INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

1. Risk Assessment

- **Potential Compliance Risks:**
    - *HIPAA*: Risks include unauthorized access to patient data, data breaches, failure to encrypt sensitive information, and inadequate employee training on data privacy.
    - *SOX*: Risks involve inaccurate financial reporting, lack of internal controls, insufficient documentation of financial processes, and cybersecurity vulnerabilities impacting financial systems**.**
- **Risk Analysis:**
    - Assess risks based on likelihood and impact. For example:
        - Data breaches (High likelihood, High impact).
        - Failure to document financial controls (Medium likelihood, High impact).
        - Employee non-compliance with policies (Medium likelihood, Medium impact).
- **Risk Matrix:**

Risk Description	Likelihood	Impact	Priority
Data breaches	High	High	High
Inadequate financial documentation	Medium	High	High
Employee non-compliance	Medium	Medium	Medium

2. Regulatory Mapping

- HIPAA Compliance Requirements:

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

  - Ensure the confidentiality, integrity, and availability of protected health information (PHI).
  - Implement administrative, physical, and technical safeguards.
  - Conduct regular risk assessments and maintain breach notification protocols**.**

- **SOX Compliance Requirements:**
  - Establish and maintain internal controls for financial reporting.
  - Conduct regular audits to ensure accuracy in financial statements.
  - Certify compliance with SOX requirements through management and external auditors.

3. Governance Structure

- **Governance Framework:**
  - Form a Compliance Committee responsible for overseeing HIPAA and SOX compliance.
  - Define roles such as:
    - *Compliance Lead*: Oversees overall compliance efforts.
    - *Data Privacy Officer*: Focuses on HIPAA-related requirements.
    - *Internal Auditor*: Ensures SOX compliance through audits.
    - *IT Security Manager*: Manages cybersecurity risks.
- Establish reporting lines to ensure accountability.

4. POLICIES AND CONTROLS

A. **Data Security Policy (HIPAA)**

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- Access Control: Implement role-based access controls (RBAC) to limit patient health information (PHI) access.
- Encryption: Require PHI encryption at rest and in transit.
- Incident Management: Define incident reporting, investigation, and data breach mitigation processes.
- Data Retention and Disposal: Establish standards for proper storage and secure disposal of PHI.
- Third-Party Compliance: Require vendors dealing with PHI to sign Business Associate Agreements (BAAs).

B. **Financial Controls Policy (SOX)**

- Internal Audits: Periodic audits to assure differential integrity in finances and internal controls.
- Separation of Duties: Duties have been separated to prevent loss or fraud.
- Data Integrity: The financial report should use version control to prevent unauthorized changes.
- Documentation Standards: All transactions and controls have been adequately documented.

C. **Incident Response Policy**

- Identification & Reporting: Procedures should be developed for security incidents reported by employees to the IT Security team within 24 hours of detection.
- Incident Classification: Severity levels and response actions should be defined based upon the type of incident.
- Containment & Mitigation: Protocol to control the affected systems and minimize damage resulting from information exposure.
- Recovery & Post-Incident Review: Data recovery after the incident and ensure completeness of review.

D. **Employee Conduct Policy**

- Code of Ethics: Employees answerable for reporting confidential matters or violations.
- Training Requirements: Regular training on HIPAA and SOX compliance.

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- Whistleblower Protection: Means by which employees can anonymously report complaints.

Automated Compliance and Security Controls

1. Automated Compliance Checks
Access logs are checked by means of compliance software using various features in detecting anomalies and flagging security risks threatening the organization.
Automated alerts notify administrators about unusual access patterns or unauthorized modifications.

2. Multi-Factor Authentication (MFA)
MFA must be enabled for sensitive systems or financial communication to boost security provisions.
Strong authentication mechanisms, otherwise known as biometric verification or time-based one-time passwords (TOTP) are required.

3. Audit Trails
All transactions must maintain an auditable history of structured client and financial information that contains a complete history of access, modifications, and activities associated with PHI and financial records.

4. Regular Penetration Testing
Conduct simulated cyberattacks to discover weaknesses and correct them to strengthen the defenses against intruders.
Testing consists of a classic checklist that includes a network test, application testing, and a social engineerable test to build a protective wall against vulnerability attempts.

5. Access Controls
Implement Role-Based Access Control (RBAC) to those who are responsible for the sensitive healthcare and financial data systems.

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

User access is basically limited to functions they perform, which minimizes unnecessary access or exposure levels that some might access otherwise.

6. Data Encryption
Industry-standard encryption must be utilized for all PHI and financial data, both at rest and in transit.
Secure key management practices are enforced to stay out of the unauthorized decryption route.

7. Change Management
Change management should be a formal process enabling the relevant process for IT systems and their financial controls.
Ensure proper testing and approval procedures before the change is implemented in the system should take place.

