



Vendor: ISC2

Exam Code: HCISPP

Exam Name: HealthCare Information Security and Privacy
Practitioner

Version: DEMO

QUESTION 1

Which one of the following is NOT a fundamental component of a Regulatory Security Policy?

- A. What is to be done.
- B. When it is to be done.
- C. Who is to do it.
- D. Why is it to be done

Answer: C

Explanation:

Regulatory Security policies are mandated to the organization but it up to them to implement it. "Regulatory - This policy is written to ensure that the organization is following standards set by a specific industry and is regulated by law. The policy type is detailed in nature and specific to a type of industry. This is used in financial institutions, health care facilities, and public utilities."

QUESTION 2

Which of the following embodies all the detailed actions that personnel are required to follow?

- A. Standards
- B. Guidelines
- C. Procedures
- D. Baselines

Answer: C

Explanation:

As stated in the dictionary, here are 3 definitions of procedure:

1. A manner of proceeding; a way of performing or effecting something: standard procedure.
2. A series of steps taken to accomplish an end: a medical procedure; evacuation procedures.
3. A set of established forms or methods for conducting the affairs of an organized body such as a business, club, or government.

QUESTION 3

Under HIPAA, what is the entity that processes healthcare claims and performs related functions for a health plan?

- A. Policy Advisory Group
- B. Third Party Administrator
- C. Joint Commission on Accreditation of Healthcare Organizations
- D. Plan Sponsor

Answer: B

Explanation:

A Third Party Administrator processes healthcare claims and performs related functions for a health plan.

QUESTION

When responding to a client's request for information about the disclosure of his/her protected health information, which is NOT required?

- A. The purpose of the disclosure
- B. A description of what information was sent

- C. Disclosures for treatment, payment, or health care operations
- D. The dates of disclosure and to whom the information was sent

Answer: C

Explanation:

When responding to a client's request for information about the disclosure of his/her protected health information, the health care provider must account for the disclosures by including a description of what information was sent, the dates of disclosure and to whom the information was sent, and the purpose of the disclosure. This information should be presented to the client in writing.

QUESTION 5

Part of Administrative Safeguards under HIPAA is Workforce Security measures. Which is NOT a key element of a Workforce Security Element?

- A. Identification of barriers to client electronic Personal Health Information
- B. Clearance Procedures
- C. Termination Procedures
- D. Authorization and Supervision

Answer: A

Explanation:

Identification of barriers to client electronic Personal Health Information is more indicative of Risk Assessment, not Workforce Security.

QUESTION 6

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:

The impact of the HITECH Act in relation to HIPAA requirements and maintaining client records electronically is that there is no requirement yet to maintain client records electronically, but clients have the right to insist on electronic access to an electronic health record, if it exists.

QUESTION 7

Which is NOT one of the three major categories of Security Safeguards identified by HIPAA in the regulations?

- A. Administrative
- B. Professional
- C. Physical

D. Technical

Answer: B

Explanation:

The three identified major categories of Security Safeguards are administrative, physical, and technical.

QUESTION 8

Which is NOT consistent with Personnel Clearance Procedures needed to comply with HIPAA Administrative Safeguards?

- A. Current database of what personnel has access to buildings, offices, filing cabinets, computers, and databases
- B. New employees, contractors, and unpaid staff have references checked
- C. Appropriate exit interviews for outgoing personnel
- D. Discretion given to who does and does not have access to secure office spaces or keys/door codes

Answer: C

Explanation:

Appropriate exit interviews for outgoing personnel is least consistent with personnel clearance procedures needed to comply with Administrative Safeguards.

QUESTION 9

Marcus is responsible for security management within a HIPAA-covered entity. He is reviewing administrative safeguards and examining the organization's risk analysis. Which element is NOT part of risk analysis?

- A. Developing adequate communication with all contractors, interns, and staff in relation to the agency's security policies
- B. Assessing vulnerabilities of integrity and availability of electronic personal health information
- C. Determining how client electronic personal health information confidentiality may be compromised
- D. Determining barriers in existence to needed client electronic personal health information

Answer: A

Explanation:

Developing communication is not a function of risk analysis.

