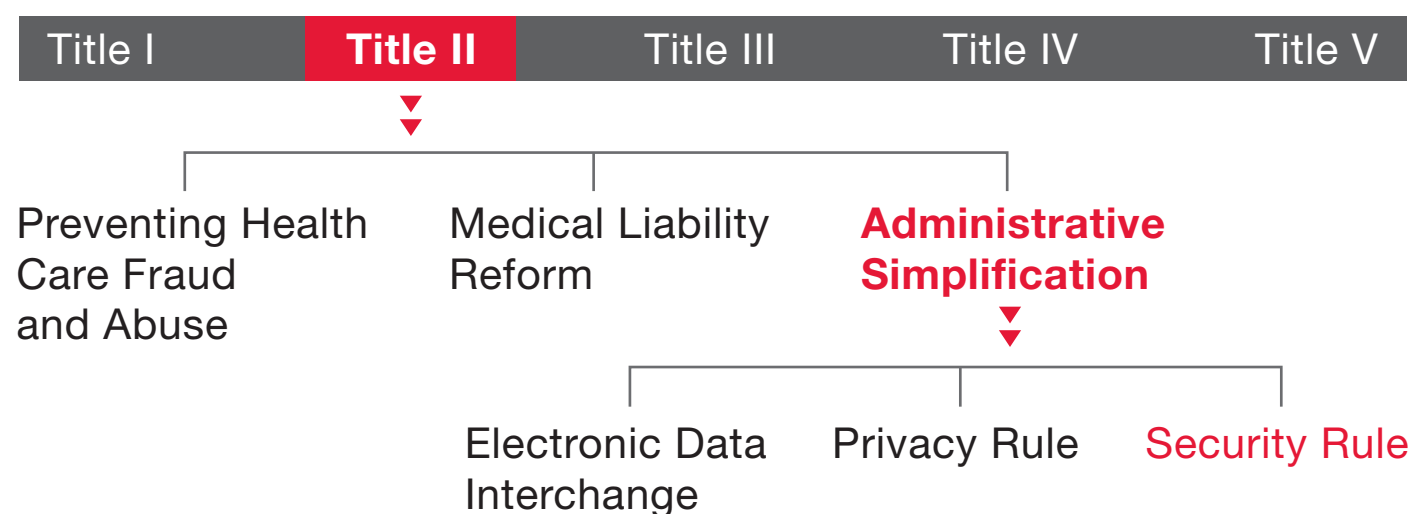


Components of a HIPAA Risk Analysis and How it Maps to the HIPAA Security Rule

HIPAA Health Insurance Portability and Accountability Act



Redspin's HIPAA Gap Analysis Covers the Following Standards

Administrative Safeguards	Physical Safeguards	Technical Safeguards
Organizational Safeguards	Policies and Procedures and Documentation Requirements	

HIPAA SECURITY RULE STANDARDS DETAILS

- Business Associate Contracts and Other Arrangements (§ 164.308(b)(1)), (§ 164.314(a)(1))

- Contingency Plan (§ 164.308(a)(7))
- Access Control (§ 164.312(a)(1))

- Information Access Management (§ 164.308(a)(4))
- Device and Media Controls (§ 164.310(d)(1))
- Integrity (§ 164.312(c)(1))

- Security Management Process (§ 164.308(a)(1))
- Assigned Security Responsibility (§ 164.308(a)(2))
- Security Incident Procedures (§ 164.308(a)(6))
- Evaluation (§ 164.308(a)(8))
- Audit Controls (§ 164.312(b))
- Policies and Procedures (§ 164.316(a))
- Documentation (§ 164.316(b)(1))

- Access Control (§ 164.312(a)(1))
- Audit Controls (§ 164.312(b))
- Integrity (§ 164.312(c)(1))
- Transmission Security (§ 164.312(e)(1))

- Workforce Security (§ 164.308(a)(3))
- Security Awareness and Training (§ 164.308(a)(5))

- Facility Access Controls (§ 164.310(a)(1))
- Workstation Use (§ 164.310(b))
- Workstation Security (§ 164.310(c))

- Access Control (§ 164.312(a)(1))
- Audit Controls (§ 164.312(b))
- Integrity (§ 164.312(c)(1))
- Person or Entity Authentication (§ 164.312(d))

FUNCTIONAL ASSESSMENT SCOPE HOW TO AUDIT THE STANDARDS

Business Associate Oversight

Identification of Critical Vendors, Vendor Due Diligence, and Documentation Review

Business Continuity

Data Backup, Disaster Recovery, and Business Impact Analysis

Data Security

EPHI Disposal, Storage, and Transmission

Information Security Program

Risk Management and Incident Detection and Response

Network Analysis

Architecture, Access Control, Device Management, and Event Management

Personnel Security

Hiring Processes, Security Awareness, and Security Training

Physical Security

Data Center, Facilities, and Environmental Concerns

Systems Analysis

Patching, System Hardening, Anti-Virus, Upgrade Procedures, System Access, Logging, Password Policies, and Account Lockouts