PassQueen
a.k.a dumpsqueen.com

HealthCare Information Security and Privacy Practitioner

ISC2 HCISPP

Version Demo

Total Demo Questions: 37

Total Premium Questions: 370

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Healthcare Industry	184
Topic 2, Regulatory Environment	82
Topic 3, Privacy and Security in Healthcare	64
Topic 4, Information Governance and Risk Management	20
Topic 5, Information Risk Assessment	11
Topic 6, Third-Party Risk Management	6
Topic 7, Mix Questions	3
Total	370

QUESTION NO: 1

A risk assessment report recommends upgrading all perimeter firewalls to mitigate a particular finding. Which of the following BEST supports this recommendation?

A. The inherent risk is greater than the residual risk.

B. The Annualized Loss Expectancy (ALE) approaches zero.

C. The expected loss from the risk exceeds mitigation costs.

D. The infrastructure budget can easily cover the upgrade costs.

ANSWER: C

Explanation:

The expected loss from the risk exceeds mitigation costs. This conclusion provides the strongest business and risk-management justification for upgrading the perimeter firewalls because it compares the anticipated financial impact of leaving the risk untreated with the cost of the proposed safeguard. When the expected loss is greater than the cost to implement and operate the control, the upgrade is economically justified: the organization can reduce its probable loss exposure for less than the amount it expects to lose if the finding is not addressed.

Risk treatment decisions should be based on risk analysis and organizational risk tolerance, including the consequences and likelihood associated with the identified threat scenario. A firewall upgrade is a control-selection decision, so the assessment should demonstrate that the control is appropriate to reduce the relevant risk and that its cost is proportionate to the reduction achieved. This cost-versus-expected-loss comparison supports accountable allocation of security resources while aligning the remediation action to a documented risk finding. NIST describes risk assessment as informing risk responses and control decisions in SP 800-30 Rev. 1, while its risk-management guidance addresses selecting and implementing controls as part of responding to risk in SP 800-37 Rev. 2.

QUESTION NO: 2

What time period was the Cannon of Medicine in?

A. Ancient

B. Modern

C. Medieval

D. Prehistoric

ANSWER: C

Explanation:

Medieval is correct. The question is referring to *The Canon of Medicine* (also known by its Latin title, *Canon medicinae*), the major medical encyclopedia written by the Persian physician and philosopher Avicenna, or Ibn Sina. It was completed around 1025 CE, placing its composition firmly within the medieval period. The work organized medical knowledge from Greek, Roman, Persian, and Arabic traditions into a systematic five-book reference covering medical principles, simple drugs, diseases of individual organs, general diseases, and compound remedies.

The *Canon of Medicine* had an exceptionally long influence on medical education and clinical practice. After it was translated into Latin during the twelfth century, it became a foundational text at European universities and remained influential for centuries. Its historical importance includes its structured approach to diagnosis, pharmacology, observation, and the ethical practice of medicine. In the history of health care, it is therefore recognized as a landmark of medieval Islamic medicine that substantially shaped later Western medical learning. Britannica dates Avicenna's *Canon of Medicine* to approximately 1025 and describes its enduring role in medieval European education: Encyclopaedia Britannica: Avicenna. Additional historical context is available from the U.S. National Library of Medicine.

QUESTION NO: 3

Transcribes, dictations and creates medical reports for hospital administrations.

A. Coders

B. Cancer registrars

C. Medical Transcriptionist

ANSWER: C

Explanation:

Medical Transcriptionist is correct because this role converts healthcare providers' dictated audio into accurate, structured written documentation, such as medical histories, examination findings, operative reports, discharge summaries, and consultation reports. The work requires strong knowledge of medical terminology, anatomy, pharmacology, diagnostic procedures, and documentation conventions, as well as careful listening and editing to ensure the resulting report faithfully reflects the clinician's dictation. These reports become part of the patient's health record and support continuity of care, billing, quality activities, and legal documentation. In a hospital environment, transcription personnel may receive recordings through dictation platforms, apply approved formatting and templates, identify unclear content for clarification, and protect protected health information throughout the workflow. The U.S. Bureau of Labor Statistics describes medical transcriptionists as professionals who listen to recordings made by healthcare workers and convert them into written reports. This directly matches the stated responsibility of transcribing dictations and creating medical reports for hospital administration. See the U.S. Bureau of Labor Statistics Occupational Outlook Handbook and the AHIMA health information career resources.

QUESTION NO: 4

In the preindustrial era, asylums were built by_____ to accommodate patients with severe and chronic mental illness.

A. The federal government

B. Private entrepreneurs

C. Psychiatrists

D. The state governments

ANSWER: D

Explanation:

The state governments is correct. In the United States, the nineteenth-century expansion of large public mental hospitals was principally a state responsibility. Reformers argued that people with severe, persistent mental illness needed structured, humane institutional care rather than confinement in jails, almshouses, or private homes. Their advocacy helped prompt states to establish and fund purpose-built hospitals or asylums, often located outside crowded cities and intended to provide long-term supervision, shelter, and treatment.

This state-led model reflected the era's developing public-welfare role: state legislatures authorized institutions, appropriated funds, and created governance arrangements for them. Dorothea Dix's well-known reform campaign, for example, sought public support for dedicated institutions for people with mental illness and contributed to the creation or enlargement of many state hospitals. Although local entities, charitable organizations, and private facilities could also play roles in mental-health care, the defining institutional expansion of public asylums for severe and chronic illness was led by state governments. This historical context is important in healthcare practice because it explains the origins of state mental-health systems and the long-term institutional-care model that later policy reforms sought to replace or supplement with community-based services. See the National Library of Medicine's Dorothea Dix historical collection and the National Academies' discussion of the historical development of U.S. mental-health care in Ending Discrimination Against People with Mental and Substance Use Disorders.

QUESTION NO: 5

Are employers required to submit enrollments by the standard transactions?

A. Though Employers are not CEs and they have to send enrollment using HIPPA standard transactions. However, the employer health plan IS a CE and must be able to conduct applicable transactions using the HIPPA standards

B. Employers are not CEs and do not have to send enrollment using HIPPA standard transactions. However, the employer health plan IS a CE and must be able to conduct applicable transactions using the HIPPA standards.

