DUMPSBOSS.

Certified HIPAA Professional

HIPAA HIO-201

Version Demo

Total Demo Questions: 24

Total Premium Questions: 248

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Use or disclosure of Protected Health Information (PHI) for Treatment, Payment, and Health care Operations (TPO) is:

A. Limited 1o the minimum necessary to accomplish the intended purpose.

B. Left to the professional judgment and discretion of the requestor.

C. Controlled totally by the requestor's pre-existing authorization document.

D. Governed by industry "best practices" regarding use

E. Left in force for eighteen (18) years.

F. Permitted without an individual's authorization for treatment, payment, and health care operations; however, the minimum necessary standard does not apply to treatment.

ANSWER: F

Explanation:

"Permitted without an individual's authorization for treatment, payment, and health care operations; however, the minimum necessary standard does not apply to treatment" is correct. The HIPAA Privacy Rule permits a covered entity to use or disclose protected health information for its own treatment, payment, and health care operations without obtaining a HIPAA authorization from the individual. It also permits certain disclosures between covered entities for these purposes, subject to the applicable regulatory conditions. This permission supports routine clinical care, billing and reimbursement activities, quality assessment, case management, audits, training, and other defined operational functions without creating an unnecessary authorization process for every routine activity.

The minimum necessary rule remains important, but its application is purpose-specific. Covered entities must make reasonable efforts to limit uses, disclosures, and requests to the minimum PHI needed for payment and health care operations. Crucially, the Privacy Rule expressly exempts uses or disclosures for treatment from the minimum necessary requirement, so a statement applying that requirement uniformly to all three TPO purposes would be inaccurate. The governing provisions are found in 45 CFR § 164.506, covering permitted TPO uses and disclosures, and 45 CFR § 164.502(b), addressing the minimum necessary standard and its treatment exception. See 45 CFR § 164.506 and 45 CFR § 164.502.

QUESTION NO: 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

Explanation:

The correct answer is **835**. Under the HIPAA Administrative Simplification transaction standards, the Health Care Claim Payment/Advice transaction is implemented using the ASC X12N 835 transaction. A health plan, insurer, or other payer sends this electronic transaction to a health care provider or its billing representative to communicate how a submitted claim was adjudicated. It conveys payment information together with remittance advice details, such as the claim and service-line amounts allowed and paid, patient responsibility, adjustments, and the relevant reason and remark codes. This standardized electronic remittance advice supports consistent exchange of payment and adjudication data between covered entities and their business partners, helping providers reconcile electronic funds transfers and post payments accurately in their practice-management or revenue-cycle systems. The HIPAA transaction regulation specifically identifies the health care claim

payment/advice standard as ASC X12N 835. CMS also describes the 835 as the electronic remittance advice transaction used to explain claim-payment decisions. See 45 C.F.R. § 162.1601 and CMS's Health Care Payment and Remittance Advice resource.

QUESTION NO: 3

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

A. $5,000 in fines.

B. 55000 in fines and six months in prison.

C. An annual cap of $50,000 in fines.

D. A fine of up to $50,000 if they wrongfully disclose PHI.

E. Six months in prison.

F. Civil monetary penalties, with amounts depending on the level of culpability and adjusted annually.

ANSWER: F

Explanation:

"Civil monetary penalties, with amounts depending on the level of culpability and adjusted annually" is correct because a covered entity's failure to comply with the HIPAA Privacy Rule is subject to the HIPAA Enforcement Rule's civil penalty framework. The Department of Health and Human Services' Office for Civil Rights investigates complaints and compliance concerns and may impose civil monetary penalties when it finds violations. The applicable penalty amount is not a single fixed fine: it depends on the organization's level of knowledge and culpability, including whether it did not know of the violation, had reasonable cause, or engaged in willful neglect. Penalty limits are also adjusted for inflation, so training materials should not present an outdated fixed dollar amount as the universal consequence of a Privacy Rule failure. In addition to monetary penalties, corrective action and resolution agreements may require changes to policies, procedures, workforce training, and compliance monitoring. The governing civil-penalty standards appear in 45 C.F.R. Part 160, Subpart D. Current penalty adjustment information is published by HHS Office for Civil Rights.

