REDE CONSULTING · HEALTHCARE PRACTICE

Healthcare *GRC* Workflow Framework

END-TO-END REFERENCE

Governance · Risk · Compliance
Integrated Workflow Architecture
Healthcare Sector | 2024–2025

SECTION 01 — KEY STAKEHOLDERS

Governance Participants

Board of Directors

Strategic oversight, GRC mandate & accountability

CEO / C-Suite

Executive sponsorship, culture & resource allocation

Chief Compliance Officer

Regulatory strategy, program leadership & reporting

Chief Risk Officer

Enterprise risk identification, assessment & mitigation

Chief Information Security Officer

Cybersecurity, data protection & PHI safeguarding

Chief Medical Officer

Clinical governance, patient safety & quality standards

Internal Audit

Independent assurance, control testing & gap assessment

Legal & Privacy Office

Regulatory counsel, BAA management & privacy impact

Department Heads

Operational risk ownership, front-line compliance implementation

Third-Party Vendors

Covered entities, business associates, supply chain partners

Regulatory Bodies

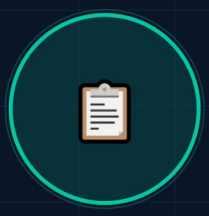
HHS/OCR, CMS, FDA, State Health Depts, Accreditors

Clinical Staff

Policy adherence, incident reporting, training completion

SECTION 02 — END-TO-END WORKFLOW

GRC Lifecycle Phases



PHASE 01

Governance Framework Setup

- → Define GRC charter & scope
- → Establish committee structure
- → Assign RACI across stakeholders
- → Set policy governance model
- → Integrate with strategic planning
- → Implement GRC technology platform

PHASE 02

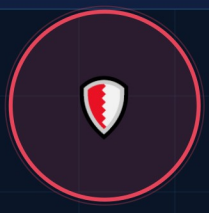
Risk Identification & Assessment

- → Asset & data flow mapping (PHI)
- → Threat landscape analysis
- → Clinical & operational risk inventory
- → Vendor/third-party risk assessment
- → Quantitative risk scoring
- → Risk register maintenance

PHASE 03

Regulatory Compliance Mapping

- → HIPAA/HITECH gap analysis
- → CMS condition of participation review
- → State law cross-mapping
- → Control framework alignment (NIST)
- → Obligation tracking & calendaring
- → Policy & procedure updates



PHASE 04

Control Implementation & Monitoring

- → Security control deployment
- → Staff training & awareness
- → Continuous compliance monitoring
- → Incident detection & response
- → Breach notification workflow
- → Audit trail management

PHASE 05

Reporting, Audit & Improvement

- → KPI dashboards to leadership
- → Internal & external audit support
- → Regulatory submissions & filings
- → Corrective action plans (CAPS)
- → Lessons learned integration
- → GRC program maturity review

SECTION 03 — REGULATORY COMPLIANCE LANDSCAPE

Key Frameworks & Obligations

HIPAA / HITECH

Privacy & Security Rule

Protected Health Information (PHI) safeguarding, patient rights, breach notification, and Business Associate Agreements.

Scope: All covered entities & BAs

CMS

Conditions of Participation

Medicare/Medicaid participation requirements including patient rights, quality standards, and medical record obligations.

Scope: Hospitals, SNFs, Home Health

FDA 21 CFR

Medical Device & Drug Regulation

Device approval, clinical trial regulations, pharmaceutical compliance, post-market surveillance, and labeling requirements.

Scope: Device manufacturers, pharma, labs

NIST CSF / SP 800-66

Cybersecurity Framework

Identify, Protect, Detect, Respond, Recover. Healthcare-tailored implementation guide for HIPAA Security Rule alignment.

Scope: All digital health entities

THE JOINT COMMISSION

Accreditation Standards

Quality, safety, and performance standards for hospitals and health systems including sentinel event review processes.

Scope: Accredited hospitals & networks

STATE REGULATIONS

State Health & Privacy Laws

State-specific privacy laws (CCPA, NY SHIELD, WA My Health MY Data), facility licensing, and reporting requirements.

Scope: Jurisdiction-dependent

SOC 2 / ISO 27001

Information Security Standards

Third-party security assurance for health IT vendors handling PHI; trust service criteria for availability and confidentiality.

Scope: Health IT vendors & SaaS

CLIA / CAP

Laboratory Compliance

Clinical Laboratory Improvement Amendments governing quality standards for labs performing testing on human specimens.

Scope: Clinical & reference labs

OIG / DOJ

Anti-Fraud & Abuse

False Claims Act, Anti-Kickback Statute, Stark Law compliance, mandatory compliance program requirements for providers.

Scope: All providers & billing entities

SECTION 04 — KEY PERFORMANCE INDICATORS

GRC Performance Metrics

98.5%

TARGET: ≥ 98%

Regulatory Compliance Rate

Percentage of applicable regulatory requirements with verified controls in place across all frameworks.

4.2h

TARGET: < 6 HRS

Mean Incident Response Time

Average time from security/compliance incident detection to initial containment actions being taken.

94%

TARGET: ≥ 90%

Staff Training Completion

Percentage of workforce completing mandatory HIPAA, security awareness, and compliance training on schedule.

12d

TARGET: ≤ 30 DAYS

Policy Review Cycle

Average number of days taken to complete a triggered policy review cycle from identification to approval.

Audit Finding Closure Rate

Percentage of internal/ external audit findings remediated within agreed-upon timeframes and validated by auditors.

TARGET: ≥ 95% within 90 days

Vendor Risk Assessment Coverage

Percentage of third-party vendors handling PHI with completed risk assessments and valid BAAs on file.

TARGET: 100% of tier-1 vendors

Residual Risk Score Reduction

Year-over-year decrease in the aggregated residual risk score across the enterprise risk register.

TARGET: ≥ 15% reduction annually

Breach Notification Timeliness

Percentage of PHI breaches where HHS/ individual notification occurred within the 60-day HIPAA requirement.

TARGET: 100% within 60 days

GRC Program Maturity Score

Overall GRC capability maturity rating based on CMMI-like scale assessed in annual program review cycle.

TARGET: Level 4 (Managed) by 2025

Control Testing Frequency

Percentage of critical controls subject to continuous or automated testing versus reliance on periodic review alone.

TARGET: ≥ 80% automated testing

RISK HEAT MAP

Low Medium High Critical

TOP RISK REGISTER

Ransomware / Cyberattack
Disruption to clinical operations; PHI encryption; HIPAA breach obligation — CISO

Unauthorized PHI Disclosure
Insider threat or system misconfiguration exposing patient records at scale — CCO + CISO

Third-Party Vendor Breach
BA security failure creating downstream HIPAA liability and reputational harm — CRO + Legal

Billing Fraud & False Claims
Inaccurate coding or upcoding triggering OIG investigation and FCA exposure — CCO + CFO

Regulatory Audit Failure
CMS survey deficiencies or HIPAA audit findings resulting in sanctions — CCO + Board

Medical Device Vulnerability
Unpatched connected devices exposing clinical networks to lateral movement — CISO + CMO

Staff Non-Compliance
Policy circumvention or training gaps resulting in preventable incidents — CCO + HR

GET EXPERT GUIDANCE

Ready to Strengthen Your Healthcare GRC Program?

Our specialists at Rede Consulting help healthcare organizations design, implement, and mature end-to-end GRC frameworks that reduce risk and ensure regulatory confidence.

Book a GRC Assessment

info@rede-consulting.com