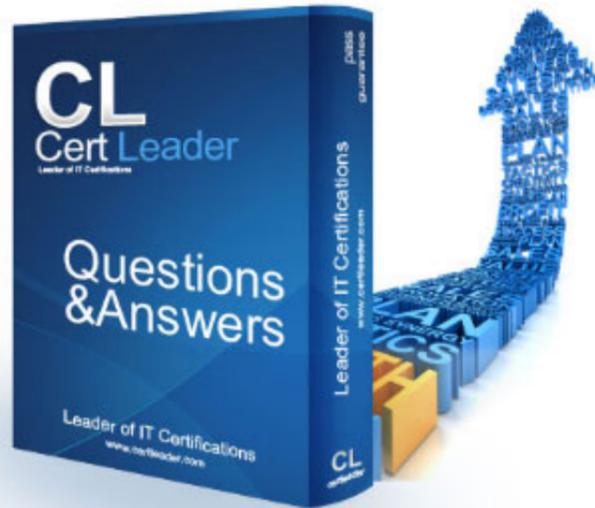


HIO-201 Dumps

Certified HIPAA Professional

<https://www.certleader.com/HIO-201-dumps.html>



NEW QUESTION 1

Which of the following is example of "Payment" as defined in the HIPAA regulations?

- A. Annual Audits
- B. Claims Management
- C. Salary disbursement to the workforce having direct treatment relationships.
- D. Life Insurance underwriting
- E. Cash given to the pharmacist for the purchase of an over-the-counter drug medicine

Answer: B

NEW QUESTION 2

Conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI is:

- A. Risk Analysis
- B. Risk Management
- C. Access Establishment and Modification
- D. Isolating Health care Clearinghouse Function
- E. Information System Activity Review

Answer: B

NEW QUESTION 3

The objective of this HIPAA security standard is to implement policies and procedures to prevent, detect, contain, and correct security violations.

- A. Security Incident Procedures
- B. Assigned Security Responsibility
- C. Security Management Process
- D. Access Control
- E. Facility Access Control

Answer: C

NEW QUESTION 4

Assigning a name and/or number for identifying and tracking users is required by which security rule implementation specification?

- A. Access Authentication
- B. Integrity Controls
- C. Authorization and/or Supervision
- D. Data Authentication
- E. Unique User Identification

Answer: E

NEW QUESTION 5

Within the context of a transaction set, the fields that comprise a hierarchical level are referred to as a(n):

- A. Loop.
- B. Enumerator.
- C. Identifier
- D. Data segment.
- E. Code set.

Answer: A

NEW QUESTION 6

Which of the following is NOT a HIPAA national health care identifier?

- A. National Provider Identifier (NPI)
- B. Social Security Number (SSN)
- C. National Health Plan Identifier (PlanID)
- D. National Employer Identifier for Health Care (EIN)
- E. National Health Identifier for Individuals (NHII)

Answer: B

NEW QUESTION 7

ANSI X12 specifies the use of a (an):

- A. Simple flat file structure for transactions.
- B. Envelope structure for transactions.
- C. Employer identifier.
- D. Health plan identifier
- E. Provider identifier.

Answer: B

NEW QUESTION 8

Select the correct statement regarding the administrative requirements of the HIPAA privacy rule.

- A. A covered entity must designate, and document, a privacy official, security officer and a HIPAA compliance officer
- B. A covered entity must designate, and document, the same person to be both privacy official and as the contact person responsible for receiving complaints and providing further information about the notice required by the regulations.
- C. A covered entity must implement and maintain written or electronic policies and procedures with respect to PHI that are designed to comply with HIPAA standards, implementation specifications and other requirements.
- D. A covered entity must train, and document the training of, at least one member of its workforce on the policies and procedures with regard to PHI as necessary and appropriate for them to carry out their function within the covered entity no later than the privacy rule compliance date
- E. A covered entity must retain the document required by the regulations for a period of ten years from the time of its creation or the time it was last in effect, whichever is later.

Answer: C

NEW QUESTION 9

Select the best statement regarding de-identified information (DII).