QUESTION 10

Under the HIPAA Privacy Rule, who is NOT considered a covered entity?

- A. Clearinghouse
- B. Client patient
- C. Health practitioner
- D. Third party

Answer: B

Explanation:

A health care provider, health plan, and a clearinghouse are all considered covered entities. HIPAA compliance is required of all covered entities.

QUESTION 11

Which is NOT an element of Security Awareness Training?

- A. Determination that all staff will receive security training
- B. Policy related to documentation of all security training
- C. Procedural issues of who will terminate user access
- D. Training on vulnerabilities of the electronic Protected Health Information policies

Answer: C

Explanation:

Procedural issues of who will terminate user access is not an element of Security Awareness Training.

QUESTION 12

Under HIPAA Administrative Simplification, what must covered entities do in relation to submission of claims?

- A. Provide standardized format in electronic or paper form
- B. Request permission for use of specific privacy software
- C. Purchase and install approved privacy software
- D. Provide standardized electronic claim formatting

Answer: D

Explanation:

Under HIPAA Administrative Simplification, covered entities must provide standardized electronic claims.

QUESTION 13

As of 2010, what is different with regard to business associates and HIPAA protections?

- A. Business associates now must notify clients directly of privacy breaches, as if they were a covered entity
- B. There are no significant changes in business associate practices
- C. Covered entities have increased responsibilities to ensure the practice of business associates
- D. Business associates are no longer required to notify clients directly of privacy breaches

Answer: A

Explanation:

As of 2010, business associates must notify clients directly of privacy breaches, as if they were a covered entity.

QUESTION 14

HIPAA requires a response and reporting of security incidents. What is required when an organization has an attempted unauthorized access of protected health information?

- A. HIPAA must be notified
- B. Nothing is required of an attempted unauthorized access
- C. The organization must respond and notify the appropriate parties
- D. Federal authorities must be notified

Answer: C

Explanation:

When an organization has an attempted unauthorized access of protected health information the organization must respond and notify the appropriate parties.

QUESTION 15

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:

Title II of HIPAA, the Administrative Simplification provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

QUESTION 16

What data-related concept identifies or characterizes entities and events in a manner that facilitates an administrative process?

- A. Non-medical or Administrative Code Sets
- B. Data Mapping
- C. Medical or Clinical Code Sets
- D. Data Elements

Answer: A

Explanation:

Non-medical or Administrative Code Sets identify or characterize entities and events in a manner that facilitates an administrative process.

QUESTION 17

Title I of The Health Insurance Portability and Accountability Act protects:

- A. Electronic health care transactions
- B. Client's medical records
- C. Restrictions that a group health plan can place on benefits for preexisting conditions
- D. Health insurance coverage for workers and their families

Answer: D

Explanation:

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title I prohibits any group health plan from creating eligibility rules or assessing premiums for individuals in the plan based on health status, medical history, genetic information, or disability. Title I also limits restrictions that a group health plan can place on benefits for preexisting conditions.

QUESTION 18

Do the same requirements apply to both medical records and mental health records?

- A. No, a client is not allowed to have access to any part of a mental health record, with or without psychotherapy notes
- B. Generally, including conditioning enrollment in a plan on the client granting authorization for disclosure of psychotherapy notes
- C. Yes, and client is entitled to all of the same information in both settings
- D. Generally, psychotherapy notes are not included in the provision that allows clients to see and copy their health information

Answer: D

Explanation:

Both medical records and mental health records have generally the same requirements, however, psychotherapy notes are not included in the provision that allows clients to see and copy their health information.

QUESTION 19

HIPAA's Administrative Simplification procedures were prompted by the desire to:

- A. Reduce administrative overhead in provider-payer transactions
- B. Simplify administrative functions such as payroll and benefits
- C. Create multiple forms for various transactions
- D. Add more details to the processing of electronic transactions

Answer: A

Explanation:

HIPAA's Administrative Simplification procedures were prompted by the desire to reduce administrative overhead in provider-payer transactions. By having one form for each type of transaction, the chances of doing the transactions electronically and semi-automating the process are improved.