C. Employers are CEs and have to send enrollment using HIPPA standard transactions. However, the employer health plan IS a CE and must be able to conduct applicable transactions using the HIPPA standards.

D. Employers are CEs and do not have to send enrollment using HIPPA standard transactions. Further, the employer health plan IS also a CE and must be able to conduct applicable transactions using the HIPPA standards.

ANSWER: B

Explanation:

“Employers are not CEs and do not have to send enrollment using HIPPA standard transactions. However, the employer health plan IS a CE and must be able to conduct applicable transactions using the HIPPA standards.” is correct. Under HIPAA Administrative Simplification, an employer is not itself a covered entity merely because it sponsors or administers benefits for its workforce. Thus, an employer is not required to use the HIPAA standard enrollment and disenrollment transaction when communicating enrollment information in its role as employer.

In contrast, an employer-sponsored group health plan is a health plan and therefore is a HIPAA covered entity. When that health plan conducts a transaction for which HIPAA has adopted a standard, including the enrollment and disenrollment in a health plan transaction, it must comply with the applicable transaction, code-set, and implementation-specification requirements. This distinction is important because the legal obligation attaches to the group health plan’s covered-entity functions, rather than to the employer’s ordinary employment-related activities. The HIPAA transaction standards applicability rule is available at 45 CFR § 162.1101. HHS also describes the adopted standard transactions, including enrollment and disenrollment, at HIPAA standard transactions.

QUESTION NO: 6

A covered entity determines that an unencrypted laptop containing protected health information was stolen. After completing the required risk assessment, the organization cannot demonstrate a low probability that the PHI was compromised. What must the organization do?

A. Provide breach notification as required by the HIPAA Breach Notification Rule

B. Take no further action because the laptop was protected by a password

C. Notify affected individuals only if more than 500 records were stored on the laptop

D. Wait until the laptop is recovered before evaluating notification obligations

ANSWER: A

Explanation:

The organization must provide breach notification in accordance with the HIPAA Breach Notification Rule. An impermissible acquisition, access, use, or disclosure of unsecured PHI is presumed to be a breach unless the covered entity or business associate demonstrates through the required risk assessment that there is a low probability the PHI has been compromised. A stolen unencrypted laptop is a common example requiring careful assessment because the information may be accessible to an unauthorized person.

When notification is required, the covered entity must notify affected individuals without unreasonable delay and no later than 60 calendar days after discovery. Additional notification obligations depend on the number and location of affected individuals. Encryption consistent with HHS guidance can render PHI unusable, unreadable, or indecipherable and may prevent the information from being considered unsecured PHI; the laptop in this scenario was unencrypted. See 45 CFR § 164.402 and HHS Breach Notification Rule guidance.

QUESTION NO: 7

If a person has the ability to access facility of company systems or applications, they have a right to view any information contained in that system or application.

A. True

B. False

ANSWER: B

Explanation:

False is correct because the technical ability to enter a company system or application does not itself confer authorization to view all information held there. In healthcare, access decisions must follow the principle of least privilege: workforce members receive only the minimum access and data permissions needed to perform their assigned job duties. Access must also be role-based and governed by organizational authorization policies, so being able to authenticate to an application or navigate to a data location is not equivalent to having a legitimate business need or permission to view every record.

For protected health information, the HIPAA Privacy Rule's minimum necessary standard requires reasonable efforts to limit uses, disclosures, and requests to the minimum necessary information for the intended purpose. The HIPAA Security Rule likewise requires access controls that restrict access to authorized users and support appropriate authorization management. Healthcare organizations should enforce these requirements through role-based access control, unique user identification, audit logging, periodic access reviews, and prompt removal or adjustment of access when duties change. More information is available from HHS guidance on the minimum necessary requirement and HHS Security Rule guidance.

QUESTION NO: 8

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

A. Document the system as high risk

B. Perform a vulnerability assessment

C. Perform a quantitative threat assessment

D. Notate the information and move on

ANSWER: B

Explanation:

Perform a vulnerability assessment is the best approach because an in-house-developed application that creates, receives, maintains, or transmits PHI must be evaluated for technical weaknesses that could affect the confidentiality, integrity, or availability of that information. Organizational awareness of HIPAA requirements and an assertion of compliance do not eliminate the need to assess the application itself. Custom-developed software can introduce implementation-specific issues, such as insecure authentication, authorization flaws, unpatched components, insecure configuration, inadequate encryption, or insufficient audit logging. A vulnerability assessment provides actionable evidence about these weaknesses and supports risk treatment decisions during the project risk-assessment phase.

HIPAA's Security Rule requires covered entities and business associates to conduct an accurate and thorough assessment of potential risks and vulnerabilities to ePHI. The CISO should therefore ensure that the application is assessed in its actual

operating context, document identified vulnerabilities, evaluate their risk, and track remediation through the organization's risk-management process. This is consistent with HHS guidance on security risk analysis and NIST's HIPAA Security Rule implementation guidance in NIST SP 800-66 Rev. 2.

QUESTION NO: 9

In addition to first contact care, the key task(s) of primary care include.

A. Longitudinality, or following a patient over time

B. Comprehensiveness

C. Coordination

D. All of the above

ANSWER: D

Explanation:

All of the above is correct because primary care is classically defined by four core functions: first-contact access, longitudinality, comprehensiveness, and coordination. Longitudinality means an ongoing, person-focused relationship in which a clinician or care team knows the patient over time, rather than treating isolated encounters. This continuity supports preventive care, recognition of changing health needs, and care that reflects the patient's history and preferences.

Comprehensiveness means primary care addresses the broad majority of a population's health needs, including prevention, acute concerns, chronic disease management, health promotion, and referral when specialized services are needed. Coordination ensures that services from specialists, hospitals, laboratories, community resources, and other settings are organized around the patient, with relevant information communicated across the care continuum. Together, these functions make primary care more than an initial entry point into the healthcare system; they establish it as the setting responsible for integrating and sustaining care. The American Academy of Family Physicians describes primary care using these same foundational functions, and the National Academies similarly identifies accessible, comprehensive, coordinated, and continuous care as central characteristics. See the AAFP primary care policy and the National Academies overview of primary care.

QUESTION NO: 10

Medicare and Medicaid are apart of social security amendments?