- A. De-identified information is PHI that has had all individually (patient) identifiable information removed.
- B. PHI may be used only with the authorization of the individual.
- C. PHI remains PHI.
- D. The only approved method of de-identification is to have a person with appropriate knowledge and experience de-identify the PHI.
- E. All PHI use and disclosure requirements do not apply to re-identified DII.

Answer: A

NEW QUESTION 10

This code set is used to describe or identify radiological procedures and clinical laboratory tests:

- A. ICD-9-CM, Volumes 1 and 2.
- B. CPT-4.
- C. CDT.
- D. ICD-9-CM, Volume 3.
- E. HCPCS.

Answer: E

NEW QUESTION 10

The implementation specifications for this HIPAA security standard (within Technical Safeguards) must support emergency access and unique user identification:

- A. Audit Control
- B. Integrity
- C. Access Control
- D. Person or Entity Authentication
- E. Transmission Security

Answer: C

NEW QUESTION 15

The National Provider File (NPF) includes information such as:

- A. Effective date.
- B. CPT-4.
- C. CDT.
- D. ICD-9-CM.
- E. Enrollment date.

Answer: A

NEW QUESTION 16

A hospital is preparing a file of treatment information for the state of California. This file is to be sent to external medical researchers. The hospital has removed SSN, name, phone and other information that specifically identifies an individual. However, there may still be data in the file that potentially could identify the individual. Can the hospital claim "safe harbor" and release the file to the researchers?

- A. Yes - the hospital's actions satisfy the "safe harbor" method of de-identification.
- B. No - a person with appropriate knowledge and experience must determine that the information that remains cannot identify an individual.
- C. No - authorization to release the information is still required by HIPAA
- D. No - to satisfy "safe harbor" the hospital must also have no knowledge of a way to use the remaining data to identify an individual.
- E. Yes - medical researchers are covered entities and "research" is considered a part of "treatment" by HIPAA.

Answer: D

NEW QUESTION 18

As part of their HIPAA compliance process, a small doctor's office formally puts the office manager in charge of security related issues. This complies with which security rule standard?

- A. Security Awareness and Training
- B. Security Management Process
- C. Access Control
- D. Assigned Security Responsibility
- E. Security Incident Procedures

Answer: D

NEW QUESTION 19

Select the correct statement regarding the requirements of HIPAA regulations.

- A. A covered entity must have and apply sanction against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity)
- B. A covered entity does not need to train all members of its workforce whose functions are affected by a change in policy or procedure.
- C. A covered entity must designate, and document, a privacy officer, and a HIPAA compliance officer
- D. A covered entity may require individuals to waive their rights.
- E. A covered entity must require the individual to sign the Notice of Privacy Practices prior to delivering any treatment related service.

Answer: A

NEW QUESTION 20

Once a year, a team at ABC Hospital reviews environmental and operational changes that may have had an impact on the security of electronic PHI. This is an example of:

- A. Transmission Security
- B. Evaluation
- C. Audit Controls
- D. Integrity
- E. Security Management Process

Answer: B

NEW QUESTION 21

Establishing policies and procedures for responding to an emergency or other occurrence that damages systems is an example of a(n):

- A. Security Awareness and Training
- B. Security Incident Procedure
- C. Information Access Management
- D. Security Management Process
- E. Contingency Plan

Answer: E

NEW QUESTION 22

An Electronic Medical Record (EMR):

- A. Is another name for the Security Ruling.
- B. Requires the use of biometrics for access to records.
- C. Is electronically stored information about an individual's health status and health care.
- D. Identifies all hospitals and health care organizations.
- E. Requires a PKI for the provider and the patient.

Answer: C

NEW QUESTION 23

Processes enabling an enterprise to restore any lost data in the event of fire, vandalism, natural disaster, or system failure are defined under:

- A. Risk Analysis
- B. Contingency Operations
- C. Emergency Mode Operation Plan
- D. Data Backup Plan
- E. Disaster Recover Plan

Answer: E

NEW QUESTION 26

Workstation Use falls under which Security Rule area?

- A. Person or Entity Authentication
- B. Technical Safeguards
- C. Administrative Safeguards
- D. Physical Safeguards
- E. Transmission Security

Answer: D

NEW QUESTION 28

Patient identifiable information may include:

- A. Country of birth.
- B. Telephone number.
- C. Information on past 3 employers.
- D. Patient credit reports.
- E. Smart card-based digital signatures.

