



HIPAA

Exam Questions HIO-201

Certified HIPAA Professional

NEW QUESTION 1

Security to protect information assets is generally defined as having:

- A. Controls
- B. PKI
- C. Biometrics
- D. VPN technology
- E. Host-based intrusion detection

Answer: A

NEW QUESTION 2

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 3

When using the Health Care Eligibility Request/Response (270/271), if a provider submits certain minimum information and the patient/subscriber is in their database, the payer must generate a response. Which of the following is one of the minimum information fields?

- A. Patient's country of birth
- B. Patient's pet name
- C. Patient's weight
- D. Patient's address
- E. Patient's date of birth

Answer: E

NEW QUESTION 4

A doctor sends patient records to another company for data entry services. A bonded delivery service is used for the transfer. The records are returned to the doctor after entry is complete, using the same delivery service. The entry facility and the network they use are secure. The doctor is named as his own Privacy Officer in written policies. The doctor has written procedures for this process and all involved parties are documented as having been trained in them. The doctor does not have written authorizations to disclose Protected Health Information (PHI). Is the doctor in violation of the Privacy Rule?

- A. No - This would be considered an allowed "routine disclosure" between the doctor and his business partner
- B. Yes - There is no exception to the requirement for an authorization prior to disclosure, no matter how well intentioned or documented.
- C. Yes - a delivery service is not considered a covered entity
- D. Yes - to be a ??routine disclosure?? all the parties must have their own Privacy Officer as mandated by HIPAA
- E. Yes - this is not considered a part of "treatment", which is one of the valid exceptions to the Privacy Rule

Answer: A

NEW QUESTION 5

Health information is protected by the Privacy Rule as long as:

- A. The authorization has been revoked by the physician.
- B. The patient remains a citizen of the United States.
- C. The information is under the control of HHS.
- D. The information is in the possession of a covered entity.
- E. The information is not also available on paper forms.

Answer: D

NEW QUESTION 6

HIPAA establishes a civil monetary penalty for violation of the Administrative Simplification provisions. The penalty may not be more than:

- A. \$1,000,000 per person per violation of a single standard for a calendar year.
- B. \$10 per person per violation of a single standard for a calendar year.
- C. \$25,000 per person per violation of a single standard for a calendar year.
- D. \$2,500 per person per violation of a single standard for a calendar year.
- E. \$1000 per person per violation of a single standard for a calendar year.

Answer: C

NEW QUESTION 7

Dr Jones, a practicing dentist, has decided to directly implement an EDI solution to comply with the HIPAA transaction rule Dr. Jones employs a small staff of 4 persons for whom he has sponsored a health care plan. Dr. Jones has revenues of less than \$1 million. Select the code set that Dr. Jones should consider supporting for his EDI system.

- A. 837 - Professional
- B. 834
- C. CPT-4
- D. 837 - Institutional
- E. CDT

Answer: E

NEW QUESTION 8

The version of the ANSI ASC X12N standard required by HIPAA regulations is:

- A. 3070
- B. 3050
- C. 3045
- D. 4010
- E. 4020

Answer: D

NEW QUESTION 9

This transaction type is a "response" transaction that may include information such as accepted/rejected claim, approved claim(s) pre-payment, or approved claim(s) post- payment:

- A. 270.
- B. 820
- C. 837.
- D. 277.
- E. 278.

Answer: D

NEW QUESTION 10

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 10

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 11

Implementing policies and procedures to prevent, detect, contain, and correct security violations is required by which security standard?

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

Answer: E

NEW QUESTION 12

One implementation specification of the Security Management Process is:

- A. Risk Analysis
- B. Authorization and/or Supervision
- C. Termination Procedures
- D. Contingency Operations
- E. Encryption and Decryption

Answer: A

NEW QUESTION 13

The Data Backup Plan is part of which Security Standard?