A. True

B. False

ANSWER: A

Explanation:

True is correct. Medicare and Medicaid were established through the Social Security Amendments of 1965, which President Lyndon B. Johnson signed into law on July 30, 1965. The amendments added Title XVIII to the Social Security Act, creating Medicare, a federal health insurance program initially focused on people age 65 and older. They also added Title XIX, creating Medicaid as a jointly funded federal-state program that provides medical assistance to eligible individuals with limited income and resources.

This legislative origin is important in healthcare compliance and privacy because both programs are administered under statutory and regulatory structures connected to the Social Security Act. Although Medicare and Medicaid have evolved substantially through later laws and regulations, their foundational authority remains the 1965 amendments. The Centers for Medicare & Medicaid Services provides a historical overview of the programs' creation at CMS History. The Social Security Administration also identifies the Social Security Amendments of 1965 as the legislation that established Medicare and Medicaid in its historical account of the 1965 amendments.

QUESTION NO: 11

Are there penalties under HIPPA?

A. No penalties

B. HIPPA calls for severe civil and criminal penalties for noncompliance, including: -- fines up to $25k for multiple violations of the same standard in a calendar year -- fines up to $250k and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information.

C. HIPPA calls for severe civil and criminal penalties for noncompliance, includes: -- fines up to 50k for multiple violations of the same standard in a calendar year -- fines up to $500k and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information

D. HIPPA calls for severe civil and criminal penalties for noncompliance, including: -- fines up to $100 for multiple violations of the same standard in a calendar year -- fines up to $750k and/or imprisonment up to 20 years for knowing misuse of individually identifiable health information

E. HIPAA provides tiered civil monetary penalties, adjusted for inflation, and criminal penalties up to $250,000 and 10 years' imprisonment for knowing misuse with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.

ANSWER: E

Explanation:

Yes. HIPAA establishes both civil monetary penalties and criminal penalties for violations involving protected health information. The accurate current statement is that civil penalties are assessed under tiered categories based on the level of culpability, with statutory amounts adjusted periodically for inflation. The Department of Health and Human Services Office for Civil Rights may impose these civil penalties and considers factors such as the nature and extent of the violation, the harm resulting from it, and the organization's compliance history. Criminal enforcement is handled by the Department of Justice. Criminal penalties can reach up to $250,000 and up to 10 years' imprisonment when an individual knowingly obtains or discloses individually identifiable health information with intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm. This distinction is important: the maximum criminal sentence applies to a specific aggravated intent standard, rather than to every knowing misuse. HIPAA compliance programs should therefore address both organizational safeguards and workforce conduct, including appropriate access, disclosure, training, and sanctions. HHS summarizes civil enforcement and penalty requirements at HHS HIPAA Compliance and Enforcement; criminal provisions are codified at 42 U.S.C. § 1320d-6.

QUESTION NO: 12

Which of the following methods MOST efficiently manages user accounts when using a third-party cloud-based application and directory solution?

A. Cloud directory

B. Directory synchronization

C. Assurance framework

D. Lightweight Directory Access Protocol (LDAP)

ANSWER: B

Explanation:

Directory synchronization is correct because it automates the controlled replication of identity data from an authoritative organizational directory to the cloud directory used by a third-party application. This provides a scalable account-lifecycle process: when administrators create, update, disable, or remove a user in the source directory, the corresponding cloud account and relevant attributes can be provisioned or updated through the synchronization service. Managing identities from one authoritative source reduces manual administration, avoids duplicate account-maintenance workflows, and improves consistency in usernames, group memberships, and access-related attributes.

For healthcare organizations, this efficiency also supports timely deprovisioning when a workforce member changes roles or leaves, an important control for protecting systems that may process electronic protected health information. Synchronization should be governed through defined attribute mappings, least-privilege service permissions, monitoring of synchronization failures, and a documented process for handling exceptions. Microsoft's identity documentation describes directory synchronization as a mechanism for synchronizing users, groups, and contacts between on-premises Active Directory and Microsoft Entra ID: Microsoft Entra Connect Sync. Guidance on identity lifecycle management and automated provisioning is also available from NIST SP 800-63-4.

QUESTION NO: 13

What grants a " deemed status " , has conditions of participation and makes sure hospitals meet certain requirements to get reimburse for medicare/medicaid?

A. HIPPA

B. The Joint Commission (formerly JCAH)

C. Food and Drug Act

ANSWER: B

Explanation:

The Joint Commission is correct because it is a CMS-approved accrediting organization with deeming authority for hospitals. When a hospital successfully completes The Joint Commission's accreditation process, it may be "deemed" to meet applicable Medicare Conditions of Participation, rather than undergoing a separate CMS certification survey for those requirements. This accreditation relationship supports a hospital's eligibility to participate in the Medicare and Medicaid programs and receive associated reimbursement, provided the organization continues to meet all applicable program requirements. The Joint Commission evaluates hospitals against accreditation standards addressing areas such as patient safety, quality of care, infection prevention, leadership, medical staff oversight, and information management. CMS recognizes selected accrediting organizations and uses their survey processes as part of its oversight framework; CMS retains authority to validate accreditation findings and enforce participation requirements. The current organization is called The Joint Commission; "JCAH" is an older name and acronym associated with its historical predecessor. CMS explains deeming authority and its relationship to accreditation organizations at CMS Accreditation Organizations. The Joint Commission describes its hospital accreditation program and its role in Medicare deeming at The Joint Commission Hospital Accreditation.

QUESTION NO: 14

Covered entities (certain health care providers, health plans, and health care clearinghouses) are not required to comply with the HIPPA Privacy Rule until the compliance date. Covered entities may, of course, decide to:

A. unvoluntarily protect patient health information before this date

B. voluntarily comply with the HIPAA Privacy Rule before this date

C. after taking permission, voluntarily protect patient health information before this date

D. compulsorily protect patient health information before this date

ANSWER: B

Explanation:

"Voluntarily comply with the HIPAA Privacy Rule before this date" is correct because a regulatory compliance date establishes the point at which a covered entity is legally required to meet the Rule's requirements; it does not prevent the entity from adopting those protections earlier. A health care provider, health plan, or health care clearinghouse may therefore implement Privacy Rule policies, workforce training, administrative processes, safeguards, and patient-rights procedures in advance of the applicable deadline. Early voluntary implementation can help an organization operationalize appropriate uses

and disclosures of protected health information, prepare its workforce, test procedures, and establish a mature privacy program before compliance becomes mandatory.