Answer: B

NEW QUESTION 30

The code set that must be used to describe or identify outpatient physician services and procedures is:

- A. ICD-9-CM, Volumes 1 and 2
- B. CPT-4
- C. CDT
- D. ICD-9-CM, Volume 3
- E. NDC

Answer: B

NEW QUESTION 34

When limiting protected health information (PHI) to the minimum necessary for a use or disclosure, a covered entity can use:

- A. Their professional judgment and standards.
- B. The policies set by the security rule for the protection of the information.
- C. Specific guidelines set by WEDI.
- D. Measures that are expedient and reduce costs.
- E. The information for research and marketing purposes only.

Answer: A

NEW QUESTION 35

Select the correct statement regarding code sets and identifiers.

- A. The social security number has been selected as the National Health Identifier for individuals.
- B. The COT code set is maintained by the American Medical Association.
- C. Preferred Provider Organizations (PPO) are not covered by the definition of "health plan" for purposes of the National Health Plan Identifier
- D. HIPAA requires health plans to accept every valid code contained in the approved code sets
- E. An important objective of the Transaction Rule is to reduce the risk of security breaches through identifiers.

Answer: D

NEW QUESTION 36

Information in this transaction is generated by the payer's adjudication system:

- A. Eligibility (270/271)
- B. Premium Payment (820)
- C. Unsolicited Claim Status (277)
- D. Remittance Advice (835)
- E. Functional Acknowledgment (997)

Answer: D

NEW QUESTION 41

Select the FALSE statement regarding violations of the HIPAA Privacy rule.

- A. Covered entities that violate the standards or implementation specifications will be subjected to civil penalties of up to \$100 per violation except that the total amount imposed on any one person in each calendar year may not exceed \$25,000 for violations of one requirement
- B. Criminal penalties for non-compliance are fines up to \$65,000 and one year in prison for each requirement or prohibition violated
- C. Criminal penalties for willful violation are fines up to \$50,000 and one year in prison for each requirement or prohibition violated.
- D. Criminal penalties for violations committed under "false pretenses" are fines up to \$100,000 and five years in prison for each requirement or prohibition violated
- E. Criminal penalties for violations committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm are fines up to \$250,000 and ten years in prison for each requirement or prohibition violated

Answer: B

NEW QUESTION 45

Select the correct statement regarding the requirements for oral communication in the HIPAA regulations.

- A. Covered entities must reasonably safeguard PHI, including oral communications, from any intentional or unintentional use or disclosure that is in violation of the

Privacy Rule.

- B. Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of de-identified data.
- C. Covered entities are prohibited from marketing through oral communications
- D. The Privacy Rule requires covered entities to document any information, including oral communications, which is used or disclosed for TPO purposes.
- E. The Privacy Rule will often require major structural changes, such as soundproof rooms and encryption of telephone systems, to provide the "reasonable safeguards" of oral communications required by the regulations

Answer: A

NEW QUESTION 48

The Security Rule requires that the covered entity identifies a security official who is responsible for the development and implementation of the policies and procedures. This is addressed under which security standard?:

- A. Security Incident Procedures
- B. Response and Reporting
- C. Assigned Security Responsibility
- D. Termination Procedures
- E. Facility Access Controls

Answer: C

NEW QUESTION 50

Which of the following is primarily concerned with implementing security measures that are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

- A. Access Establishment and Modification
- B. Isolating Health care Clearinghouse Functions
- C. Information System Activity Review
- D. Risk Management
- E. Risk Analysis

Answer: D

NEW QUESTION 54

A pharmacist is approached by an individual and asked a question about an over-the-counter medication. The pharmacist needs some protected health information (PHI) from the individual to answer the question. The pharmacist will not be creating a record of this interaction. The Privacy Rule requires the pharmacist to:

- A. Verbally request 3 consent and offer a copy of the Notice of Privacy Practices.
- B. Verbally request specific authorization for the PHI.
- C. Do nothing more.
- D. Obtain the signature of the patient on their Notice of Privacy Practices.
- E. Not respond to the request without an authorization from the primary physician.

