anchor@anchor-cyber:~$ cat hipaa-security-rule.md

ANCHOR CYBER SECURITY LLC

HIPAA Security Rule Quick Reference

45 CFR Part 164, Subpart C — Administrative, Physical, and Technical safeguards for ePHI. Required vs. Addressable specifications, Breach Notification timelines, and OCR risk analysis requirements.

$ hipaa-sr --legend

Required (R) — must implement exactly as stated

Addressable (A) — implement a reasonable equivalent OR document why not applicable

Addressable ≠ optional. If an implementation specification is addressable, a covered entity must still implement it if reasonable and appropriate — or document its reasoning and implement an equivalent measure. Source: 45 CFR § 164.306(d).

$ hipaa-sr --administrative

Administrative Safeguards § 164.308

Security Management Process § 164.308(a)(1)

REQUIRED	Risk analysis — identify threats and vulnerabilities to ePHI
	Risk management — implement security measures to reduce risk
	Sanction policy — apply appropriate sanctions for policy violations
	Information system activity review — audit logs, access reports

Assigned Security Responsibility § 164.308(a)(2)

REQUIRED	Designate a security official responsible for HIPAA Security Rule compliance

Workforce Security § 164.308(a)(3)

ADDRESSABLE	Authorization and/or supervision procedures
	Workforce clearance procedures
	Termination procedures

Information Access Management § 164.308(a)(4)

REQUIRED	Isolating healthcare clearinghouse functions (where applicable)
ADDRESSABLE	Access authorization procedures
	Access establishment and modification procedures

Security Awareness and Training § 164.308(a)(5)

ADDRESSABLE	Security reminders
	Protection from malicious software
	Log-in monitoring
	Password management

Security Incident Procedures § 164.308(a)(6)

REQUIRED	Incident response and reporting procedures

Contingency Plan § 164.308(a)(7)

REQUIRED	Data backup plan
	Disaster recovery plan
	Emergency mode operation plan
ADDRESSABLE	Testing and revision procedures
	Applications and data criticality analysis

Evaluation § 164.308(a)(8)

REQUIRED	Periodic technical and non-technical evaluation of compliance with Security Rule

Business Associate Contracts § 164.308(b)(1)

REQUIRED	BAA must require BA to implement reasonable and appropriate safeguards for ePHI
	BA must report security incidents to covered entity

$ hipaa-sr --physical

Physical Safeguards § 164.310

Facility Access Controls § 164.310(a)(1)

ADDRESSABLE	Contingency operations (facility access during emergency)
	Facility security plan
	Access control and validation procedures
	Maintenance records

Workstation Use § 164.310(b)

REQUIRED	Policies specifying proper functions performed on workstations and their physical environment

Workstation Security § 164.310(c)

REQUIRED	Physical safeguards for workstations accessing ePHI — restrict access to authorized users only

Device and Media Controls § 164.310(d)(1)

REQUIRED	Disposal — final disposition of ePHI before reuse or disposal of media
	Media reuse — removal of ePHI before media is reused
ADDRESSABLE	Accountability — records of movements of hardware and media
	Data backup and storage before movement of equipment

$ hipaa-sr --technical

Technical Safeguards § 164.312

Access Control § 164.312(a)(1)

REQUIRED	Unique user identification — assign unique name/number to each user
	Emergency access procedure — obtain ePHI during emergencies
ADDRESSABLE	Automatic logoff
	Encryption and decryption of ePHI

Audit Controls § 164.312(b)

REQUIRED	Hardware, software, and/or procedural mechanisms to record and examine activity in information systems containing ePHI

Integrity § 164.312(c)(1)

ADDRESSABLE	Electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner

Person or Entity Authentication § 164.312(d)

REQUIRED	Verify that a person or entity seeking access to ePHI is the one claimed

Transmission Security § 164.312(e)(1)

ADDRESSABLE	Integrity controls — guard against unauthorized modification of ePHI in transit
	Encryption of ePHI in transit

$ hipaa-sr --breach-notification

Breach Notification Rule §§ 164.400–414

A "breach" is the unauthorized acquisition, access, use, or disclosure of PHI that compromises its security or privacy, unless a specific exception applies. An impermissible use or disclosure is presumed a breach unless the covered entity demonstrates low probability that PHI was compromised under a four-factor risk assessment.

60 days

→ Affected Individuals

Written notification. First-class mail. Substitute notice if contact info is outdated. § 164.404

60 days

→ HHS Secretary

Breaches of 500+: notify simultaneously. Breaches under 500: log and report annually. § 164.408

60 days

→ Media (500+ in state)

Prominent media outlet notification for breaches affecting 500+ in a state or jurisdiction. § 164.406

ASAP + 60 days

Business Associate → CE

BA notifies Covered Entity "without unreasonable delay" and within 60 days of discovery. § 164.410

$ hipaa-sr --risk-analysis

OCR Risk Analysis Requirements § 164.308(a)(1)(ii)(A)

The Security Risk Assessment (SRA) is the first document OCR investigators and enforcement agents request. It must be accurate, thorough, and documented. The following eight elements are drawn from OCR's published guidance on risk analysis.

1. **Scope** — Identify all ePHI your organization creates, receives, maintains, or transmits. Include all systems, applications, and media.
2. **Data collection** — Document where ePHI is stored, accessed, and transmitted. Interviews + technical review.
3. **Threat identification** — Identify reasonably anticipated threats to ePHI (natural, human, environmental).
4. **Vulnerability identification** — Identify current security vulnerabilities and the controls already in place.
5. **Likelihood determination** — Assess the probability that each threat will exploit each vulnerability. Low / Medium / High.
6. **Impact analysis** — Determine the impact of a threat exploiting a vulnerability on confidentiality, integrity, and availability.
7. **Risk level** — Assign risk levels as combinations of likelihood and impact. Document the methodology.
8. **Finalize + document** — Produce a written report. Risk analysis must be reviewed and updated periodically and when operations change.

Source: 45 CFR Parts 160 and 164 (HIPAA Security Rule) — HHS.gov · OCR Guidance on Risk Analysis, 2010 · HIPAA Breach Notification Rule §§ 164.400-414