The HIPAA Privacy Rule sets national standards for protecting individuals' identifiable health information held or transmitted by covered entities and establishes rights concerning that information. The U.S. Department of Health and Human Services identifies the entities subject to the Rule and explains its privacy protections at HHS HIPAA Privacy. The HIPAA regulations also provide for compliance dates in 45 C.F.R. § 164.534, available through the Electronic Code of Federal Regulations. Voluntary early compliance is therefore consistent with both the purpose and implementation structure of the Privacy Rule.

QUESTION NO: 15

A health plan may conduct its covered transactions through a clearinghouse, and may require a provider to conduct covered transactions with it through a clearinghouse. The incremental cost of doing so must be borne

A. by the HIPAA authorities

B. by the health plan

C. by any other entity but the health plan

D. by insurance companies

ANSWER: B

Explanation:

by the health plan is correct. HIPAA administrative simplification rules permit a health plan to use a clearinghouse to conduct covered electronic transactions, such as claims, eligibility inquiries, and payment-related transactions. A health plan may also require a health care provider to use a clearinghouse when conducting those transactions with the plan. However, the plan cannot shift the additional expense created by that requirement to the provider. The regulation expressly places responsibility for the incremental cost on the health plan.

"Incremental cost" means the added cost attributable to the plan's clearinghouse requirement, rather than ordinary expenses a provider would otherwise incur in conducting standard transactions. This requirement supports HIPAA's goal of standardized electronic administrative transactions while preventing a health plan from imposing the financial consequences of its own routing or intermediary preference on providers. The relevant provision is 45 C.F.R. § 162.923, which states that a health plan that requires use of a clearinghouse must bear the incremental costs of using that clearinghouse. See the eCFR text of 45 C.F.R. § 162.923 and HHS's HIPAA transaction standards overview.

QUESTION NO: 16

Avicenna was known for what?

A. Penicillin

B. Bacteria

C. The Canon of Medicine

ANSWER: C

Explanation:

Avicenna was known for **The Canon of Medicine**, a major medical encyclopedia written in Arabic during the early eleventh century. Avicenna, also called Ibn Sina, organized inherited Greek, Roman, Persian, and Arabic medical knowledge into a systematic work covering medical principles, diagnosis, pharmacology, anatomy, disease, and treatment. The work was especially influential because it presented medicine as a disciplined body of knowledge, including attention to observation, causes of illness, and practical therapeutic guidance. Its structured approach made it a foundational teaching text in the Islamic world and, after translation into Latin, in European medical education for centuries. In the context of healthcare history, the work illustrates the long intellectual tradition that informed later clinical practice and the formal study of medicine.

The title is properly spelled *Canon*, rather than “Cannon.” The Encyclopaedia Britannica describes Avicenna’s medical writings and the lasting importance of this work: https://www.britannica.com/biography/Avicenna. The U.S. National Library of Medicine also provides historical context on Avicenna and his medical legacy: https://www.nlm.nih.gov/hmd/arabic/med10.html.

QUESTION NO: 17

Was known for identifying anthrax.

A. Robert Koch

B. Edward Jenner

C. Louis Pasteur

ANSWER: A

Explanation:

Robert Koch is correct because he provided the first convincing demonstration that a specific microorganism causes a specific disease when he established that *Bacillus anthracis* causes anthrax. In 1876, Koch carefully examined blood from infected animals, isolated and cultured the anthrax bacillus, documented its life cycle—including its ability to form spores—and showed that material from the organism could transmit anthrax to healthy animals. This work was foundational to modern bacteriology and directly supported the germ theory of disease.

Koch’s anthrax investigations also helped establish the experimental approach later formalized as Koch’s postulates: associating a microorganism with disease, isolating it, growing it in culture, reproducing disease in a susceptible host, and recovering the organism again. Although the postulates have important limitations in contemporary microbiology, the anthrax work remains a landmark example of demonstrating microbial causation. The U.S. National Library of Medicine describes Koch’s demonstration that anthrax was caused by bacteria as a major breakthrough in medicine. See the National Library of Medicine’s overview of Koch’s work and Encyclopaedia Britannica’s biography of Robert Koch.

QUESTION NO: 18

All of these factors impact the health status of an individual, however, the one exerting the least influence is.

A. Medical care

B. Educational level

C. Income level

D. Broad socioeconomic factors

ANSWER: A

Explanation:

Medical care is correct because access to and quality of clinical services, while essential for diagnosing, treating, and managing illness, accounts for a comparatively limited share of overall population health status. Health is shaped over an entire lifetime by the conditions in which people are born, grow, live, work, and age. These conditions affect exposure to risks, opportunities for healthy choices, chronic stress, nutrition, housing stability, safety, and the ability to obtain preventive and ongoing care. Consequently, a person’s health often reflects circumstances that occur before a clinical encounter and that cannot be fully remedied through treatment alone.

This principle is especially relevant to health-care security and privacy professionals because equitable, trustworthy health systems must recognize the broader context in which patients use services and experience health outcomes. Protecting information and making care available remain important, but clinical care is only one contributor within a much wider set of health determinants. The World Health Organization describes social determinants of health as the non-medical factors that influence health outcomes, and the U.S. Office of Disease Prevention and Health Promotion identifies health care access

and quality as one of several determinant domains. See the World Health Organization's social determinants of health overview and Healthy People 2030 social determinants resource.

QUESTION NO: 19

HIPPA results in

A. sweeping changed in some healthcare transaction and administrative information systems

B. sweeping changes in most healthcare transaction and administrative information systems

C. minor changes in most healthcare transaction and administrative information systems D. no changes in most healthcare transaction and minor changes in administrative information systems

ANSWER: B

Explanation:

"sweeping changes in most healthcare transaction and administrative information systems" is correct because HIPAA established national standards that substantially reshaped how much of the U.S. healthcare sector handles administrative and electronic health-information processes. The Administrative Simplification provisions require covered entities to use standardized electronic transactions, code sets, unique identifiers, and operating rules in applicable business processes. These requirements affect common administrative activities such as claims, eligibility inquiries, referrals, remittance advice, enrollment, and payment-related transactions.

