◇ EASY (Q1–Q10)

Q1. HIPAA primarily protects which type of information?
A. Financial data
B. Intellectual property
C. Protected Health Information (PHI)
D. Network configuration data

Q2. HIPAA was enacted in which year?
A. 1990
B. 1994
C. 1996
D. 2000

Q3. Which organization enforces HIPAA compliance?
A. ISO
B. PCI SSC
C. HHS (Office for Civil Rights)
D. SEC

Q4. HIPAA applies to which of the following?
A. Only hospitals
B. Only insurance companies
C. Covered entities and business associates
D. All private companies

Q5. Which term refers to health data in electronic form?
A. PHI
B. ePHI
C. PII
D. SPI

Q6. Which HIPAA rule establishes standards for safeguarding ePHI?
A. Privacy Rule
B. Enforcement Rule
C. Security Rule
D. Breach Rule

Q7. The minimum necessary principle requires organizations to:
A. Encrypt all data
B. Share only required information
C. Eliminate data storage
D. Obtain consent every time

Q8. Which HIPAA rule requires notification after a data breach?
A. Privacy Rule
B. Security Rule
C. Enforcement Rule
D. Breach Notification Rule

Q9. Which HIPAA title is MOST relevant to information security?
A. Title I
B. Title II
C. Title III
D. Title IV

Q10. HIPAA primarily focuses on which security objectives?
A. Performance and scalability
B. Confidentiality, integrity, and availability
C. Profitability and efficiency
D. Automation and analytics

◇ MEDIUM (Q11–Q25)

Q11. HIPAA Privacy Rule governs:
A. Network security controls
B. Use and disclosure of PHI
C. Technical safeguards only
D. Incident response procedures

Q12. HIPAA Security Rule safeguards are categorized into:
A. Technical and legal
B. Administrative, physical, and technical
C. Operational and financial
D. Preventive and detective

Q13. Which entity handles PHI on behalf of a covered entity?
A. Covered entity
B. Data controller
C. Business associate
D. Auditor

Q14. HIPAA requires organizations to perform which activity regularly?
A. Penetration testing
B. Risk analysis
C. Code review
D. Certification audits

Q15. Which safeguard category includes policies and workforce training?
A. Technical
B. Physical
C. Administrative
D. Legal

Q16. Which HIPAA rule defines penalties and enforcement actions?
A. Privacy Rule
B. Security Rule
C. Enforcement Rule
D. Breach Rule

Q17. HIPAA violations can result in:
A. No penalties
B. Civil and criminal penalties
C. Warnings only
D. Technical sanctions only

Q18. Which right allows patients to request corrections to their records?
A. Right to access
B. Right to restriction
C. Right to amendment
D. Right to portability

Q19. HIPAA Security Rule is best described as:
A. Prescriptive
B. Risk-based and flexible
C. Checklist-driven
D. Optional

Q20. Which safeguard addresses facility access controls?
A. Administrative
B. Technical
C. Physical
D. Legal

Q21. HIPAA Breach Notification Rule requires notification to individuals and:
A. ISO
B. PCI SSC
C. HHS
D. FBI

Q22. Which HIPAA requirement MOST directly supports accountability?
A. Data encryption
B. Documentation and policies
C. Firewall deployment
D. Antivirus software

Q23. HIPAA compliance is primarily a responsibility of:
A. IT department only
B. Security team only
C. Entire organization
D. External auditors

Q24. Which HIPAA concept limits PHI access based on job role?
A. Data minimization
B. Minimum necessary
C. Least privilege
D. Access control

Q25. HIPAA requires business associate agreements to ensure:
A. Cost reduction
B. Legal accountability for PHI protection
C. Vendor certification
D. Faster processing

△ HARD (Q26–Q40)

Q26. Which scenario BEST illustrates a HIPAA violation?
A. Authorized doctor accessing patient data
B. Employee accessing records without job-related need
C. Encrypted backup storage
D. Risk assessment documentation

Q27. Which HIPAA safeguard MOST directly prevents insider misuse?
A. Physical locks
B. Workforce training and policies
C. Network segmentation
D. Data backups

Q28. An organization fully compliant with HIPAA but lacking incident response plans MOST likely violates:
A. Privacy Rule
B. Security Rule
C. Enforcement Rule
D. Title I

Q29. Which factor MOST increases HIPAA compliance complexity?
A. Single clinic operation
B. Outsourced data processing
C. Limited workforce
D. Local data storage

Q30. Which HIPAA rule MOST closely aligns with cybersecurity governance?
A. Privacy Rule
B. Security Rule
C. Breach Rule
D. Enforcement Rule

Q31. HIPAA penalties are tiered based on:
A. Organization size
B. Level of negligence
C. Type of technology used
D. Number of systems

Q32. Which governance failure MOST leads to repeated HIPAA violations?
A. Strong leadership
B. Lack of risk analysis
C. Regular training
D. Incident reporting

Q33. HIPAA Security Rule flexibility allows organizations to:
A. Ignore safeguards
B. Tailor controls based on risk and size
C. Eliminate documentation
D. Avoid audits

Q34. Which HIPAA requirement MOST supports patient trust?
A. Audit logging
B. Confidentiality of PHI
C. System uptime
D. Encryption strength

Q35. A healthcare organization relying only on technical safeguards MOST likely fails to address:
A. Network threats
B. Governance and policy controls
C. Malware risks
D. Availability issues

Q36. Which HIPAA rule requires timely breach reporting to affected individuals?
A. Security Rule
B. Privacy Rule
C. Breach Notification Rule
D. Enforcement Rule

Q37. HIPAA compliance audits primarily assess:
A. Business profitability
B. Security and privacy controls
C. Software quality
D. Network speed

Q38. Which HIPAA safeguard MOST directly supports audit evidence?
A. Incident response drills
B. Documentation and records
C. Firewall rules
D. Encryption keys

Q39. Which HIPAA principle MOST aligns with ethical handling of patient data?
A. Accountability
B. Minimum necessary
C. Confidentiality
D. Availability

Q40. The PRIMARY objective of HIPAA is to:
A. Standardize healthcare software
B. Protect patient privacy and data security
C. Eliminate healthcare fraud
D. Replace cybersecurity standards