- A. Contingency Plan
- B. Evaluation
- C. Security Management Procedures
- D. Facility Access Control
- E. Security Incident Procedures

Answer: A

NEW QUESTION 14

A grouping of functional groups, delimited by a header/trailer pair, is called a:

- A. Data element
- B. Data segment
- C. Transaction set
- D. Functional envelope
- E. Interchange envelope

Answer: E

NEW QUESTION 17

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 21

Periodic testing and revision of contingency plans is addressed by:

- A. Testing and Revision Procedures
- B. Information System Activity Review
- C. Response and Reporting
- D. Data Backup Plan
- E. Emergency Access Procedure

Answer: A

NEW QUESTION 22

One implementation specification of a contingency plan is:

- A. Risk analysis
- B. Applications and Data Criticality Analysis
- C. Risk Management
- D. Integrity Controls
- E. Encryption

Answer: B

NEW QUESTION 24

This implementation specification might include actions such as revoking passwords, and collecting keys

- A. Sanction Policy
- B. access Authorization
- C. Facility Security Plan
- D. Termination Procedures
- E. Unique User Identification

Answer: D

NEW QUESTION 27

The transaction number assigned to the Health Care Eligibility Request transaction is:

- A. 270
- B. 276
- C. 278
- D. 271
- E. 834

Answer: A

NEW QUESTION 30

Which HIPAA Title is fueling initiatives within organizations to address health care priorities in the areas of transactions, privacy, and security?

- A. Title I.
- B. Title II
- C. Title III
- D. Title IV.
- E. Title V.

Answer: B

NEW QUESTION 33

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 34

Select the best example of a business associate (if they had access to PHI).

- A. Accountants
- B. Hospital employees
- C. A covered entity's internal IT department
- D. CEO of the covered entity
- E. The covered entity's billing service department

Answer: A

NEW QUESTION 37

HIPAA Security standards are designed to be:

- A. Technology specific
- B. State of the art
- C. Non-Comprehensive
- D. Revolutionary
- E. Scalable

Answer: E

NEW QUESTION 40

Title 1 of the HIPAA legislation in the United States is about:

- A. PKI requirements for hospitals and health care providers.
- B. Encryption algorithms that must be supported by hospitals and health care providers.
- C. Fraud and abuse in the health care system and ways to eliminate the same.
- D. Guaranteed health insurance coverage to workers and their families when they change employers.
- E. The use of strong authentication technology that must be supported by hospitals and health care providers.

Answer: D

NEW QUESTION 44

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 46

Formal, documented instructions for reporting security breaches are referred to as:

- A. Business Associate Contract
- B. Response and Reporting
- C. Emergency Access Procedure
- D. Sanction policy
- E. Risk Management

Answer:

B

NEW QUESTION 47

Select the best statement regarding the definition of protected health information (PHI).

- A. PHI includes all individually identifiable health information (IIHI).
- B. PHI does not include physician's hand written notes about the patient's treatment.
- C. PHI does not include PHI stored on paper.
- D. PHI does not include PHI in transit.
- E. PHI includes de-identified health information

Answer: A

NEW QUESTION 48

To comply with the Final Privacy Rule, a valid Notice of Privacy Practices:

- A. Is required for all Business Associate Contracts.
- B. Must always be associated with a valid authorization.
- C. Must be signed before providing treatment to a patient.
- D. Must be associated with a valid Business Associate Contract.
- E. Must describe the individual's rights under the Privacy Rule.

Answer: E

NEW QUESTION 52

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 54

The transaction number assigned to the Health Care Claim Payment/Advice transaction is:

- A. 270
- B. 276
- C. 834
- D. 835
- E. 837

Answer: D

NEW QUESTION 57

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 58

HIPAA defines transaction standards for:

- A. Encrypted communication between patient and provider.
- B. All patient events.
- C. Security.
- D. Benefits inquiry.
- E. Emergency treatment.