HIPAA also created nationally applicable privacy and security requirements for protected health information. As a result, organizations that create, receive, maintain, or transmit this information electronically must implement appropriate administrative, physical, and technical safeguards, as well as policies, procedures, workforce practices, and vendor-management arrangements. The impact therefore extends beyond isolated systems: it requires coordinated changes to workflows, data exchange, system configuration, record handling, and governance across healthcare organizations and their business partners. HHS describes these Administrative Simplification standards at CMS HIPAA Administrative Simplification, while the regulatory standards are published in 45 CFR Part 162.

QUESTION NO: 20

What is the title given to the group authorized by the HIPAA Privacy Rule to approve a waiver of authorization for the disclosure and/or use of personally identifiable health information?

A. Cohort Group

B. Institutional Review Board

C. Privacy Board

D. Board of Directors

ANSWER: C

Explanation:

Privacy Board is correct. Under the HIPAA Privacy Rule, a covered entity may use or disclose protected health information for research without an individual's authorization when a properly constituted Privacy Board has documented approval of a waiver or alteration of authorization. The board must determine that the privacy risks are reasonable in relation to anticipated benefits, that the requested information is necessary for the research, and that there is an adequate plan to protect identifiers from improper use and disclosure. Its documentation must identify the approving board, state that the required waiver criteria were satisfied, and be signed by the board chair or another authorized member. This mechanism supports research while preserving HIPAA's principle that identifiable health information should not be used or disclosed beyond what is justified and appropriately safeguarded. HHS describes waiver documentation and the required criteria in its HIPAA research guidance. The regulatory requirements are codified at 45 CFR § 164.512(i).

QUESTION NO: 21

Breach notification exceptions are provided to all, EXCEPT:

A. Business associates who access information by good faith, unintentional means and do not further disclose information

B. Unintentional, good faith access by employees of covered entities if the information was not further disclosed

C. If the information impacted less than 500 people within a single demographic area

D. Inadvertent disclosure made individual to individual within a covered entity who is authorized to access protected health information

ANSWER: C

Explanation:

If the information impacted less than 500 people within a single demographic area is correct because the number of individuals affected is not an exception to the HIPAA breach definition or to the obligation to provide individual notification. A breach affecting fewer than 500 individuals generally still requires notification to the affected individuals, the Secretary of HHS, and any other parties required by applicable law. The 500-individual threshold instead affects the reporting process and the potential requirement to notify prominent media outlets. For breaches involving fewer than 500 individuals, a covered entity may maintain a log and submit the information to HHS no later than 60 days after the end of the calendar year in which the breaches were discovered. The geographic phrasing does not create an exception either: location becomes relevant to media notification when a breach involves more than 500 residents of a state or jurisdiction. HIPAA's narrowly defined exceptions concern the nature and circumstances of an acquisition, access, use, or disclosure of protected health information, not a breach's size. HHS summarizes the notification requirements at HHS Breach Notification Rule; the governing regulatory requirements appear at 45 CFR Part 164, Subpart D.

QUESTION NO: 22

The Physician Assistant (PA) profession was developed in order to.

A. Function alongside a physician without having to complete the many years of medical education and residency

B. Replace the overly-paid physician role

C. Perform the few roles broadly skilled physicians are not licensed to perform

D. All of the above

ANSWER: A

Explanation:

"Function alongside a physician without having to complete the many years of medical education and residency" is correct because the profession was created to expand the healthcare workforce by preparing clinicians through a shorter, focused medical-training pathway than the education and residency required of physicians. The first formal educational program began at Duke University in 1965, drawing in part on the experience of former military medical corpsmen. Its purpose was to help meet healthcare needs, particularly by increasing the availability of clinically trained practitioners who could provide medical services as members of physician-led teams. Modern physician assistants/physician associates are educated in the medical model and practice medicine in collaboration with physicians and other healthcare professionals. Their scope of practice is defined by education, demonstrated competence, organizational policies, and applicable state law. The profession therefore supports access to care and team-based delivery while retaining a distinct educational route from that of a physician. The American Academy of Physician Associates describes the profession's origins and its development in response to a need for additional medical providers: AAPA: History of PAs. Duke University also documents the founding of the first physician assistant program in 1965: Duke PA Program History.

QUESTION NO: 23

Which of the following disaster recovery test plans will be MOST effective while providing minimal risk?

A. Read-through

B. Parallel

C. Full interruption

D. Simulation

ANSWER: B

Explanation:

Parallel is the most effective test approach that maintains minimal operational risk because recovery systems, procedures, personnel, and data-restoration capabilities can be exercised alongside normal production operations. The organization can validate that the alternate processing environment is available, that applications can run there, that required data can be restored and synchronized, and that recovery staff can perform their assigned activities. Since the primary production environment continues to provide live business services, the test does not deliberately interrupt patient-care or other critical operations. This gives management significantly stronger evidence of recoverability than a discussion-based exercise while avoiding the service-disruption exposure inherent in a full operational cutover.

NIST identifies parallel testing as a contingency-plan test in which systems are processed at the alternate site while primary-site processing continues. It is therefore a practical balance between realistic technical validation and controlled business risk. Test planning should still define success criteria, safeguards for test data, rollback procedures, and post-test lessons learned. See NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and CISA's contingency planning resource.

QUESTION NO: 24 - (SIMULATION)

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.

ANSWER: See the explanation for the answer

Explanation:

Best approach: The CISO should ensure the in-house PHI application and the college's related business processes are included in the University's BC/DR program. HIPAA compliance alone does not establish that the application can be recovered or that PHI will remain available during a disruption. Perform a business impact analysis (BIA), select and document recovery strategies, create/update the recovery plans, and test and maintain them with the college.

BC/DR phase order:

1. **Risk Assessment** (the phase described in the scenario)
2. **Business Impact Analysis (BIA)** — identify critical processes, dependencies, acceptable downtime, and recovery objectives.
3. **Develop Recovery/Continuity Strategies** — choose controls and recovery methods for the PHI application, data, infrastructure, and personnel.
4. **Develop and Implement the BC/DR Plan** — document roles, procedures, communications, backups, and restoration steps.
5. **Test, Train, and Exercise the Plan** — validate that the college can recover the application and PHI within required objectives.
6. **Maintain the Plan** — review and update it after changes, exercises, incidents, and periodic reassessments.

Therefore, place the remaining draggable phases after *Risk Assessment* in this sequence: **BIA → recovery/continuity strategy development → plan development/implementation → testing/training/exercises → maintenance.**

QUESTION NO: 25

True or false: For people with Medicaid coverage, access to health care is guaranteed.

A. True

B. False

ANSWER: B

Explanation:

False is correct because Medicaid coverage establishes eligibility for covered health services, but it does not guarantee that an individual can obtain care when and where it is needed. Actual access depends on practical factors such as whether clinicians and facilities participate in the person's Medicaid plan, availability of appointments, the adequacy of provider networks, geographic location, transportation, language access, and whether a particular service is available locally. People may also face administrative barriers related to enrollment, plan changes, referrals, or continuity of care.

Medicaid is jointly administered by federal and state governments, so benefits, delivery systems, and provider participation can vary by state. Enrollment therefore creates an important coverage entitlement, but coverage is distinct from access. From a healthcare privacy and security practitioner's perspective, this distinction matters because protected health information may be exchanged among plans, providers, and care-coordination organizations to support access, yet data sharing alone cannot ensure that a participating provider or timely appointment exists. The Centers for Medicare & Medicaid Services describes Medicaid as a source of health coverage, while federal reporting continues to evaluate beneficiaries' ability to obtain needed services. See Medicaid.gov: Medicaid overview and MACPAC: Access in Brief.

QUESTION NO: 26

Price inflation has been a major contributor to the rise of health care costs in the recent decades. This inflation has been due to:

A. Prices of health care rising more rapidly than prices in the overall economy.

B. An increase in the quantities of health care utilized relative to increases in the overall quantity of goods and services.

C. Both A and B

D. Factors other than price or quantity of health care.

ANSWER: A

Explanation:

Price inflation in health care refers specifically to health care prices increasing faster than prices across the overall economy. Health-spending analyses separate changes in spending into distinct drivers, commonly including price growth, the intensity or quantity of services used, population growth, and population aging. In that framework, the price component measures the effect of rising prices for health care goods and services, often compared with economy-wide inflation measures such as the gross domestic product price index or consumer price indexes.

Therefore, "Prices of health care rising more rapidly than prices in the overall economy." directly states the mechanism described by the question. A higher relative price means that the same type and amount of care costs more in real terms than it did previously, contributing to growth in total health expenditures. This distinction is important for health care security, privacy, and administration professionals because cost trends affect organizational budgeting, technology investment, vendor contracting, and resource prioritization. The Centers for Medicare & Medicaid Services discusses health spending growth and its price-related drivers in its National Health Expenditure Accounts materials: CMS National Health Expenditure Data. The Peterson-KFF Health System Tracker also presents evidence and context on health care prices and spending: Peterson-KFF Health System Tracker.

QUESTION NO: 27

What is a credential for Cancer Registrar?

A. AAPC

B. ACMCS

C. AHIMA

D. Certified Tumor Registrar (CTR), awarded through NCRA

ANSWER: D

Explanation:

The **Certified Tumor Registrar (CTR), awarded through the National Cancer Registrars Association (NCRA)**, is the recognized professional credential for cancer registrars. Cancer registrars collect, manage, analyze, and report cancer data used for patient care, cancer-program accreditation, public-health surveillance, research, and quality improvement. The CTR credential demonstrates that an individual has met established eligibility requirements and passed a competency-based examination addressing the specialized knowledge required for this work, including cancer registry operations, abstracting, coding and staging concepts, data quality, and reporting.

NCRA identifies the CTR as the standard certification for professionals in oncology data management and cancer registry practice. Maintaining the credential also reflects an ongoing commitment to professional development through continuing education and adherence to the profession's standards. Therefore, when a question asks for the credential associated with a cancer registrar, the specific credential is CTR; NCRA is the professional organization and certification body associated with it. See NCRA's Certified Tumor Registrar information and its professional association overview for details on the credential and the cancer registrar profession.

QUESTION NO: 28

Which of the following is the MOST significant benefit to implementing a third-party federated identity architecture?

A. Attribute assertions as agencies can request a larger set of attributes to fulfill service delivery

B. Data decrease related to storing personal information

C. Reduction in operational costs to the agency

D. Enable business objectives so departments can focus on mission rather than the business of identity management

ANSWER: C

Explanation:

Reduction in operational costs to the agency is the most significant benefit because a third-party federated identity architecture lets an agency rely on a trusted identity provider for functions that would otherwise require substantial internal resources. These functions can include identity proofing, credential lifecycle management, authentication infrastructure, account recovery, monitoring, and user-support processes. Rather than independently establishing and maintaining accounts and authentication mechanisms for every service, the agency can accept trusted identity assertions from the federated provider. This reduces duplicated technology, administrative effort, operational overhead, and the cost of maintaining specialized identity-management capabilities.

Federation also supports scalable access to multiple services while allowing the relying agency to concentrate its security and operational resources on its healthcare mission and service delivery. NIST explains that federation enables a relying party to use identity assertions from an identity provider and can reduce the burden of performing identity proofing and credential management itself. See NIST SP 800-63C: Federation and Assertions and NIST: Back to Basics—Federation and Assertions.

QUESTION NO: 29

All of the following were a result of the Flexner Report in 1910 EXCEPT.

A. Academic standards of medical schools became much more rigorous

B. Many medical schools closed

C. Homeopathic schools sanctioned homeopaths as "physicians"

D. Only schools meeting rigorous educational standards were able to award MD degrees

ANSWER: C

Explanation:

Homeopathic schools sanctioned homeopaths as "physicians" is the exception. Published in 1910 by the Carnegie Foundation, Abraham Flexner's report evaluated North American medical education and advocated a science-based model built on robust admission requirements, university affiliation, laboratory instruction, and clinical training. Its influence helped accelerate reform of medical education, including consolidation and closure of schools that could not support these expectations. Rather than endorsing or strengthening homeopathic medical education, the report treated homeopathic institutions critically and contributed to the broader movement toward standardized, scientific medical training. In this historical context, the report did not provide professional sanction for homeopaths as physicians. The Carnegie Foundation provides the original report and historical context at Medical Education in the United States and Canada. A scholarly overview of the report's role in reshaping medical education is also available through the National Library of Medicine.

QUESTION NO: 30

What is impact of the HITECH Act in relation to HIPAA requirements and maintaining client records electronically?

