ISC.Premium.HCISPP.30q - DEMO

Number: HCISPP
Passing Score: 800
Time Limit: 120 min

Exam Code: HCISPP
Exam Name: HealthCare Information Security and Privacy Practitioner
Website: https://VCEup.com/
Team-Support: Support@VCEup.com

QUESTION 1
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
A health care provider is considering Internet access for their employees and patients. Which of the following is the organization's MOST secure solution for protection of data?

A. Public Key Infrastructure (PKI) and digital signatures
B. Trusted server certificates and passphrases
C. User ID and password
D. Asymmetric encryption and User ID

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
Which of the BEST internationally recognized standard for evaluating security products and systems?

A. Payment Card Industry Data Security Standards (PCI-DSS)
B. Common Criteria (CC)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Sarbanes-Oxley (SOX)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
The threat modeling identifies a man-in-the-middle (MITM) exposure. Which countermeasure should the information system security officer (ISSO) select to mitigate the risk of a protected Health information (PHI) data leak?

A. Auditing
B. Anonymization
C. Privacy monitoring
D. Data retention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
Which of the following is considered the last line defense in regard to a Governance, Risk managements, and compliance (GRC) program?

A. Internal audit
B. Internal controls
C. Board review
D. Risk management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
Which of the following is the BEST example of weak management commitment to the protection of security assets and resources?

A. poor governance over security processes and procedures
B. immature security controls and procedures
C. variances against regulatory requirements
D. unanticipated increases in security incidents and threats

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
Which of the following is the BEST reason for the use of security metrics?

A. They ensure that the organization meets its security objectives.
B. They provide an appropriate framework for Information Technology (IT) governance.
C. They speed up the process of quantitative risk assessment.
D. They quantify the effectiveness of security processes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
Which of the following is the BEST reason for writing an information security policy?

A. To support information security governance
B. To reduce the number of audit findings
C. To deter attackers

D. To implement effective information security controls

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
A covered healthcare provider which a direct treatment relationship with an individual need not:

A. provide the notice no later than the date of the first service delivery, including service delivered electronically
B. have the notice available at the service delivery site for individuals to request and keep
C. get a acknowledgement of the notice from each individual on stamped paper
D. post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered healthcare provider to be able to read it

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Health Information Rights although your health record is the physical property of the healthcare practitioner or facility that compiled it, the information belongs to you. You do not have the right to:

A. obtain a paper copy of the notice of information practices upon request inspect and obtain a copy of your health record as provided for in 45 CFR 164.524
B. request a restriction on certain uses and disclosures of your information outside the terms as provided by 45 CFR 164.522
C. amend your health record as provided in 45 CFR 164.528 obtain an accounting of disclosures of your health information as provided in 45 CFR 164.528
D. revoke your authorization to use or disclose health information except to the extent that action has already been taken

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
Title II of HIPPA includes a section, Administrative Simplification, not requiring:

A. Improved efficiency in healthcare delivery by standardizing electronic data interchange
B. Protection of confidentiality of health data through setting and enforcing standards
C. Protection of security of health data through setting and enforcing standards
D. Protection of availability of health data through setting and enforcing standards

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
Who is not affected by HIPPA?

A. clearing houses
B. banks

C. universities
D. billing agencies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
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 HIPPA authorities
B. by the health plan
C. by any other entity but the health plan
D. by insurance companies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
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 protect patient health information before this date
C. after taking permission, voluntarily protect patient health information before this date
D. compulsorily protect patient health information before this date

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
The HIPPA task force must first

A. inventory the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient care and central to the organization's business

B. inventory the organization's systems, processes, policies, procedures and data to determine which elements are non critical to patient care and central to the organization's business
C. inventory the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient complaints and central to the organization's peripheral businesses
D. modify the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient care and central to the organization's business

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
The confidentiality of alcohol and drug abuse patient records maintained by this program is protected by federal law and regulations. Generally, the program may not say to a person outside the program that a patient attends the program, or disclose any information identifying a patient as an alcohol or drug abuser even if:

A. The person outside the program gives a written request for the information
B. the patient consent in writing
C. the disclosure is allowed by a court order
D. the disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Incident handling is not related to disaster recovery, it is related to security incidents.
Explanation:

QUESTION 18
What is a Covered Entity? The term "Covered Entity" is defined in 160.103 of the regulation.