Answer: D

NEW QUESTION 61

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 64

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 65

This security standard requires that the covered entity establishes agreements with each organization with which it exchanges data electronically, protecting the security of all such data:

- A. Security Incident Procedures
- B. Integrity
- C. Person or Entity Authentication
- D. Assigned Security Responsibility
- E. Business Associate Contracts and other Arrangements

Answer: E

NEW QUESTION 67

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 69

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 70

Individually identifiable health information (IIHI) includes information that is:

- A. Transmitted to a business associate for payment purposes only.
- B. Stored on a smart card only by the patient.
- C. Created or received by a credit company that provided a personal loan for surgical procedures.
- D. Created or received by a health care clearinghouse for claim processing.
- E. Requires the use of biometrics for access to records.

Answer: D

NEW QUESTION 74

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 78

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 82

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 85

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 89

The Privacy Rule interacts with Federal and State laws by:

- A. Establishing an orderly hierarchy where HIPAA applies, then other Federal law, then State law.
- B. Defining privacy to be a national interest that is best protected by Federal law
- C. Allowing State privacy laws to provide a cumulative effect lower than HIPAA.
- D. Mandating that Federal laws preempt State laws regarding privacy.
- E. Establishing a "floor" for privacy protection.

Answer: E

NEW QUESTION 90

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 hearth 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 94

This transaction, which is not a HIPAA standard, may be used as the first response when receiving a Health Care Claim (837):

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

Answer: E

NEW QUESTION 97

The Integrity security standard has one addressable implementation standard which is:

- A. Encryption
- B. Authorization and/or Supervision
- C. Mechanism to Authenticate Electronic PHI
- D. Applications and Data Critically Analysis
- E. Isolating Health care Clearing House Functions

Answer: C

NEW QUESTION 100

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 105

This transaction is typically used in two modes: update and full replacement:

- A. Premium Payment.
- B. Health Care Claim.
- C. First Report of Injury.
- D. Health Plan Enrollment and Dis-enrollment.
- E. Coordination of Benefits.

Answer: D

NEW QUESTION 108

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 110

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 113

Performing a periodic review in response to environmental or operational changes affecting the security of electronic protected health information is called:

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

Answer: B

NEW QUESTION 114

The applicable methods for HIPAA-related EDI transactions are:

- A. Remote and enterprise.
- B. Claim status and remittance advice.
- C. Subscriber and payer
- D. Batch and real-time.
- E. HCFA-1500and837.

Answer: D

NEW QUESTION 119

Ensuring that physical access to electronic information systems and the facilities in which they are housed is limited, is addressed under which security rule standard?

- A. Security Management Process

- B. Transmission Security
- C. Person or Entity Authentication
- D. Facility Access Controls
- E. Information Access Management

Answer: D

NEW QUESTION 124

A key date in the transaction rule timeline is:

- A. October 16, 2003 - small health plans to begin testing without ASCA extension
- B. October 16, 2004 - full compliance deadline for small health plans
- C. April 16, 2004 - small health plans to begin testing with ASCA extension
- D. April 16, 2003 - deadline to begin testing with ASCA extension
- E. April 14, 2003; deadline to begin testing with the ASCA extension.

Answer: D

NEW QUESTION 128

Under the Privacy Rule, an individual may request a covered provider to restrict routine use or disclosure beyond what exists in the provider's Notice of Privacy Practices. Upon that request, the provider.

- A. Must store the information in an encrypted format.
- B. May refuse the request but still offer treatment.
- C. Must comply within seventy-five (75) days.
- D. Must only transfer the information using the ASC X12 format specification.
- E. Can request binding arbitration.

Answer: B

NEW QUESTION 130

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

HIO-201 Practice Exam Features:

- * HIO-201 Questions and Answers Updated Frequently
- * HIO-201 Practice Questions Verified by Expert Senior Certified Staff
- * HIO-201 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * HIO-201 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The HIO-201 Practice Test Here](#)