Vendor: HIPAA

Exam Code: HIO-201

Exam Name: Certified HIPAA Professional

Version: Demo

Question: 1

This final security rule standard addresses encryption of data,

A. Security Management Process
B. Device and Media Controls
C. Information Access Management
D. Audit Controls
E. Transmission Security

Answer: E

Question: 2

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

Question: 3

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

Question: 4

Implementation features of the Security Management Process include which one of the following?

A. Power Backup plan
B. Data Backup Plan
C. Security Testing
D. Risk Analysis
E. Authorization and/or Supervision

Answer: D

Question: 5

The Privacy Rule gives patients the following right

A. Access to the psychotherapy notes.
B. Request an amendment to their medical record.
C. Receive a digital certificate.
D. See an accounting of disclosures for which authorization was given.
E. The use of a smart card for accessing their records.

Answer: B

Question: 6

This transaction type may be used in three ways:
1. Reply to a Health Care Claim Status Request.
2. Unsolicited notification of a health care claim status.
3. Request for additional information about a health care claim.

A. 837.
B. 820.
C. 277.
D. 835.
E. 278.

Answer: C

Question: 7

The scope of the Privacy Rule includes:

A. All Employers.
B. The Washington Publishing Company
C. Disclosure of non-identifiable demographics.
D. Oral disclosure of PHI.
E. The prevention of use of de-identified information.

Answer: D

Question: 8

The Privacy Rule has broad administrative requirements. Which one of the following requirements is defined under the Privacy Rule?

A. Designate a security officer.
B. Document termination procedures.
C. Use biometrics to authenticate transactions.
D. Deploy tokens and smart cards to all medical personnel.
E. Verify that business associates treat patient information respectfully.

Answer: E

Question: 9

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 HIPA4.
D. Mandating that Federal laws preempt State laws regarding privacy.
E. Establishing a ‘floor” for privacy protection.

Answer: E

Question: 10

The code set that must be used to describe or identify inpatient hospital services and surgical procedures is:

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

Answer: D

Question: 11

The Privacy Rule's penalties for unauthorized disclosure:

A. Imposes fines and imprisonment as civil penalties for violations.
B. Limits penalties to covered entities and their business associates.
C. Imposes criminal penalties for noncompliance with standards.
D. Limits imprisonment to a maximum often years.
E. Is $1000 per event of disclosure.

Answer: D

Question: 12

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. B Security Management Process

Answer: D

Question: 13

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

Question: 14

Which transaction covers information specific to accidents?

A. Accident Report.
B. First Report of Injury.
C. Health Care Claim.
D. Health Care Claim Payment/Advice.
E. Premium Payment.

Answer: B

Question: 15

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 P1<1 for the provider and the patient.

Answer: C

Question: 16

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

Question: 17

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

Question: 18

The National Provider Identifier (NPI) will eventually replace the:

A. NPF .
B. NPS .
C. CDT .
D. ICD-9-CM, Volume 3.
E. UPIN .

Answer: E

Question: 19

A health care clearinghouse is an entity that:

A. Requires P1<1 for the provider and the patient.
B. Is exempt from HIPAA regulations.
C. Is a not-for-profit operation.
D. Identifies all hospitals and health care organizations.
E. Performs the functions of format translation and data conversion.

Answer: E

Question: 20

Which one of the following implementation specifications is associated with the Facility Access Control standard?

A. Integrity Controls
B. Emergency Access Procedure
C. Access Control and Validation Procedures
D. Security Reminders
E. Security Policy

Answer: C

Question: 21

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

Question: 22

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

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

Answer: D

Question: 23

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

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

Answer: B

Question: 24

The Security Incident Procedures standard requires just one implementation specification. That implementation specification is:

A. Termination Procedures
B. Automatic Logoff
C. Emergency Access Procedure
D. Contingency Operations
E. Response and Reporting

Answer: E

Question: 25

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 can 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

Question: 26

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 (NI-UI)

Answer: B

Question: 27

Select the correct statement regarding code sets and identifiers.

