HealthCare Information Security and Privacy Practitioner

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

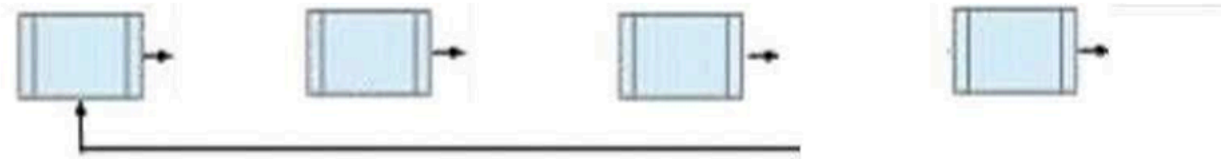
C. Perform a quantitative threat assessment

D. Notate the information and move on

Answer(s): B

---

2. DRAG DROP (Drag & Drop is not supported)
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.



Risk Assessment

Business Impact Analysis

Mitigation Strategy Development

BC\DR Plan Development

Training, Testing & Auditing

Plan Maintenance

A. See Explanation section for answer.

Answer(s): A

---

3. 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 UserID

Answer(s): A

---

4. 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)

Answer(s): B

---

5. 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

Answer(s): B

---

6. 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

Answer(s): B

---

7. 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

Answer(s): A

---

8. 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.

Answer(s): B

---

9. 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

Answer(s): A

---

10. 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

Answer(s): C

---

11. 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 CFR164.522

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

Answer(s): B

---

12. 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

Answer(s): D

---

13. Who is not affected by HIPPA?

A. clearing houses

B. banks

C. universities

D. billing agencies

Answer(s): B

---

14. 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 inmost healthcare transaction and administrative information systems

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

Answer(s): B

---

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 HIPPA authorities

B. by the health plan

C. by any other entity but the health plan

D. by insurance companies

Answer(s): B

---

16. 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

Answer(s): B

---

17. 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

Answer(s): A

---

18. 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 inwriting

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.

Answer(s): D

---

19. 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

Answer(s): D

---

20. 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(s): B