A. The definition is complicate and long.
B. The definition is referred to in the Secure Computing Act
C. The definition is very detailed.
D. The definition is deceptively simple and short

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
The HIPPA task force must inventory the organization's systems, processes, policies, procedures and data to determine which elements are critical to patient care and central to the organizations business. All must be inventoried and listed by

A. by priority as well as encryption levels, authenticity, storage-devices, availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused and carefully document all the criteria used.
B. by priority and cost as well as availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused and carefully document all the criteria used.
C. by priority as well availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused but need not document all the criteria used.
D. by priority as well as availability, reliability, access and use. The person responsible for criticality analysis must remain mission-focused and carefully document all the criteria used.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
HIPPA gave the option to adopt other financial and administrative transactions standards, "consistent with the goals of improving the operation of health care system and reducing administrative costs" to

A. ASCA prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003.
B. ASCA prohibits HHS from paying Medicare claims that are not submitted on paper after October 16, 2003
C. ASCA prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary grants a waiver from this requirement
D. No

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
May a health plan require a provider to use a health care clearinghouse to conduct a HIPPA-covered transaction, or must the health plan acquire the ability to conduct the transaction directly with those providers capable of conducting direct transactions?

A. 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. But the incremental cost of doing so must be borne by the health plan. It is a cost-benefit decision on the part of the health plan whether to acquire the ability to conduct HIPPA transactions directly with other entities, or to require use of a clearinghouse.
B. A health plan may not conduct it's covered transactions through a clearinghouse
C. A health plan may after taking specific permission from HIPPA authorities conduct its covered transactions through a clearinghouse
D. is not as per HIPPA allowed to require provider to conduct covered transactions with it through a clearinghouse

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Business Associate Agreements are required by the regulation whenever a business associate relationship exists. This is true even when the business associates are both covered entities.

A. There are no specific elements which must be included in a Business Associate Agreement.
However some recommended but not compulsory elements are listed in 164.504(e) (2)
B. There are specific elements which must be included in a Business Associate Agreement. These elements are listed Privacy Legislation
C. There are no specific elements which must be included in a Business Associate Agreement.
D. There are specific elements which must be included in a Business Associate Agreement. These elements are listed in 164.504(e) (2)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
The implementation Guides

A. are referred to in the Transaction Rule
B. are not referred to in the Transaction Rule
C. are referred to in the Compliance Rules
D. are referred to in the Confidentiality Rule

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Business Associates

A. are entities that perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity
B. are entities that do not perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity
C. are entities that perform services that require the use of Encrypted Insurance Information on behalf of Covered Entities. One covered entity may be a business partner of another covered entity
D. are entities that perform services that require the use of Protected Health Information on behalf of Covered Entities. One covered entity cannot be a business partner of another covered entity.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
Health Care Providers, however

A. become the business associates of health plans even without joining a network
B. become the business associates of health plans by simply joining a network

C. do not become the business associates of health plans by simply joining a network
D. do not become the HIPPA associates of health plans by simply joining a network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
In terms of HIPPA what an organization currently is doing in a specific area of their organization and compared current operations to other requirements mandated by state or federal law is called

A. HIPPA status analysis
B. gap analysis
C. comparison analysis
D. stop-gap analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
Group Health Plans sponsored or maintained by employers, however,

A. ARE SOMETIMES covered entities.
B. ARE NOT covered entities.
C. ARE covered entities
D. ARE called uncovered entities

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Employers often advocate on behalf of their employees in benefit disputes and appeals, answer Question:s with regard to the health plan, and generally help them navigate their health benefits. Is this type of assistance allowed under the regulation?

A. The final rule does nothing to hinder or prohibit plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plans.
B. The final rule prohibits plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plans
C. The final rule does hinder but does not prohibit plan sponsors from advocating on behalf of group health plan participants or providing assistance in understanding their health plans
D. The final rule does no advocating on behalf of group health plan participants or provide assistance in understanding their health plan.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: