Identifying compliance risks associated with Wellcare's operations under HIPAA and SOX

Introduction:
As Wellcare expands internationally, the organization must comply with HIPAA to protect patient health information and SOX to ensure strong internal financial controls. Expansion brings additional complexity due to cross-border data flows, multiple vendors, and varying regulatory landscapes. The following assessment identifies and prioritizes key compliance risks

Risk Assessment and Risk Analysis Matrix

Potential Compliance risks associated with Wellcare operations under HIPAA and SOX

A. HIPAA Potential Risks and Risk Analysis Matrix

Category	Risk	Impact	Likelihood	Impact	Priority
Data Security / Access Control	Unauthorized access to PHI by internal or external users	Regulatory fines, lawsuits, reputational damage	High	High	P1
Data Security / Encryption	Unencrypted PHI transmission or storage	Data breach, privacy violations, breach notification requirements	High	High	P1
Breach Management	Delayed breach detection or notification	Regulatory penalties, patient mistrust	Low	High	P2
Vendor / Third- Party Risk	Missing or weak Business Associate Agreements (BAAs)	Shared liability, loss of compliance with HIPAA	High	Medium	P2
International Data Transfers	Cross-border PHI transfers conflicting with GDPR	Dual regulatory exposure, large fines	Medium	High	P2

B. SOX Potential Risks and Risk Analysis Matrix

Category	Risk	Impact	Likelihood	Impact	Priority
Cybersecurity	Ransomware/ malware attacks	System downtime, data loss, corrupted financial records, inability to report	Medium	High	P1
Change Management	Unauthorized system changes	Data corruption, inaccurate reporting, control failures	High	High	P1
Financial Reporting / Controls	Inadequate segregation of duties	Fraud risk, inaccurate reporting	High	High	P1
IT General Controls	Unauthorized changes to financial systems	Data integrity loss	Medium	High	P1
Regulatory	Missing CEO/CFO certifications	Non- compliance penalties	Medium	High	P1
Financial Systems	No backup verification process	Data loss, inability to produce financial statements, business continuity failure	Low	Medium	P3

2. **Regulatory Mapping for HIPAA**

Requirement Area	**Description / Compliance Expectation**	**Reference Section**
Privacy Rule	Protect patient information (PHI) from unauthorized disclosure and ensure it's only used for legitimate healthcare purposes.	**45 CFR §164.502**
Security Rule – Administrative Safeguards	Implement policies, employee training, and risk assessments to protect PHI.	**45 CFR §164.308**
Security Rule – Technical Safeguards	Use access controls, encryption, and authentication to secure PHI in electronic systems (ePHI).	**45 CFR §164.312**
Security Rule – Physical Safeguards	Restrict physical access to facilities and devices storing PHI.	**45 CFR §164.310**
Breach Notification Rule	Notify affected individuals, HHS, and sometimes the media of any data breaches involving PHI.	**45 CFR §164.404–§164.410**
Business Associate Agreements (BAAs)	Ensure all third parties handling PHI comply with HIPAA through formal BAAs.	**45 CFR §164.308(b)**
International Data Handling	When operating globally, ensure PHI transfers comply with both HIPAA and local data protection laws (e.g., GDPR).	*Best Practice / Cross-Jurisdictional Compliance*

2B. Regulatory Mapping for SOX

Category	**Risk (from Q1)**	**Compliance Requirement / Control Objective**	**Relevant SOX Section**

Cybersecurity	Ransomware / malware attacks	Implement IT General Controls (ITGCs) to ensure system security, integrity, and access restrictions over financial reporting systems.	Section 404 – Internal Controls over Financial Reporting
Change Management	Unauthorized system changes	Establish formal change management procedures, including testing, approvals, and documentation for all financial system updates.	Section 404 – Internal Controls
Financial Reporting / Controls	Inadequate segregation of duties	Segregate duties among accounting personnel to prevent conflicts of interest or fraud; implement regular management review.	Section 404 – Internal Controls
IT General Controls	Unauthorized changes to financial systems	Maintain strict access controls, audit trails, and periodic reviews of user permissions for systems affecting financial data.	Section 404 – ITGCs
Regulatory / Governance	Missing CEO/CFO certifications	Require senior executives to personally certify the accuracy of financial statements and disclosure controls.	Section 302 – Corporate Responsibility for Financial Reports

Financial Systems	No backup verification process	Implement data backup, recovery testing, and documentation procedures to ensure financial data integrity and availability.	Section 404 – Internal Control Documentation & Testing

3. Structure of Governance

A. Framework for Governance

In order to guarantee supervision, responsibility, and ongoing development in the areas of SOX and HIPAA compliance, Wellcare will implement a Compliance Governance Framework. The framework incorporates compliance into the company's entire risk management and corporate governance procedures.