QUESTION 20

_____ is one of the main objectives of HIPAA.

- A. Secrecy
- B. Accountability
- C. Anonymity
- D. Complexity

Answer: B

Explanation:

The main objectives of HIPAA are Accountability (reduce waste, fraud, and abuse; new penalties will be imposed), Insurance Reform (continuity and portability of health insurance, providing limits on pre-existing provisions), and Administrative simplification (standards on electronic data transactions in a confidential and secure manner).

QUESTION 21

If a medical entity is in compliance with the Division of Medical Assistance's (DMA's) Health Data

Marketing Guidelines, is the entity in compliance with HIPAA guidelines?

- A. No. HIPAA is law while DMA guidelines are not law, and require less than HIPAA
- B. Yes. HIPAA is federal law and DMA is state law, which is usually more restrictive, and the more restrictive standard should be met.
- C. No. HIPAA law is federal and DMA law is state, so HIPAA supersedes DMA law.
- D. Yes. DMA's guidelines are stricter and will supersede those minimum standards of HIPAA.

Answer: A

Explanation:

If a medical entity is in compliance with the Division of Medical Assistance's (DMA's) Health Data Marketing Guidelines, they are not in compliance with HIPAA guidelines because HIPAA is law while DMA guidelines are not, requiring less than HIPAA.

QUESTION 22

If a client requests a restriction for disclosure of a certain part of their PHI to a health plan, the health care provider is:

- A. Required to agree to the requested restriction if the disclosure is for treatment or payment, is not required by law, and if the information is specifically related to a health care item or service that the client has paid for in full
- B. Required to agree only if the client specifies why he/she wants the restriction
- C. Required to agree only if the client specifies who he/she wants the restriction to apply to
- D. Required to agree to the requested restriction

Answer: A

Explanation:

A client can request a restriction of a certain part of their medical record for treatment, payment, and healthcare options. The client can also request restriction of medical information to people involved in their care (i.e., friends and family). The client should specify why he/she wants the restriction and who he/she wants the restriction to apply to. Under the "Final Rule" for HIPAA issued in 2013, a client can request to restrict disclosures of their health information and that request has to be granted by the provider if

1) the disclosure is for treatment or payment, 2) the disclosure is not required by law, and 3) the information is specifically related to a healthcare item or service that the client has paid for in full.

QUESTION 23

February 17, 2010 was the effective date for updated changes to HIPAA triggered by the Health Information Technology for Economic and Clinical Health Act (HITECH). As part of HITECH, what must providers who have clients who opt to self-pay do when those clients request the provider not inform their health care insurance provider?

- A. The provider has the option to not disclose the information to the health care insurance provider
- B. The provider must disclose the information anyway to the health care insurance provider
- C. The provider must not disclose the information to the health care insurance provider
- D. The provider must have the client sign a waiver freeing the provider from the compulsion to report to the provider

Answer: C

Explanation:

The provider must not disclose the information to the health care provider under the new rules. Previously, the provider's compliance with the request was optional under HIPAA guidelines.

QUESTION 24

HIPAA guidelines say employers that sponsor employee group health plans must maintain privacy of which _____ in secured locations, if kept in the office?

- A. Information related to lawsuits against employers
- B. Enrollment and claim information
- C. Workman's Compensation claims
- D. Deidentified information

Answer: B

Explanation:

Enrollment and claim information must be kept locked and secured if maintained in office spaces.

QUESTION 25

Under HIPAA, Regional Health Information Organizations and Personal Health Record Vendors are considered to be:

- A. Health care clearinghouses
- B. Business associates
- C. Covered entities
- D. Personal health care vendors

Answer: B

Explanation:

Under HIPAA, Regional Health Information Organizations and Personal Health Record Vendors are considered to be business associates.

QUESTION 26

What administrative safeguard puts into place measures to assure that only authorized persons have access to electronic personal health information?

- A. Log-in monitoring
- B. Information management
- C. Workforce security
- D. Termination procedures

Answer: C

Explanation:

Workforce security puts into place measures to assure that only authorized persons have access to electronic personal health information.

Thank You for Trying Our Product

Passleader Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.passleader.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14