QUESTION NO: 4

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

A. National Patient 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

Explanation:

National Patient Identifier is correct because no national, standard patient identifier was established or implemented as part of HIPAA Administrative Simplification. HIPAA's Administrative Simplification provisions directed the Department of Health and Human Services to adopt standards that improve the efficiency and security of health-information administration, including standards for electronic transactions, code sets, privacy, security, and certain identifiers. Although the original HIPAA statute included language concerning an individual unique health identifier, Congress has repeatedly prohibited the use of federal funds to develop or implement a national patient identifier. As a result, HHS has not adopted a National Patient Identifier standard comparable to the National Provider Identifier. This distinction is important in HIPAA compliance: organizations may use internal patient identifiers and other permitted matching methods, but there is no federally established

universal patient ID under the Administrative Simplification program. CMS describes Administrative Simplification standards and identifiers at CMS Administrative Simplification. The statutory restriction on development of a unique health identifier is reflected in annual appropriations legislation and summarized in the Congressional Research Service report on health-information privacy.

QUESTION NO: 5

The standard electronic transaction used to submit a health care claim or encounter information is:

A. 271

B. 276

C. 277

D. 835

E. 837

ANSWER: E

Explanation:

The correct answer is **837**. The ASC X12N 837 Health Care Claim transaction is used to submit health care claims or encounter information electronically. Versions of the transaction support professional, institutional, and dental claims.

The 837 communicates information needed for claim processing, such as patient and subscriber data, provider information, diagnoses, procedures, services, charges, and coordination-of-benefits data. It is distinct from the 835 payment/advice transaction and the 277 claim status response transaction. HIPAA adopts the 837 as the standard for health care claims or equivalent encounter information at 45 C.F.R. § 162.1102. CMS describes the applicable HIPAA transaction standards.

QUESTION NO: 6

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 make reasonable efforts to limit uses, disclosures, and requests for PHI to the minimum necessary to accomplish the 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

Explanation:

They must make reasonable efforts to limit uses, disclosures, and requests for PHI to the minimum necessary to accomplish the intended purpose. This expresses HIPAA’s “minimum necessary” standard, a core Privacy Rule responsibility for covered entities, including health care providers and health plans. In routine operations, a covered entity must establish policies and procedures that reasonably limit workforce access to protected health information (PHI), internal uses, disclosures, and requests for PHI to what is needed for the specific purpose. The standard is operational rather than merely aspirational: organizations should use role-based access, defined disclosure procedures, and criteria for recurring requests so personnel receive only the information necessary to perform their duties. For nonroutine disclosures or requests, the entity must make an individualized reasonable assessment of what information is necessary. HIPAA recognizes specified circumstances in which the minimum-necessary requirement does not apply, such as disclosures to or requests by a health

care provider for treatment and disclosures made pursuant to an individual's authorization. These exceptions do not remove the general obligation to implement and apply minimum-necessary safeguards in the many routine uses and disclosures where the standard governs. The regulatory requirement appears at 45 C.F.R. § 164.502(b), with practical guidance from HHS's Minimum Necessary Requirement guidance.

QUESTION NO: 7

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

F. Yes - the data-entry company is a business associate, and the facts do not establish the required written business associate agreement.

ANSWER: F

Explanation:

Yes — because the data-entry company is a business associate and the facts do not establish the required written business associate agreement or other permitted written arrangement. A company performing data-entry services on patient records creates, receives, maintains, or transmits PHI on the doctor's behalf in performing a function for the covered entity. Before disclosing PHI to that company, the doctor must obtain satisfactory assurances, documented through a HIPAA-compliant written contract or arrangement, that the company will appropriately safeguard the information and use or disclose it only as permitted. Security measures, delivery safeguards, internal procedures, training, and designation of a Privacy Officer are important compliance practices, but they do not replace this written business associate requirement. Individual patient authorizations are generally not required for a properly structured disclosure to a business associate for a covered function; however, the absence of patient authorizations does not eliminate the separate obligation to have the required business associate agreement in place. HHS describes the business associate relationship and the requirement for satisfactory assurances at HHS Business Associates guidance. The governing Privacy Rule provisions are available at 45 CFR §164.502(e).

QUESTION NO: 8

A covered entity may use or disclose protected health information without an individual's authorization for its own health care operations. Which of the following is an example of health care operations?