Important Elements:

Board of Directors and Audit Committee - Regulatory conformity is ensured, audit results are reviewed, and compliance procedures are ultimately overseen by the Board of Directors and Audit Committee.

Compliance Committee - The Compliance Committee oversees the SOX and HIPAA procedures, keeps an eye on how the policies are being applied, and provides the board with quarterly reports.

Chief Compliance Officer (CCO) - The Chief Compliance Officer (CCO) or Compliance Office oversees risk assessments, compliance strategy, and regulatory relations.

Departmental Compliance Leads: Oversee daily compliance tasks in operations, finance, human resources, and information technology.

Internal Audit Team: Conducts routine audits and keeps an eye on the efficacy of controls.

Role	**Responsibility**
Chief Compliance Officer (CCO)	Chairs the committee, ensures alignment with corporate objectives, and oversees policy implementation.
HIPAA Privacy Officer	Ensures patient data protection, manages breach responses, and updates HIPAA policies.
SOX Compliance Manager	Oversees financial reporting controls, segregation of duties, and control testing.
IT Security Lead	Implements and monitors technical safeguards (encryption, access control).
HR / Training Lead	Coordinates employee training, certification, and policy acknowledgment.
Legal Counsel	Reviews regulatory updates and advises on international data protection laws (GDPR, etc.).
Internal Auditor	Conducts periodic audits and reports findings to the Compliance Committee.

4. Policies and Controls

C. Security Incident Response

Policy Statement:
Wellcare will promptly detect, contain, and report security incidents involving PHI or financial systems to minimize risk and maintain regulatory compliance.

Scope:
Applies to all employees, contractors, and business associates.

Category	**Severity**	**Examples**
1 – Critical	Major system compromise or confirmed PHI breach	Ransomware attack, data exfiltration

2 – High	Potential data breach or malware infection	Unauthorized access attempt, detected malware
3 – Medium	Policy or procedural violation	Lost laptop, suspicious email activity
4 – Low	Minor security events	Failed logins, spam or phishing (no compromise)

Incident Responses

Phase	**Timeline**	**Key Actions**
Detection & Reporting	0–2 hours	Report incidents to SOC; assign severity; notify CISO/CPO for critical cases
Assessment & Containment	2–8 hours	Assemble response team, assess scope, isolate affected systems, preserve evidence
Investigation & Remediation	1–5 days	Conduct root cause analysis, apply corrective actions, document findings
Notification & Reporting	As required	Notify affected parties and regulators per HIPAA/SOX timelines (≤60 days)
Post-Incident Review	Within 30 days	Conduct lessons learned, update policies, and retrain as needed

D. Code of Conduct and Employee

Responsibilities Policy Statement:

All workforce members must uphold integrity, protect confidential data, and comply with HIPAA, SOX, and Wellcare policies. Violations may result in discipline or legal consequences.

Core Principles

- **Integrity:** Conduct business honestly and ethically.
- **Compliance:** Adhere to all regulatory and company requirements.
- **Confidentiality:** Safeguard PHI and financial information.
- **Respect:** Treat others with professionalism and dignity.

- **Accountability:** Take ownership of decisions and actions.

Responsibilities of Employees

Area	Responsibilities
HIPAA Compliance	Access PHI only as required, report breaches, and complete annual HIPAA training.
SOX Compliance	Maintain accurate financial records, follow internal controls, and support audits.
Reporting Violations	Report issues to supervisor, CCO, or hotline (anonymous option). No retaliation under SOX §806.
Conflicts of Interest	Disclose conflicts, avoid personal gain, complete annual COI certification.

High level control mechanisms to ensure compliance with regulatory requirements

HIPAA Controls

Control Area	Type	Key Control	Frequency
Access Control	Preventive	Role-based system access	Ongoing
Access Review	Detective	Quarterly user access audits	Quarterly
Encryption	Preventive	Encrypt PHI in storage and transit	Ongoing
Audit Logging	Detective	Review access logs for anomalies	Daily
Training	Preventive	Annual HIPAA awareness sessions	Annually
Risk Assessment	Detective	Enterprise security risk review	Annually
Breach Response	Corrective	Implement incident response plan	As needed
Vendor Management	Preventive	Enforce signed BAAs before PHI access	Prior to onboarding

Physical Security	Preventive	Secure areas with key/badge entry	Ongoing
Mobile Devices	Preventive	Use MDM with remote wipe capability	Ongoing

