytics and automated decision making, preventing potential security threats, learning from past incidents, and taking action before issues arise. Penetration testing and

vulnerability scanning should be conducted regularly to prevent attackers from exploiting them.

Security Plan

1. Cloud Service and Deployment Models
    a. IaaS for flexibility and control
    b. Hybrid Cloud for separating sensitive data in a private cloud and public for non sensitive
2. Identity and Access Management
    a. Multi-factor authentication
    b. Role based access control
    c. Audit Trails
3. Data Protection
    a. Encryption, Data at Rest and Data in Transit
    b. Azure Key Vault - secure key management
4. Network Security
    a. Google Cloud (VPC)
    b. Azure Network Security Groups - firewalls and security Groups
    c. Google Cloud (VPN)
5. Incident Response
    a. Detection (IDS/IPS)
    b. Containment
    c. Eradication and Recovery

    d. Communication
        i. HIPAA (regulatories organizations)
        ii. Stakeholders
        iii. Media
6. Compliance and Governance
    a. HIPAA compliance
    b. Data Residency and Sovereignty
    c. Auditing and Reporting
7. Security Monitoring
    a. Azure Monitor - Centralized Logging
    b. Azure Security Center - Continuous monitoring
    c. Splunk (SIEM)
    d. Penetration testing and vulnerability scanning