INFO 7374 - Cybersecurity Audit and Compliance
Week 10 - Assignment 9

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Section 1: Trust Services Criteria (TSC)

1. **Key Controls for Trust Services Criteria (TSC)**
   To meet the **Trust Services Criteria (TSC)**, HealthCloud should implement the following key controls:
   a) **Security (Mandatory Criteria)**
      - Implement multi-factor authentication (MFA) to allow user access to EHR Systems.
      - Use encryption (AES-256) for data at rest and in transit.
      - Perform regular penetration testing and vulnerability assessments.

   b) **Availability**
      - Deploy redundant cloud infrastructure with automatic failover capabilities.
      - Implement disaster recovery (DR) and business continuity planning (BCP), and conduct periodic tests that provide evidence of the establishment of your plans.
      - Establish real-time system health monitoring and alerts.

   c) **Confidentiality**
      - Use role-based access control (RBAC) to permit access to sensitive data only to personnel with a need to know and are appropriately trained and qualified.
      - Create and conduct periodic access reviews and audits.
      - Enfine data masking where non-essential users are permitted to access patient records.

2. **Why Security is Mandatory for SOC 2 and Its Alignment with HIPAA**
   SOC 2 is built upon security which applies to all other trust service criteria. Security ensures that private patient information is protected from unauthorized access, which overlaps with HIPAA's Security Rule.
   - HIPAA's Administrative Safeguards - These require risk management and employee training which align with SOC 2 security controls.
   - HIPAA's Technical Safeguards - These require encryption, access controls, and audit logs, which encapsulated in SOC 2's security criteria. SOC 2 security controls would be a way for HealthCloud to satisfy HIPAA and SOC 2 security criteria at the same time.

INFO 7374 - Cybersecurity Audit and Compliance
Week 10 - Assignment 9

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Section 2: HIPAA Integration

1. **Integrating HIPAA Requirements into SOC 2 Compliance**

   HealthCloud can integrate **HIPAA and SOC 2** compliance through shared controls:

HIPAA Requirement	SOC 2 Equivalent Control	Example
Access Control (Technical Safeguard)	Logical Access Controls	Role-based access, MFA
Audit Controls (Technical Safeguard)	Logging & Monitoring	SIEM tools for real-time log monitoring
Data Encryption	Data Confidentiality Controls	AES-256 encryption for data at rest and in transit
Risk Management Program	Security Controls	Regular risk assessments & penetration testing

2. **Challenges of Integrating HIPAA and SOC 2 & Mitigation Strategies**

Challenges	Mitigation Strategies
Different Focus Areas (SOC 2 is broader, HIPAA is healthcare-specific)	Use a Unified Compliance Framework (UCF) that maps control both frameworks.
Continuous Monitoring Overhead	Implement automated compliance tools (e.g., Drata, Vanta).
Varying Reporting Requirements	Prepare both internal SOC 2 reports and HIPAA compliance documentation.

INFO 7374 - Cybersecurity Audit and Compliance
Week 10 - Assignment 9

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Section 3: Continuous Improvement

1. **Steps to Maintain Compliance as HealthCloud Develops:**
   - Automate compliance processes using GRC (Governance, Risk, Compliance) tools.
   - Implement a Compliance Officer role to manage regulatory compliance.
   - Develop a vendor risk management program to oversee third-party compliance.
   - Conduct semi-annual internal audits for SOC 2 and HIPAA compliance before the external SOC 2 audit.
2. **Continuous Monitoring for ComplianceLogging and Event Monitoring:**
   - Use a SIEM tool (for example, Splunk, or AWS CloudTrail) to identify anomalies.
   - Automating Compliance Dashboards: Use automated report generation to report real-time for SOC 2, SOC 3, and HIPAA audits.
   - Employee Training: Conduct semi-annual security awareness training for all employees.
   - Third-Party Risk Assessment: Regularly assess cloud service providers AWS, Azure and GCP.

INFO 7374 - Cybersecurity Audit and Compliance
Week 10 - Assignment 9

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Section 4: Risk Management

1. Key Risks HealthCloud Faces

Risk	**Impact**
Data Breaches	Exposure of sensitive patient data, regulatory fines
Non-Compliance with HIPAA or SOC 2	Legal penalties, loss of client trust
Insider Threats	Unauthorized access by employees
Ransomware Attacks	System downtime, data loss
Vendor Security Gaps	Third-party vulnerabilities affecting HealthCloud

2. Risk Management Framework & Mitigation Strategies

Risk Management Component	**Mitigation Strategy**
Risk Assessment	Conduct annual risk assessments using NIST frameworks.
Access Management	Implement Zero Trust Architecture (ZTA) for enhanced security.
Incident Response	Develop and test an Incident Response Plane (IRP).
Vendor Management	Require SOC 2 Type II reports from third-party providers.

INFO 7374 - Cybersecurity Audit and Compliance
Week 10 - Assignment 9

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

Section 5: Incident Response

1. Key Components of HealthCloud's Incident Response Plan

- Preparation: Employee security training, penetration testing, and IRP documentation.
- Detection & Analysis: Real-time intrusion detection systems (IDS) and log monitoring.
- Containment & Eradication: Isolate affected systems and remove threats.
- Recovery: Restore from secure backups, validate data integrity.
- Lessons Learned: Conduct post-incident review and update policies.

2. Aligning the Incident Response Plan with SOC 2 and HIPAA

- SOC 2 Alignment: Implement continuous security monitoring and auditable logs.
- HIPAA Alignment: Report breaches within 60 days, as per HIPAA's Breach Notification Rule.
- Unified Strategy: Develop a single incident response team to handle both SOC 2 and HIPAA events.