A. A covered entity must use the applicable code set that is valid at the time the transaction is initiated.
B. April 14, 2003 is the compliance date for implementation of the National Provider Identifier.
C. CMS is responsible for updating the CPT-4 code setS
D. An organization that assigns NPIs is referred to as National Provider for Identifiers.
E. HHS assigns the Employer Identification Number (EIN), which has been selected as the National Provider Identifier for Health Care.

Answer: A

Question: 28

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

Question: 29

Select the FALSE statement regarding code sets and identifiers.

A. The CPT-4 code set is maintained by the American Medical Association (AMA).
B. A covered entity must use the applicable medical code set that is valid at the time the health care is delivered.
C. The National Provider Identifier (NPI) will be assigned by the National Provider System (NPS).
D. The Centers for Medicare and Medicaid Services is responsible for updating the HCPCS code set.
E. The National Provider Identifier (NPI) will be assigned to health plans.

Answer: E

Question: 30

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

Question: 31

This code set is used to describe or identity 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

Question: 32

HIPAA Security standards are designed to be:

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

Answer: E

Question: 33

This security rule standard requires policies and procedures for authorizing access to electronic protected health information that are consistent with its required implementation specifications-which are Isolating Health Care Clearinghouse Function, Access Authorization, and Access Establishment and Modification

A. Access Control
B. Security Incident Procedures
C. information Access Management
D. Workforce Security
E. Security Management Process

Answer: C

Question: 34

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

Question: 35

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

Question: 36

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

Question: 37

In an emergency treatment situation, a health care provider:

A. Must obtain the signature of the patient before disclosing PHI to another provider.
B. Must contact a relative of the patient before disclosing PHI to another provider.
C. May use their best judgment in order to provide appropriate treatment.
D. May use PHI but may not disclose it to another provider
E. Must inform the patient about the Notice of Privacy Practices before delivering treatment.

Answer: C

Question: 38

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

Question: 39

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

A. A covered entity must mitigate, to the extent practicable, any harmful effect that it becomes aware of from the use or disclosure of PHI in violation of its policies and procedures or HIPAA regulations.
B. A covered must not in any way intimidate, retaliate, or discriminate against any individual or other entity, which tiles a compliant.
C. A covered entity may not require individuals to waive their rights as a condition for treatments payment, enrollment in a health plan, or eligibility for benefits,
D. A covered entity must retain the documents required by the regulations for a period of six years
E. A covered entity must change its policies and procedures to comply with HIPAA regulations no later than three years after the change in law

Answer: E

Question: 40

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

Question: 41

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 l-IIPAA.
E. Yes - this is not considered a part of "treatment", which is one of the valid exceptions to the Privacy Rule.

Answer: A

Question: 42

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

Question: 43

Select the correct statement regarding the responsibilities of providers and payers under HIPAA’s privacy rule.

A. Optionally, they might develop a mechanism of accounting for all disclosures of PHI for purposes other than TPO.
B. They must redesign their offices, workspaces, and storage systems to afford maximum protection to PHI from intentional and unintentional use and disclosure.
C. They must develop methods for disclosing only the minimum amount of protected information necessary to accomplish any intended purpose.
D. They must obtain a “top secret” security clearance for all member of their workforce.
E. They must identify business associates that need to use PHI to accomplish their function and develop authorization forms to allow PHI to be shared with these business associates.

Answer: C

Question: 44

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

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

Answer: C

Question: 45

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

Question: 46

This code set describes drugs:

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

Answer: E

Question: 47

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

Question: 48

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

Question: 49

Which one of the following is a required implementation specification of the Security Management Process?

A. Risk Analysis
B. Access Control and Validation Procedures
C. Integrity Controls
D. Access Authorization
E. Termination Procedures

Answer: A

Question: 50

A business associate:

A. Requires PKI for the provider and the patient.
B. Is electronically stored information about an individual's lifetime health status and health care.
C. Is another name for an HMO.
D. Identifies all non-profit organizations.
E. Is a person or an entity that on behalf of the covered entity performs or assists in the performance of a function or activity involving the use or disclosure of health-related information.

Answer: E

Question: 51

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

Question: 52

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

A. A covered entity must apply disciplinary sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity.
B. A covered entity need not train all members of its workforce whose functions are materially affected by a change in policy or procedure
C. A covered entity must designate, and document, a contact person responsible for receiving acknowledgements of Notice of Privacy Practice.
D. A covered entity may require individuals to waive their rights.
E. A covered entity must provide maximum safeguards for PHI from any intentional or unintentional use or disclosure that is in violation of the regulations and to limit incidental uses and disclosures made pursuant to permitted or required use or disclosure.

Answer: A

Question: 53

Select the FALSE statement regarding the responsibilities of providers with direct treatment relationships under HIPAA's privacy rule.

A. Provide the individual with a Notice of Privacy Practices that describes the use of PHI.
B. Obtain a written authorization for each and every TPO event.
C. Obtain a written authorization for any disclosure or use of PHI other than for the purposes of TPO.
D. Provide access to the PHI that it maintains to the individual and make reasonable efforts to correct possible errors when requested by the individual.
E. Establish procedures to receive complaints relating to the handling of PHI.

Answer: B

Question: 54

A business associate must agree to:

A. Report to the covered entity any security incident of which it becomes aware
B. Ensure the complete safety of all electronic protected health information
C. Compensate the covered entity for penalties incurred because of the business associate's security incidents.
D. Register as a business associate with HHS
E. Submit to periodic audits by HHS of critical systems containing electronic protected health information

Answer: A

Question: 55

Which one of the following security standards is part of Technical Safeguards?

A. Access control
B. Security Management Process
C. Facility Access Controls
D. Workstation Use
E. Device and Media Controls

Answer: A

Question: 56

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 document1 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 it's creation or the time it was last in effect, which ever is later.

Answer: C

Question: 57

The best example of a party that would use the 835 - Health Care Claim Payment/Advice transaction is:

A. HHS
B. A community health management information system.
C. Health statistics collection agency.
D. Government agency.
E. Insurance Company.

Answer: E

Question: 58

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 decertify the information?

A. The protected health information must be removed from the information. A substitute "key" may be supplied to allow re-identification, if needed.
B. Limit the information to coverage, dates of treatment. and payment amounts to avoid collecting any protected data.
C. Nothing. An oversight agency has the right to access this information without prior authorization.
D. Request that the insurance commissioner ask for an exception from HIPAA from the Department of Health and Human Services.
E. B A written authorization is required from the patient.

Answer: C

Question: 59

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 M
E. Title V.

Answer: B

Question: 60

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 CDT 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. HIPAS 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

Question: 61

HIPAA transaction standards apply to:

A. Employee drug tests.
B. Health component of auto insurance.
C. Stored health information data.
D. Eligibility inquiries.
E. Non-reimbursed employee medical expenses.

Answer: D

Question: 62

Under the Privacy Rule, an individual may request a covered provider to restrict routine use or disclosure beyond what exists in the providers 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

Question: 63

Select the correct statement regarding the “Minimum Necessary” standard in the HIPAA regulations.

A. In some circumstances a covered entity is permitted, but not required, to rely on the judgment of the party requesting the disclosure as to the minimum amount of information necessary for the intended purpose. Some examples of these requesting parties are: another covered entity or a public official.
B. The privacy rule prohibits use, disclosure, or requests for an entire medical record,
C. Non-Covered entities need to redesign their facility to meet the requirement for minimum necessary uses.
D. The minimum necessary standard requires covered entities to prohibit maintenance of medical charts at bedside and to require that X-ray light boards be totally isolated.
E. If there is a request for more than the minimum necessary PHI, the privacy rule requires a covered entity to deny the disclosure of information after recording the event in the individual’s case file.

Answer: A

Question: 64

The version of the ANSI ASC Xl 2N standard required by HIPAA regulations is:

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

Answer: D

Question: 65

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

Question: 66

Which of the following was not established under the Administrative Simplification title?

A. National P1<1 Identifier.
B. National Standard Health Care Provider Identifier.
C. National Standard Employer Identifier.
D. Standards for Electronic Transactions and Code Sets.
E. Security Rule.

Answer: A

Question: 67

Physical safeguards using media controls do not include procedures to:

A. Control access to tapes, floppies, and re-writeable CDs.
B. Track the access of record able media.
C. Dispose of storage devices,
D. Backup copies of health information.
E. Prohibit alteration of health information.