High Level SOX Controls

Control Area	**Type**	**Key Control**	**Frequency**
Segregation of Duties	Preventive	Separate authorization and reconciliation roles	Continuous
Access Management	Preventive	Role-based access to finance systems	Ongoing
Access Review	Detective	Quarterly access verification	Quarterly
Change Management	Preventive	Approve and document all system changes	Per change
Account Reconciliation	Detective	Monthly ledger reconciliations	Monthly
Journal Entry Review	Detective	Supervisor review of manual entries	Monthly
Financial Close	Detective	Multi-tier review of statements	Monthly/Quarterly
SOX Testing	Detective	Annual control effectiveness testing	Annually
Audit Documentation	Detective	Maintain proof of control execution	Ongoing
Management Certification	Preventive	CEO/CFO certifications (SOX §302)	Quarterly

Training and Awareness

Phase	**Training Focus**	Target	Timeline
Onboarding	Overview of HIPAA and SOX principles, employee obligations.	All new hires	Upon hiring

Role-Based Training	Department-specific compliance procedures.	IT, Finance, HR	Semi-annually
Annual Refresher	Reinforce HIPAA and SOX updates, lessons learned from incidents.	All employees	Annually
Leadership Workshops	Advanced governance and accountability training.	Managers and executives	Annually

B . Methods of Continuous Learning

Case studies and quizzes in e-learning modules.
Newsletters on compliance every month.
Workshops with scenarios and phishing simulations.
Micro assessments to gauge understanding are given every three months.

TASK 6: MONITORING AND REPORTING

A. Ongoing Compliance Monitoring Methods

Security log monitoring	HIPAA	SIEM tool tracks PHI access, failed logins, suspicious activity	Daily	CISO
User access reviews	HIPAA & SOX	Review all user permissions for PHI and financial systems	Quarterly	IT Security Lead
Control testing	SOX	Test key financial controls (SoD, approvals, reconciliations)	Quarterly	SOX Manager

Vulnerability scanning	HIPAA & SOX	Automated scans of all systems for security weaknesses	Weekly	IT Security Lead
Vendor compliance checks	HIPAA	Verify BAAs signed and vendor security assessments current	Annually	CCO
Encryption verification	HIPAA	Audit all devices/systems storing PHI for encryption compliance	Monthly	CISO
Change management review	SOX	Review all financial system changes for proper approval	Monthly	SOX Manager
Financial reconciliations	SOX	Account reconciliation completion and review	Monthly	CFO

B. Internal Audit Program

Audit Type	Scope	Frequency	Deliverable	Recipient
HIPAA Security Audit	PHI access controls, encryption, audit logs, BAAs, breach response readiness	Semi-annually	Audit report with findings and recommendations	Compliance Committee, CISO

Audit Type	Scope	Frequency	Deliverable	Recipient
SOX Controls Audit	ITGCs (access, change, backup), financial controls (SoD, approvals), documentation	Annually (before external audit)	Control effectiveness assessment	Audit Committee, CFO
Privacy Compliance Audit	Patient rights processes, privacy notices, complaint handling	Annually	Privacy program assessment	CPO, Compliance Committee
Vendor Risk Audit	High-risk vendors with PHI/financial data access	Annually	Vendor risk rating and remediation plan	CCO
Incident Response Testing	Tabletop exercise simulating breach or financial system failure	Annually	Test results and process improvements	CISO, CFO, CCO

C. Reporting Mechanisms

Report Type	Content	Audience	Frequency	Format
Compliance Status Report	Overall compliance posture, KPI dashboard, open audit findings, training completion, policy violations, upcoming risks	Compliance Committee	Monthly	Written report + dashboard
Incident Summary	All security incidents, breach determinations, root causes, corrective actions	Compliance Committee, Audit Committee	Monthly	Written report
Executive Compliance Report	High-level compliance status, material issues, audit findings, control	Audit Committee	Quarterly	Presentation + written report

Report Type	Content	Audience	Frequency	Format
	deficiencies, KPIs, strategic initiatives			
Board Compliance Briefing	Program health, significant regulatory changes, material risks, whistleblower complaints, regulatory examinations	Board of Directors	Quarterly	Executive summary
SOX Certification	CEO/CFO personal certification of financial statement accuracy and control effectiveness	SEC (for public filing)	Quarterly (10-Q/10-K)	Formal certification
Breach Notification	Details of PHI breach, individuals affected, steps taken	Affected individuals, HHS, media (if >500)	Within 60 days of discovery	Written notice
Critical Incident Alert	Immediate notification of major breach, ransomware, or financial control failure	CEO, CCO, CISO, CFO, Legal Counsel	Within 2 hours of discovery	Email/text alert + 24-hour detailed report

TASK 7: COMPLIANCE METRICS AND KPIs

Key Performance Indicators (Combined HIPAA & SOX)

KPI	Description	Target	Tracking Frequency	Owner	Regulation
Training Completion Rate	% of workforce completing annual compliance training on time	100%	Monthly	CCO	HIPAA & SOX