Answer: C

NEW QUESTION 59

This rule covers the policies and procedures that must be in place to ensure that the patients' health information is respected and their rights upheld:

- A. Security rule.
- B. Privacy rule.
- C. Covered entity rule.
- D. Electronic Transactions and Code Sets rule.
- E. Electronic Signature Rule.

Answer: B

NEW QUESTION 62

A State insurance commissioner is requesting specific, individually identifiable information from an insurer as a part of a routine review of the insurer's practices. What must the insurer do to deidentify the information?

- A. The protected health information must be removed from the informatio
- B. A substitute "key" may be supplied to allow re-identification, if needed.
- C. Limit the information to coverage, dates of treatment, and payment amounts to avoid collecting any protected data.
- D. Nothin
- E. An oversight agency has the right to access this information without prior authorization.
- F. Request that the insurance commissioner ask for an exception from HIPAA from the Department of Health and Human Services.
- G. A written authorization is required from the patient.

Answer: C

NEW QUESTION 66

The security standard that has the objective of implementing mechanisms to record and examine system activity is:

- A. Access Control
- B. Audit Controls
- C. Authorization Controls

- D. Data Authentication
- E. Person or Entity Authentication

Answer: B

NEW QUESTION 67

Select the FALSE statement regarding the X12N Implementation Guides.

- A. The Washington Publishing Company has the exclusive rights to publish the X12N Implementation Guides.
- B. HHS has adopted the Implementation Guides as standards for HIPAA transactions.
- C. The guides are intended to be instructive and need not be followed strictly.
- D. The guides may be downloaded free from WPC's Website.
- E. The guides explain the usage of the transaction set segments and data elements.

Answer: C

NEW QUESTION 70

ABC Hospital implements policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information. These policies and procedures satisfy which HIPAA security standard?

- A. Security Management Process
- B. Facility Access Control
- C. Security Awareness and Training
- D. Workforce Security
- E. Security Management Process

Answer: D

NEW QUESTION 74

Select the correct statement regarding the 834 - Benefit Enrollment and Maintenance transaction.

- A. It cannot be used to transfer enrollment information from a plan sponsor to a health care insurance company or other benefit provider.
- B. It can be used by a health insurance company to notify a plan sponsor that it has dropped one of its members.
- C. It cannot be used to enroll, update, or dis-enroll employees and dependents in a health plan.
- D. A sponsor can be an employer, insurance agency, association or government agency but unions are excluded from being plan sponsors.
- E. It can be used in either update or full replacement mode.

Answer: E

NEW QUESTION 75

One characteristic of the Notice of Privacy Practices is:

- A. It must be written in plain, simple language
- B. It must explicitly describe all uses of PHI
- C. A description about the usage of hidden security cameras for tracking patient movements for implementing privacy.
- D. A description of the duties of the individual
- E. A statement that the individual must abide by the terms of the Notice.

Answer: A

NEW QUESTION 77

The objective of this document is to safeguard the premises and building from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering and theft

- A. Contingency Plan
- B. Facility Security Plan
- C. Emergency Mode Operation Plan
- D. Accountability
- E. Device and Media Controls

Answer: B

NEW QUESTION 79

The transaction number assigned to the Benefit Enrollment and Maintenance transaction is:

- A. 270
- B. 276
- C. 278
- D. 280
- E. 834

Answer: E

NEW QUESTION 82

This Administrative Safeguard standard implements policies and procedures to ensure that all members of its workforce have appropriate access to electronic

information.

- A. Security Awareness Training
- B. Workforce Security
- C. Facility Access Controls
- D. Workstation Use
- E. Workstation Security

Answer: B

NEW QUESTION 84

The key objective of a contingency plan is that the entity must establish and implement policies and procedures to ensure the:

- A. Creation and modification of health information during and after an emergency.
- B. Integrity of health information during and after an emergency.
- C. Accountability of health information during and after an emergency.
- D. Vulnerability of health information during and after an emergency.
- E. Non-repudiation of the entity.

Answer: B

NEW QUESTION 86

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your HIO-201 Exam with Our Prep Materials Via below:

<https://www.certleader.com/HIO-201-dumps.html>