A. There is a push toward paper records to prevent the hacking and electronic violation of electronic records, which is easily done without detection

B. Providers must now maintain client records electronically, but may continue to provide clients a paper copy when access is requested

C. There is no requirement to maintain client records electronically, but clients have the right to insist on electronic access to an electronic health record, if it exists

D. Electronic records now face intensified scrutiny, requiring practitioners to implement more sophisticated software and detailed accounting of records

ANSWER: C

Explanation:

There is no requirement to maintain client records electronically, but clients have the right to insist on electronic access to an electronic health record, if it exists. HITECH did not create a universal requirement that every HIPAA covered entity adopt or maintain electronic health records. Instead, it strengthened individuals' access rights when protected health information is maintained electronically. Under the HITECH Act's amendments to HIPAA, when a covered entity uses or maintains an electronic health record with respect to an individual, the individual may obtain a copy of the information in an electronic format and may direct that it be transmitted to a designated person or entity, subject to applicable requirements and limitations. HIPAA's Privacy Rule similarly requires a covered entity to provide access in the requested electronic form and format when the protected health information is maintained electronically and the requested format is readily producible. This rule supports patient control, portability, and meaningful access to health information while recognizing that the law does not mandate electronic recordkeeping itself. The U.S. Department of Health and Human Services explains this electronic-access right in its HIPAA right of access guidance; the statutory HITECH provision is available through Public Law 111-5.

QUESTION NO: 31

Which of the following is the BEST reason to maintain an inventory of information systems and electronic protected health information locations?

A. To support a complete risk analysis

B. To eliminate the need for access controls

C. To avoid executing business associate agreements

D. To ensure every system stores the same data

ANSWER: A

Explanation:

To support a complete risk analysis is the best answer. An organization cannot adequately assess risks to electronic protected health information without identifying the systems, devices, applications, media, cloud services, and business processes in which the information is created, received, maintained, or transmitted. The inventory establishes the scope for identifying threats, vulnerabilities, existing safeguards, and potential impacts to confidentiality, integrity, and availability.

An inventory also supports asset ownership, access management, contingency planning, vendor oversight, patching, and incident response. However, its most fundamental compliance value is enabling a complete and accurate risk analysis, which is the foundation for the HIPAA Security Rule's risk-management process. See HHS guidance on risk analysis and 45 CFR § 164.308(a)(1).

QUESTION NO: 32

Each state has the same laws, rules, and/or regulations governing confidentiality of health care information.

A. True

B. False

ANSWER: B

Explanation:

False is correct because U.S. health-care confidentiality requirements are not uniform across all states. HIPAA establishes a federal baseline for protecting protected health information, but states can enact and enforce their own privacy and confidentiality statutes, regulations, professional rules, and medical-record requirements. Consequently, the scope of protected information, authorization requirements, patient access rights, breach-notification duties, retention requirements, and special protections for sensitive records may differ by jurisdiction.

HIPAA’s preemption framework specifically recognizes that a state law is not preempted when it is “more stringent” than the federal Privacy Rule with respect to the privacy of individually identifiable health information. Health-care organizations therefore must identify the laws applicable to the state or states in which they operate and apply the requirement that affords the appropriate level of privacy protection. This is particularly important for multistate providers, business associates, and organizations handling records involving categories that may receive additional state-level confidentiality protections. The U.S. Department of Health and Human Services describes how HIPAA interacts with state laws at HHS: HIPAA Privacy Rule and state laws. The federal preemption standard is codified at 45 CFR § 160.203.

QUESTION NO: 33

Under Title II of The Health Insurance Portability and Accountability Act, the administrative simplification provision:

A. Forbids individual health plans from denying coverage or imposing preexisting condition exclusions

B. Creates opportunities for fraud and abuse within the health care system

C. Requires the establishment of national standards for electronic health care transactions

D. Protects health insurance coverage for workers and their families

ANSWER: C

Explanation:

Under Title II of HIPAA, the administrative simplification provision requires the establishment of national standards for electronic health care transactions. This statutory framework was designed to improve the efficiency and consistency of administrative processes throughout the U.S. health-care system by standardizing how covered entities exchange certain electronic information, including claims, eligibility inquiries, payment and remittance advice, referrals, and enrollment transactions. Title II also provides for standards involving code sets, unique identifiers, security, and the privacy of individually identifiable health information. The Department of Health and Human Services implements these requirements through regulations in 45 CFR Part 162, which identifies the applicable transaction standards and requires covered entities to conduct covered electronic transactions in the adopted standard format. Standardization supports interoperable, predictable electronic exchanges between health plans, health-care clearinghouses, and providers, reducing the need for each organization to maintain incompatible proprietary formats. HHS describes Administrative Simplification as the HIPAA provisions establishing national standards for electronic health-care transactions and code sets, unique health identifiers, and rules protecting health information. See HHS Administrative Simplification and the transaction standards regulation at 45 CFR Part 162.

QUESTION NO: 34

Discovered the immunity to small pox.

A. Edward Jenner

B. Robert Koch

C. Hippocrates

ANSWER: A

Explanation:

Edward Jenner is correct because his late-eighteenth-century observations and experiments established the basis of immunity to smallpox through vaccination. Jenner observed that people who had contracted cowpox, a generally mild disease, appeared protected from the far more dangerous smallpox. In 1796, he tested this observation by inoculating James Phipps with material from a cowpox lesion and later demonstrating that Phipps did not develop smallpox after exposure. This work provided the first scientific demonstration that deliberate inoculation with a related agent could prevent smallpox infection.

Jenner's method became known as vaccination, a term derived from *vacca*, the Latin word for cow. His discovery was foundational to preventive medicine, immunology, and public health. Widespread smallpox vaccination ultimately enabled a global eradication campaign; the World Health Organization certified smallpox eradicated in 1980, making it the first human disease eradicated worldwide. The historical background and public-health significance of vaccination are described by the Centers for Disease Control and Prevention and the World Health Organization.