8. Regular Audits
A HIPAA and SOX compliance audit is performed internally and externally every year.
The audit result is reviewed, and measures taken intending to fix compliance gaps identified during the review.

Through the application of these security compliance tools, Wellcare can enhance data protection, reduce risks, and ensure they remain compliant with both HIPAA and SOX requirements.

5. TRAINING AND AWARENESS PROGRAM

Introductory Compliance

- Brief overview of HIPPA and SOX regulations

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- The importance of compliance in healthcare and financial reporting

HIPAA Compliance Training

- Dealing with Protected Health Information (PHI) and (Electronic Protected Health Information) ePHI
- The rights of the patients and best practices to secure data
- Common HIPAA violations and how to avoid them

SOX Compliance Training

- The requirements for financial reporting
- Internal control and fraud prevention
- Pre-qualification activities and documentation requirements

Incident Response and Reporting

- Identifying and taking action concerning security incidents
- Role-specific duties during an incident

Ethics and Code of Conduct

- Whistleblower protection and misconduct reporting
- Consequences of non-compliance

Continuous Learning Methods

Quarterly Webinars and Workshops: Keep employees up to date with today's knowledge on regulatory modifications.
Training Modules: Self-paced courses with interactive scenarios.
Phishing Simulations: Employee awareness of threat actors' cyber capability.
Annual Recertification Assessments: Employees must take certain outcomes.

Periodic Assessments

- Annual mandatory compliance quiz for all employees
- Department-specific compliance assessments based on job roles
- Simulated phishing exercises to test employee awareness

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

6. MONITORING AND REPORTING

Continuous Monitoring of the Compliance Department and Internal Audits

- Automated System Monitoring: Tools will be employed for real-time access pattern, data, and system change monitoring for PHI and financial data.
- HIPAA Audits: Conduct weekly reviews of access logs, data handling practices, and law compliance.
- SOX Audits: Conduct quarterly internal audits of financial statements, controls, and reporting systems.
- Regular Testing of Controls: Testing of key HIPAA and SOX controls for effective operation every quarter.
- Risk-Based Audit Approach: An audit will investigate risk levels using the base: risk assessments, historical findings, and emerging threats.
- Process Walkthrough: Walkthrough key business and IT processes to ensure compliance with HIPAA and SOX policies.
- Data Analysis: Use analytical tools to look for deviations or patterns that could be grounds for the compliance risks.
- Third-Party Assessment: Engage external auditors to complete an annual assessment of compliance status and suggest improvements.

Mechanisms of Reporting

- Compliance Dashboard: Develop a real-time dashboard for compliant metrics and status updates for executives.
- Incident Reporting System: Set-up a central incident reporting system for employees.
- Quarterly Reports for the Management: Reports comprehensive to the management, detailing the audit findings, updates on policies, and corrective actions.
- On Board Briefings: Presentation to the senior leadership about high-risk compliance concerns and major regulatory updates to support key strategic decisions.

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- Annual Compliance Review: Full review of external HIPAA and SOX compliance efforts, including audit results and planned action items for compliance improvement.

7. COMPLIANCE METRICS AND KPIS

Key Performance Indicators (KPIs)

- The Percentage of Employees Trained: 100% as target of compliance training.
- Incident Response Time: Monitoring the average time spent on detection, containment, and resolution of compliance incidents.
- Access Control Violations: Reports of attempts to gain unauthorized access to sensitive data.
- Data Breach Incidents: Keeping track of both the number and severity of security incidents occurring in the respective quarter.
- Accuracy of Financial Reporting: Reporting freedom from material misstatements in the financial statements.
- Internal Audit Reports Deficiencies: Identifying and keeping track of the findings of deficiencies that are issued in compliance audits.
- Control Effectiveness Score: Rating criterion for security and financial control assigned between 1 and 10 in accordance with audit outcomes.
- Audit Findings Closure Rate: Rate of the audit findings that have been fully resolved within the agreed time.

Compliance Performance Metrics

- Number of Reported HIPAA Violations: Number of HIPAA-related incidents and/or near-misses.
- SOX Control Deficiencies: The identified number of control deficiencies arising during the audit.

INFO 7374 - Cybersecurity Audit and Compliance
Week 5 Assignment

Group Members:
Krisha Lakhani – 002334794
Nisarg Sheth - 002308269

- Response Time to Detect: Time from identification of the compliance violations security incidents.
- Financial Restatements: Amount of re-reported financial statements due to compliance issues.
- Percentage of Policy Acknowledgment: Number of employees that have acknowledged compliance policies.
- Ratio of Compliance Cost: Compliance costs over total operational expenditure.
- Results of external audits: Performance detailed in terms of external HIPAA and SOX audit ratings.
- Results of the Employee Compliance Survey: Evaluation on employees' understanding and perception of their compliance requirements.