KPI	Description	Target	Tracking Frequency	Owner	Regulation
Breach Incident Rate	Number of confirmed HIPAA breaches per quarter	0	Quarterly	CPO	HIPAA
Time to Breach Notification	Days from breach discovery to individual notification	≤60 days (regulatory max)	Per incident	CPO	HIPAA
BAA Coverage	% of vendors with PHI access having executed BAAs	100%	Quarterly	CPO	HIPAA
Encryption Compliance	% of devices/systems with PHI having encryption enabled	100%	Monthly	CISO	HIPAA
Control Testing Pass Rate	% of SOX controls tested with no deficiencies	≥95%	Quarterly	SOX Manager	SOX
Material Weaknesses	Number of material weaknesses in internal controls	0	Annually	CFO	SOX
User Access Review Completion	% of scheduled access reviews completed on time	100%	Quarterly	IT Security	HIPAA & SOX
Segregation of Duties Violations	Number of SoD conflicts per 1,000 users	<1	Quarterly	CFO	SOX
Change Management Compliance	% of financial system changes following approval process	100%	Monthly	CIO	SOX

KPI	Description	Target	Tracking Frequency	Owner	Regulation
Account Reconciliation Timeliness	% of accounts reconciled within 5 business days of month-end	100%	Monthly	CFO	SOX
Financial Close Timeliness	Days to complete monthly financial close	≤5 days	Monthly	CFO	SOX
Audit Finding Closure Rate	% of audit findings closed within agreed timeframes	≥90%	Quarterly	CCO	HIPAA & SOX
Security Awareness Effectiveness	% of employees failing simulated phishing tests	<5%	Monthly	CISO	HIPAA & SOX
Incident Response Time	Average hours from incident detection to containment	≤4 hours	Monthly	CISO	HIPAA & SOX

Performance Metrics Examples

Metric Category	Specific Metric	Measurement Method	Target	Action if Target Missed
HIPAA Training	Average days to complete HIPAA training after assignment	LMS tracking: (Sum of completion days) ÷ (Number of employees)	≤14 days	Escalate to managers; send reminders; require completion before system access
PHI Access Control	Number of inappropriate PHI access incidents	Monthly audit log sampling + incident reports	<2 per 1,000	Retraining; access recertification; disciplinary action

Metric Category	**Specific Metric**	**Measurement Method**	**Target**	**Action if Target Missed**
	per 1,000 employees			
Breach Response	Breach notification completeness score	Checklist: individuals notified, HHS notified, media notified (if required), documentation complete	100% compliance	Process review; additional training; update procedures
SOX Control Deficiencies	Control deficiency rate by control type	(Number of deficiencies) ÷ (Number of controls tested) × 100	≤5%	Focus remediation on high-deficiency areas; increase testing frequency; control redesign
Financial Close	Days to complete monthly close	Calendar days from month-end to close completion	≤5 days	Daily close meetings; identify bottlenecks; process automation; additional resources
Access Governance	% of terminated user accounts disabled within 24 hours	HR termination list vs. account disable logs	100%	Automate provisioning; improve HR-IT communication; escalation procedures
Vendor Risk	% of high-risk vendors with completed annual assessments	Vendor assessment tracker	100%	Prioritize overdue assessments; suspend vendor access if non-compliant
Incident Management	Mean time to detect (MTTD) security incidents	Average time from incident occurrence to detection	<1 hour	Enhance monitoring tools; improve alert

Metric Category	Specific Metric	Measurement Method	Target	Action if Target Missed
				tuning; 24/7 SOC coverage

KPI Dashboard Structure

Category (Needs	Green (On Target)	Yellow Attention)	Red (Critical)	Reporting Level
Training & Awareness ≥95%	Completion	Completion 85-94%	Completion <85%	Monthly - Compliance Committee
Security & Privacy	0 breaches, encryption 100%	1 minor incident, encryption 95-99%	2+ incidents or breach, encryption <95%	Monthly - Compliance Committee
Financial Controls	Pass rate ≥95%, 0 material weaknesses	Pass rate 85-94%, significant deficiencies	Pass rate <85%, material weakness	Quarterly - Audit Committee
Audit & Remediation	≥90% findings closed	75-89% findings closed	<75% findings closed	Quarterly - Audit Committee
Operational Metrics	All metrics on target	1-2 metrics missed	3+ metrics missed	Monthly - Compliance Committee

Summary:
SOX compliance at Wellcare requires robust internal controls over financial reporting, IT governance, and executive accountability. The highest-priority risks—such as inadequate segregation of duties, unauthorized system changes, and cybersecurity threats—are mitigated through strong IT General Controls, documented change management processes, and regular CEO/CFO certification of financial accuracy. These measures help ensure WellCare's financial integrity and transparency as it expands internationally.

Written by Grace Aku Nutifafa Awuma