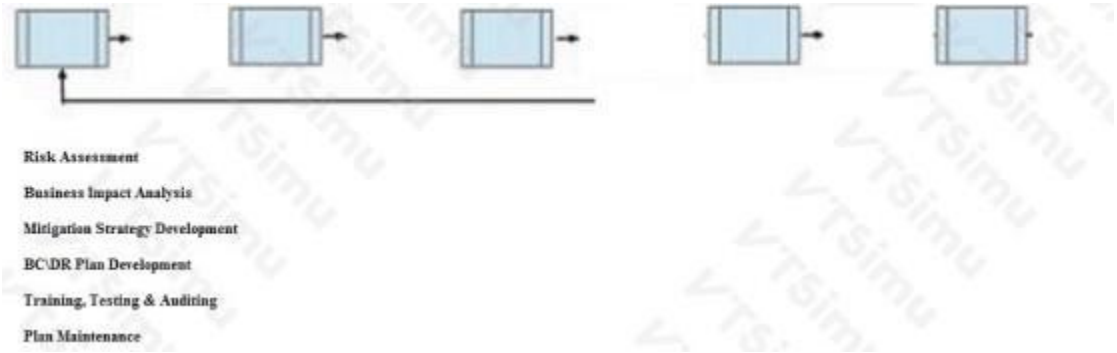
QUESTION NO: 35 - (DRAG DROP)

DRAG DROP

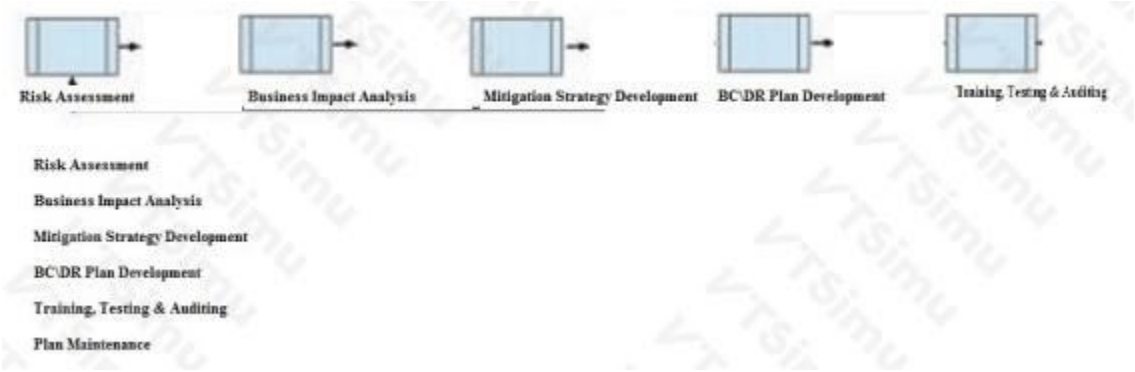
During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

Below are the common phases to creating a Business Continuity/Disaster Recovery (BC/DR) plan. Drag the remaining BC\DR phases to the appropriate corresponding location.



ANSWER:



Explanation:

The correct sequence follows the practical lifecycle used to establish a resilient business-continuity and disaster-recovery capability. It begins with **Risk Assessment**, which identifies relevant threats, vulnerabilities, likelihood, and potential impact to the college's application and the protected health information it handles. This establishes the risk context that the CISO needs before selecting continuity protections. Next, **Business Impact Analysis** determines which processes, systems, information, dependencies, recovery priorities, and recovery-time needs are most important to the organization. In a healthcare environment, this analysis helps ensure that an outage does not create unacceptable disruption to operations involving sensitive health data.

With the risks and business impacts understood, **Mitigation Strategy Development** identifies the safeguards and recovery approaches that can reduce disruption. These strategies are then documented and operationalized during **BC/DR Plan Development**, including recovery procedures, roles, communications, escalation paths, technical restoration steps, and required resources. The sequence then reaches **Training, Testing & Auditing**, where personnel practice their responsibilities and the organization validates that the documented plan can actually be executed under realistic conditions. Testing produces evidence of readiness and identifies improvements that should be incorporated through the organization's ongoing governance process.

This ordering is consistent with the continuity-planning process described by NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, which addresses business impact analysis, preventive controls and recovery strategies, plan development, testing/training/exercises, and plan maintenance. It also supports the HIPAA Security Rule expectation that covered entities and business associates establish contingency planning safeguards for electronic protected health information; see HHS HIPAA Security Rule guidance. The mapped sequence correctly reflects the diagram's assessment-through-validation workflow.

QUESTION NO: 36

What mandates all privacy in hospital administration?

A. HIPAA

B. JCAH

C. Medicare

ANSWER: A

Explanation:

HIPAA is the federal law that establishes the core U.S. privacy requirements applicable to hospitals and other covered health-care providers. Its Privacy Rule governs how protected health information may be used and disclosed, requires reasonable safeguards, gives individuals rights to access and request amendments to their records, and requires organizations to provide a notice of privacy practices. Hospital administration must implement policies, workforce training, access controls, complaint processes, and other administrative measures that support compliance with these requirements. HIPAA also applies to business associates that create, receive, maintain, or transmit protected health information for a covered entity, which is important because hospital information commonly passes through billing, technology, and other service providers. The U.S. Department of Health and Human Services explains that the Privacy Rule sets national standards protecting individuals' medical records and other identifiable health information held by covered entities. The controlling regulatory requirements are codified in the HIPAA Privacy Rule at 45 CFR Part 164, Subpart E. See the HHS HIPAA Privacy Rule overview and the electronic Code of Federal Regulations, 45 CFR Part 164 Subpart E.

QUESTION NO: 37

What mandates all privacy in hospital administration?

A. HIPAA

B. JCAH

C. Medicare

ANSWER: A

Explanation:

HIPAA is correct because the Health Insurance Portability and Accountability Act established the federal framework for protecting individuals' health information in the United States. In hospital administration, its Privacy Rule governs how covered entities, including hospitals, may use and disclose protected health information (PHI), and it establishes patients' rights to access and request amendments to their records. HIPAA also requires hospitals to implement appropriate policies, workforce training, administrative safeguards, and processes for handling privacy complaints and disclosures. The HIPAA Security Rule complements these privacy obligations by requiring safeguards for electronic protected health information, while the Breach Notification Rule establishes notification duties following certain impermissible uses or disclosures. Together, these rules make HIPAA the principal federal legal mandate directing health-information privacy practices in hospital operations. The U.S. Department of Health and Human Services explains the Privacy Rule and its application to covered entities at HHS HIPAA Privacy Rule. The statutory text and related HIPAA provisions are available through Public Law 104-191.