A. Quality assessment and improvement activities

B. Prescribing medication to an individual

C. Submitting a claim for reimbursement

D. Disclosing PHI to an employer for employment decisions

E. Selling PHI to a marketing company

ANSWER: A

Explanation:

Quality assessment and improvement activities is correct. Health care operations are administrative, financial, legal, and quality-improvement activities necessary to run a covered entity's business and support its treatment and payment functions. Examples include quality assessment, case management, competency assurance, accreditation, auditing, compliance, planning, and business management.

Uses and disclosures for a covered entity's own health care operations are generally permitted without individual authorization, subject to applicable Privacy Rule requirements, including the minimum necessary standard where it applies. Health care operations should not be confused with treatment, which concerns the provision, coordination, or management of health care, or payment, which includes billing and claims administration. See the definition at 45 C.F.R. § 160.103 and HHS guidance on uses and disclosures for treatment, payment, and health care operations.

QUESTION NO: 9

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

Explanation:

It can be used in either update or full replacement mode. The ASC X12N 834 Benefit Enrollment and Maintenance transaction is the HIPAA-adopted electronic transaction used to communicate enrollment information for members and their dependents between a sponsor and a health plan or other benefits administrator. It supports maintenance of enrollment records through additions, changes, reinstatements, terminations, and cancellations. An 834 transaction may be sent as a full-file replacement, supplying the complete current enrollment population, or as a change-only file containing incremental updates since the prior transmission. This flexibility allows organizations to align the exchange with their enrollment-administration process and the receiving organization’s operational requirements. In HIPAA’s administrative-transaction standards, the 834 is therefore an important mechanism for transmitting benefit enrollment and maintenance data electronically, rather than merely a notice of a health plan’s internal coverage action. CMS identifies the Benefit Enrollment and Maintenance transaction as the 834 standard under HIPAA’s adopted electronic transaction standards. Additional implementation context is available through the CMS HIPAA Administrative Simplification overview and the X12 834 Benefit Enrollment and Maintenance transaction page.

QUESTION NO: 10

Maintenance personnel that normally have no access to PHI are called in to investigate water that is leaking from the ceiling of the room where a large amount of PHI is stored. The room is normally secured but the file cabinets have no doors or locks. Situations like this are addressed by which Workforce Security implementation specification?

A. Risk Management

B. Written Contract or Other Arrangement

C. Accountability

D. Authorization and/or Supervision

E. integrity Controls

ANSWER: D

Explanation:

Authorization and/or Supervision is correct because the HIPAA Security Rule's Workforce Security standard requires a covered entity or business associate to implement policies and procedures ensuring that workforce members have appropriate access to electronic protected health information (ePHI) and preventing those without such access from obtaining it. The associated addressable implementation specification requires procedures for authorizing and/or supervising workforce members who work with ePHI or in locations where ePHI may be accessed.

Here, maintenance personnel ordinarily do not need access to PHI, but the emergency repair places them in a room containing accessible records. The organization should use reasonable safeguards to authorize the necessary presence and supervise the personnel while they perform the repair, such as escorting them, limiting their access to the affected area, and securing or covering records when feasible. The fact that the incident is unplanned does not remove the need to control access; it illustrates why procedures must address temporary or exceptional access situations. Although the scenario describes paper records, the Workforce Security requirement specifically concerns ePHI; the same supervised-access approach is also a sound administrative safeguard for protecting all PHI. See 45 CFR § 164.308 and HHS Security Rule guidance.

QUESTION NO: 11

Under the HIPAA Breach Notification Rule, a covered entity must notify affected individuals of a breach of unsecured protected health information without unreasonable delay and in no case later than:

A. 10 calendar days after discovery

B. 30 calendar days after discovery

C. 45 calendar days after discovery

D. 60 calendar days after discovery

E. 90 calendar days after discovery

ANSWER: D

Explanation:

60 calendar days after discovery is correct. Following discovery of a breach of unsecured protected health information, a covered entity must provide notice to each affected individual without unreasonable delay and no later than 60 calendar days after discovery. A breach is generally an impermissible use or disclosure of PHI that is presumed to be a breach unless the covered entity or business associate demonstrates a low probability that the PHI has been compromised based on the required risk assessment.

Additional notification obligations can apply, including notice to HHS and, for certain large breaches, notice to prominent media outlets. The individual-notice requirement is found at 45 C.F.R. § 164.404. HHS breach notification resources are available at HHS Breach Notification Rule.

QUESTION NO: 12

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

A. National PKI 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

Explanation:

National PKI Identifier. is correct because HIPAA's Administrative Simplification provisions did not create a national identifier based on public key infrastructure. Public key infrastructure is a security technology framework used to manage digital certificates and cryptographic keys; it is not one of the statutory administrative-simplification identifiers or standards. Administrative Simplification directed the adoption of national standards that improve the efficiency and consistency of health-care administration, including standards for electronic health-care transactions and code sets, unique identifiers, privacy, and security. The Department of Health and Human Services describes these provisions as establishing standards for electronic transactions, code sets, unique health identifiers, and security. The provider identifier adopted under this authority is the National Provider Identifier, while the employer identifier is the Employer Identification Number. Thus, although cryptography and digital certificates may be relevant to an organization's security practices, a "National PKI Identifier" was not established by the Administrative Simplification title. See HHS's HIPAA regulatory overview and CMS's Administrative Simplification overview.

QUESTION NO: 13

Before using or disclosing protected health information for a purpose that requires an authorization, the authorization must include:

A. A description of the information to be used or disclosed

B. The patient's Social Security number

C. A notarized signature from the individual

D. The signature of the covered entity's privacy officer

E. A statement that the individual waives all Privacy Rule rights

ANSWER: A

Explanation:

A description of the information to be used or disclosed is correct. A valid HIPAA authorization must contain core elements, including a description of the information to be used or disclosed; the name or other specific identification of the person or class of persons authorized to make the use or disclosure; the name or other specific identification of the recipient; a description of the purpose; an expiration date or event; and the individual's signature and date.

The authorization also must contain required statements concerning the individual's right to revoke the authorization, the potential for redisclosure by a recipient, and whether treatment, payment, enrollment, or benefits eligibility may be conditioned on signing the authorization. These requirements are set out at 45 C.F.R. § 164.508.

QUESTION NO: 14

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 set.

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

Explanation:

A covered entity must use the applicable code set that is valid at the time the transaction is initiated. HIPAA's transaction and code set regulation requires covered entities to use the applicable medical data code set specified in the standards when conducting a covered electronic transaction. Crucially, the regulation defines a "valid code set" as the version of the applicable standard code set that is valid at the time the transaction is initiated. This timing requirement promotes consistent interpretation of diagnoses, procedures, drugs, providers, and other transaction data among health plans, providers, clearinghouses, and their business partners. It also means organizations need effective change-management processes to implement required annual or periodic code-set updates and to ensure their transaction systems apply the current valid version on the date a transaction begins. The governing provision is 45 C.F.R. § 162.925(c)(2), available through the Electronic Code of Federal Regulations. HHS also summarizes the HIPAA administrative simplification standards, including standards for transactions and code sets, on its Administrative Simplification page.

QUESTION NO: 15

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

Explanation:

CDT is correct because the HIPAA Administrative Simplification standards require covered entities that conduct standard electronic transactions to use the applicable adopted medical code sets. For dental services, the applicable procedure code set is the Code on Dental Procedures and Nomenclature, commonly called Current Dental Terminology (CDT), which is maintained by the American Dental Association. A practicing dentist submitting or processing electronic dental claims needs to represent the dental procedures performed using CDT codes so that the clinical service information is consistently understood by health plans and other transaction participants.

Dr. Jones's small staff size and revenue level do not remove the need to use the required standard code set when he elects to conduct a covered transaction electronically. HIPAA's transaction and code-set rules focus on the type of transaction and the entity's role, rather than providing a general small-practice exception from the code-set standard. The Department of Health and Human Services identifies CDT as the standard medical data code set for dental procedures, and CMS explains that HIPAA-covered entities must use the adopted standards when conducting covered electronic transactions. See HHS Transaction and Code Set Standards and CMS Transactions and Code Sets.

QUESTION NO: 16

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

Explanation:

Testing and Revision Procedures is correct because it is the implementation specification within the HIPAA Security Rule's contingency plan standard that specifically requires covered entities and business associates to establish procedures for periodically testing and revising contingency plans. Contingency planning supports the availability of electronic protected health information (ePHI) during emergencies or other events that damage systems containing ePHI. Testing helps an organization confirm that its recovery and continuity processes will operate as intended, while revision ensures those procedures remain appropriate as technology, operational risks, systems, personnel, and business processes change.

The requirement appears at 45 C.F.R. § 164.308(a)(7)(ii)(D), which identifies "Testing and revision procedures" as an addressable implementation specification. "Addressable" does not mean optional: the organization must assess whether the specification is reasonable and appropriate in its environment and, if it is not, document the rationale and implement an equivalent alternative measure where reasonable and appropriate. HHS guidance also identifies testing and revision procedures as a core element of an effective contingency-planning process for maintaining access to ePHI. See 45 C.F.R. § 164.308 and HHS HIPAA Security Rule guidance.

QUESTION NO: 17

The transaction number assigned to the Health Care Claim Status Request transaction is:

A. 270

B. 271

C. 276

D. 277

E. 278

ANSWER: C

Explanation:

276 is correct. The ASC X12N 276 transaction is the Health Care Claim Status Request. A provider, clearinghouse, or other authorized entity uses it to inquire about the status of a health care claim that has been submitted for processing. The corresponding Health Care Claim Status Response is the 277 transaction.

The 276/277 transaction pair supports standardized communication about claim processing status and reduces reliance on payer-specific inquiry methods. CMS identifies these transactions among HIPAA's adopted standards at CMS HIPAA adopted standards and operating rules. X12 information is available at X12 276/277 transactions.

QUESTION NO: 18

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

Explanation:

“Obtain a written authorization for each and every TPO event.” is the false statement. The HIPAA Privacy Rule permits a covered entity to use or disclose protected health information for treatment, payment, and health care operations without obtaining the individual’s written authorization. Treatment includes activities such as consultations between health care providers and referrals; payment includes billing and claims-management activities; and health care operations include activities such as quality assessment, auditing, and compliance functions. These routine functions would be impractical if separate authorizations were required for every use or disclosure.

A provider that has a direct treatment relationship with an individual has distinct notice obligations. It must provide its Notice of Privacy Practices no later than the date of first service delivery and make a good-faith effort to obtain the individual’s written acknowledgment of receipt, except in emergency treatment situations. The notice explains, among other things, the provider’s uses and disclosures of protected health information for treatment, payment, and health care operations, as well as individual rights. Written authorization is generally required only when the Privacy Rule does not otherwise permit or require the particular use or disclosure. See 45 C.F.R. § 164.506 and 45 C.F.R. § 164.520.

QUESTION NO: 19

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

Explanation:

Unique User Identification is the required implementation specification that directly requires a covered entity or business associate to assign a unique name and/or number for identifying and tracking each user. It appears within the HIPAA Security Rule’s Access Control standard, at 45 C.F.R. § 164.312(a)(2)(i). A unique identifier links system activity to a specific individual, which supports accountability when electronic protected health information is accessed, created, modified, or transmitted. In practice, this means users should have individual accounts rather than sharing a generic login. The identifier may be a username, employee identifier, or another distinct account value, provided it reliably distinguishes the user and permits audit activity to be associated with that user. This requirement is designated “required,” meaning regulated entities must implement it; unlike addressable specifications, it cannot simply be omitted based on an internal assessment. Unique identification is also foundational to effective access management because permissions can be assigned, changed, and terminated for a particular person throughout that person’s relationship with the organization. The regulatory text is available at 45 C.F.R. § 164.312, and HHS provides implementation guidance in its HIPAA Security Rule guidance.

QUESTION NO: 20

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

Explanation:

“Must allow for the patient's written acknowledgement of receipt.” is correct because the HIPAA Privacy Rule requires a covered health care provider with a direct treatment relationship to make a good-faith effort to obtain each patient’s written acknowledgment that the patient received the Notice of Privacy Practices (NPP). The acknowledgment process gives the patient an opportunity to confirm receipt of the notice describing how the provider may use and disclose protected health information, the patient’s privacy rights, and how to file a complaint. The NPP itself need not be signed as an authorization or consent document; rather, the provider must use a process that permits written acknowledgment of receipt and must document its good-faith effort if it cannot obtain one. For example, a patient may decline to sign, or an emergency may make acknowledgment impracticable initially. In those circumstances, the provider documents the circumstances and retains that documentation. This requirement applies to direct-treatment providers, subject to the specific exceptions in the regulation. The governing requirement appears at 45 C.F.R. § 164.520. HHS also explains NPP requirements and patients’ receipt of the notice in its Notice of Privacy Practices guidance.

QUESTION NO: 21

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 Recovery Plan

ANSWER: E

Explanation:

Disaster Recovery Plan is correct because the HIPAA Security Rule requires covered entities and business associates to establish procedures for restoring lost electronic protected health information after a disaster or other damaging event. This is an implementation specification within the contingency plan standard at 45 C.F.R. § 164.308(a)(7). A disaster recovery plan addresses the practical recovery of systems, applications, and ePHI when events such as fire, vandalism, natural disasters, or system failures disrupt normal operations. Its purpose is to return affected information systems and data to an operational state while preserving the availability and integrity of ePHI. Effective disaster-recovery procedures commonly identify recovery priorities, responsible personnel, restoration methods, alternate processing capabilities, and testing practices. The plan should be coordinated with the organization’s broader contingency planning process so recovery activities can be executed reliably during an actual incident. The regulatory requirement is stated in the HIPAA Security Rule as procedures to restore any loss of data, which directly matches the scenario described. See the governing regulation at 45 C.F.R. § 164.308 and HHS guidance on the HIPAA Security Rule.

QUESTION NO: 22

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

Explanation:

Title II is correct because it contains HIPAA's Administrative Simplification provisions, the part of the statute that drove nationwide standards for electronic health care transactions, protection of health information, and safeguards for that information. Congress directed the Secretary of Health and Human Services to adopt standards for electronic transactions and code sets, unique identifiers, privacy, and security of individually identifiable health information. These requirements led to the HIPAA Transactions and Code Sets Rules, Privacy Rule, Security Rule, and related enforcement and breach-notification frameworks. In practical terms, Title II is the statutory foundation for organizational compliance initiatives involving the standardized exchange of health care data, policies governing uses and disclosures of protected health information, workforce training, risk analysis, and administrative, physical, and technical security safeguards. HHS's HIPAA overview identifies Administrative Simplification as the source of these national standards, while the statutory text places these provisions in Title II, Subtitle F. See the HHS HIPAA for Professionals overview and the HIPAA statute (Public Law 104-191).

QUESTION NO: 23

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 a 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

Explanation:

"Do nothing more." is correct because the pharmacist will not create or maintain a record of the individual as part of this brief over-the-counter medication consultation. Although the individual may voluntarily share health information so that the pharmacist can provide an appropriate answer, the Privacy Rule's Notice of Privacy Practices requirement contains a specific exception for a covered health care provider with a direct treatment relationship when the provider maintains no records of the individual. In that circumstance, the provider is not required to provide a Notice of Privacy Practices or obtain the individual's written acknowledgment of receipt of that notice. The interaction may proceed as an ordinary, limited verbal consultation without requesting a HIPAA authorization or consent solely for the individual to disclose information to the pharmacist. The pharmacist should still use professional judgment and respect the individual's privacy, such as avoiding unnecessary discussion where others can overhear it. This result follows the regulatory exception in 45 CFR 164.520(a)(3), which addresses providers that maintain no records of an individual. See the Notice of Privacy Practices regulation, 45 CFR 164.520 and HHS's Privacy Rule guidance.

QUESTION NO: 24

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

Explanation:

Facility Access Controls is correct. The HIPAA Security Rule's physical safeguards require covered entities and business associates to implement policies and procedures that limit physical access to their electronic information systems and the facilities where those systems are located, while ensuring that properly authorized access is allowed. This requirement is expressly stated at 45 C.F.R. § 164.310(a)(1), the Facility Access Controls standard. It applies to locations and equipment that house systems containing electronic protected health information (ePHI), such as offices, data centers, server rooms, network closets, and work areas with electronic devices.

Implementation may include practices such as badge or key access procedures, visitor sign-in and escort processes, security monitoring, access logs, contingency procedures for facility access during emergencies, and maintenance records for physical-security components. The exact safeguards adopted should be reasonable and appropriate to the organization's size, operations, environment, and risk analysis. Facility Access Controls help protect the confidentiality, integrity, and availability of ePHI by reducing the risk of unauthorized physical entry, theft, loss, tampering, or damage to systems that create, receive, maintain, or transmit ePHI. The regulatory text is available at 45 C.F.R. § 164.310; OCR's Security Rule guidance is available from HHS OCR.