Answer: E

Question: 68

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

Question: 69

This Security Standard addresses the proper functions to be performed on a specific workstation as well as the physical attributes of its surroundings,

A. information Access Management
B. Workstation Security
C. Access Control
D. Facility Access Controls
E. Workstation Use

Answer: E

Question: 70

In addition to code sets, HIPAA transactions also contain:

A. Security information such as a fingerprint.
B. Privacy information.
C. Information on all business associates,
D. Information on all health care clearinghouses.
E. Identifiers.

Answer: E

Question: 71

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 often years from the time of it's creation or the time it was last in effect, which ever is later

Answer: C

Question: 72

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

A. Is required for all Chain of Trust Agreements.
B. Must allow for the patient's written acknowledgement of receipt.
C. Must always be signed by the patient.
D. Must be signed in order for the patient's name to be sold to a mailing list organization.
E. Is not required if an authorization is being developed.

Answer: B

Question: 73

Security to protect information assets is generally defined as having:

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

Answer: A

Question: 74

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

Question: 75

Select the FALSE statement regarding the transaction rule.

A. The Secretary is required by statue to impose penalties of at least $100 per violation on any person or entity that fails to comply with a standard except that the total amount imposed on any one person in each calendar year may not exceed $1 .000.000 for violations of one requirement.
B. Health plans are required to accept all standard transactions.
C. Health plans may not require providers to make changes or additions to standard transactions.
D. Health plans may not refuse or delay payment of standard transactions.
E. If additional information is added to a standard transaction it must not modify the definition, condition, intent, or use of a data element.

Answer: A

Question: 76

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

Question: 77

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-1500 and 837.

Answer: D

Question: 78

A valid Notice of Privacy Practices must

A. Detail specifically all activities that are considered a use or disclosure
B. Describe in plain language what is meant by treatment, payment, and health care operations (TPO).
C. Inform the individual that protected health information (PHI) may only be used for valid medical research.
D. Inform the individual that this version of the Notice will always cover them, regardless of subsequent changes.
E. State the expiration date of the Notice.

Answer: B

Question: 79

The office manager of a small doctors office wants to donate several of their older workstations to the local elementary school. Which Security Rule Standard addresses this situation?

A. Security Management Process
B. Device and Media Controls
C. information Access Management
D. Facility Access Controls
E. Workstation Security

Answer: B

Question: 80

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

A. Eligibility (2701271)
B. Premium Payment 2O)
C. Unsolicited Claim Status (277)
D. Remittance Advice 35)
E. Functional Acknowledgment (997)

Answer: D

Question: 81

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

Question: 82

A covered entity' that fails to implement the HIPAA Privacy Rule would risk:

A. $50O0 in fines.
B. $5000 in fines and six months in prison.
C. An annual cap of $5000 in fines.
D. A fine of up to $50000 if they wrongfully disclose PHI.
E. Six months in prison.

Answer: D

Question: 83

This transaction supports multiple functions. These functions include: telling a bank to move money OR telling a bank to move money while sending remittance information

A. 277.
B. 276
C. 271
D. 820.
E. 270.

Answer: D

Question: 84

When PHI is sent or received over an electronic network there must be measures to guard against unauthorized access. This is covered under which security rule standard?

A. Device and Media Controls
B. Access Controls
C. Transmission Security
D. Integrity
E. Audit Controls

Answer: C

Question: 85

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

A. P1<1 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

Question: 86

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

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

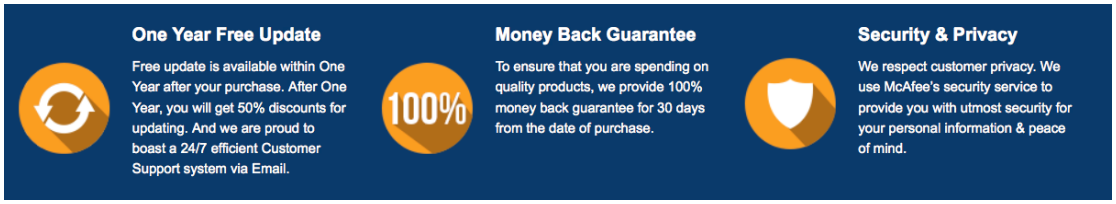
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions