Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

AHIMA-CHPS Dumps
AHIMA-CHPS Braindumps
AHIMA-CHPS Real Questions
AHIMA-CHPS Practice Test
AHIMA-CHPS Actual Questions

PASS

killexams.com

AHIMA

AHIMA-CHPS

Certified in Healthcare Privacy and Security

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/AHIMA-CHPS

Question: 1117

A policy requires regular review of user privileges and immediate removal of access for terminated employees. What compliance aspect does this safeguard primarily support?

A. Integrity of systems
B. Availability of data
C. Confidentiality and security of ePHI
D. Encryption key management

Answer: C

Explanation: Regular review and prompt revocation of access for terminated employees prevent unauthorized ePHI access, supporting confidentiality and overall security.

Question: 1118

A state law mandates breach reporting within 10 days, while HIPAA requires notification within 60 days. During a compliance review, which policy is best to ensure regulatory adherence?

A. Follow the 10-day state breach reporting requirement
B. Adhere only to the HIPAA 60-day requirement due to federal preemption
C. Combine the timelines and notify within 35 days, the average of both
D. Notify breaches only when requested by regulators

Answer: A

Explanation: The organization must comply with the more stringent 10-day state notification requirement as it does not conflict with HIPAA but enhances timely breach reporting. HIPAA sets minimum standards and states can require faster notification timelines.

Question: 1119

Following a 2024 phishing simulation exposing 40% click rates among staff, a cardiology practice in 2026 updates its training per OCR's October newsletter, but the risk assessment reveals persistent weak passwords on shared physical kiosks in exam rooms. What technical safeguard enforces credential hygiene at endpoints?

A. Monitor password spray attempts with account lockouts after three failed tries across devices.
B. Integrate adaptive authentication escalating to MFA based on login location and time patterns.
C. Rotate default kiosk passwords monthly via centralized management with complexity enforcement.
D. Deploy passwordless authentication using FIDO2 security keys for kiosk logins with biometric fallbacks.

Answer: D

Explanation: Deploying passwordless authentication using FIDO2 security keys for kiosk logins with biometric fallbacks eliminates weak password vulnerabilities, aligning with HIPAA §164.312(d) authentication and NPRM's MFA emphasis for phishing-prone environments. High click rates indicate human factors risks, as in 2024's five ransomware settlements. FIDO2 provides phishing-resistant hardware tokens, biometrics add physical layer, outperforming rotations' burden. For cardiology kiosks, this streamlines workflows, supports physical hygiene, and drives compliance via key audits, reducing initiative penalties.

Question: 1120

A hospital security team recently discovered several unauthorized attempts to access patient health records via terminal stations located in the waiting area. What is the best initial step to respond and reduce future risk of physical access to sensitive information in such areas?

A. Reconfigure terminals to automatically log off after short idle times and restrict guest access
B. Increase physical patrols and surveillance cameras in waiting and common areas
C. Apply biometric authentication exclusively at all terminal stations in the hospital
D. Relocate all terminal stations away from public waiting areas into secured rooms

Answer: A

Explanation: Reconfiguring terminals for automatic logoff after short idle periods and restricting guest access directly addresses unauthorized physical access via unattended terminals in public spaces, which is a common physical safeguard. Increasing surveillance is useful but less direct. Moving terminals may disrupt workflow, and biometric authentication only at terminals may not be feasible or enough without administrative controls like automatic logoff.

Question: 1121

A hospital network experiences multiple incidents of Denial of Service (DoS) attacks targeting its EHR system. Which technical safeguard is best suited to mitigate this threat?

A. Increase bandwidth capacity to absorb attack traffic without filtering
B. Disable all remote access to reduce attack surface
C. Implement intrusion prevention systems (IPS) with real-time traffic analysis and blocking rules
D. Schedule system maintenance during expected attack windows to minimize impact

Answer: C

Explanation: IPS devices detect and block malicious network traffic, effectively mitigating DoS attacks by stopping harmful packets before they impact the system. Disabling remote access may reduce functionality unnecessarily. Increasing bandwidth does not address the root attack and scheduling maintenance does not prevent attacks.

Question: 1122

A academic medical center collaborating on a multi-institutional AI-driven research project in 2026 must define its DRS to respond to participant requests for PHI access, including AI-analyzed imaging data from mental health studies. The project involves BAs handling ePHI with potential special protections for mental health and substance use data under aligned Part 2 rules. Recent OCR guidance stresses minimum necessary disclosures for research preparatory activities. During a mock audit, inconsistencies arise in classifying AI outputs as DRS components, risking impermissible uses. What is the optimal strategy for the privacy officer to manage DRS definition, incorporating physical safeguards and regulatory compliance?

A. Classify AI outputs outside the DRS, limit BA access to de-identified data, and secure physical storage with locked facilities for original records.
B. Define DRS to include only raw data, permit full AI disclosures to BAs without limits, and rely on video surveillance for physical security.
C. Exclude mental health data from DRS for research, update BA contracts for Part 2 consents, and use standard keycard systems for physical safeguards.
D. Include AI outputs in the DRS if used for decisions, require data use agreements with minimum necessary clauses, and implement biometric access for physical research labs.

Answer: D

Explanation: Designated record sets (DRS) encompass records used to make decisions about individuals, including research records if they influence care (§164.501), and AI outputs qualify if integrated into treatment planning. The 2024 42 CFR Part 2 alignment permits HIPAA-like disclosures for substance/mental health data with consents, but preparatory research requires minimum necessary under §164.502(b). Special protections apply, necessitating identification in program policies. Physical safeguards under Security Rule §164.310 include facility access controls like biometrics for high-risk areas. This strategy ensures DRS accuracy for access requests (§164.524), compliant BA management (§164.314), and regulatory adherence, mitigating enforcement risks amid OCR's 2026 focus on AI-related breaches.

Question: 1123

A physician’s practice suspects a breach due to a lost unencrypted laptop containing patient data. Which of the following steps must be taken in the initial response?

A. Confirm if the data on the laptop is accessible and encrypted before proceeding
B. Immediately notify the media to proactively manage public perception
C. Inform all patients regardless of the breach risk assessment outcome
D. Ignore the incident if the laptop is suspected to be lost temporarily

Answer: A

Explanation: The key initial step is to determine whether the data on the laptop is accessible and if it was encrypted because encryption can mitigate the requirement to notify individuals if data is rendered unusable. Notification decisions depend on this assessment. Media notification or notifying all patients

without assessment violates best practices.

Question: 1124

An IT auditor finds that emergency access credentials are shared among multiple trusted users without individual identification. What is the primary security issue and recommended corrective action?

A. Lack of accountability; assign unique credentials with individual audit trails
B. Simplified emergency response; continue current practice
C. Cost saving; shared credentials reduce management overhead
D. No issue as long as emergency access is restricted physically

Answer: A

Explanation:
Sharing credentials obscures individual actions and accountability, violating HIPAA requirements for access controls and auditability. Unique credentials with individual logging ensure traceability and secure emergency access management. Convenience or cost saving should not override security.

Question: 1125

Following a 2026 phishing incident at a Florida telehealth provider, the privacy officer uncovers that the incident stemmed from inadequate workforce training on recognizing social engineering attacks, violating both HIPAA administrative safeguards and Florida's strict data privacy laws on breach prevention. What is the officer's primary duty in guiding the organization's response?

A. Solely report the incident to HHS without internal remediation
B. Develop and deliver comprehensive training programs interpreting HIPAA's workforce security requirements alongside Florida's more protective standards to prevent recurrence
C. Rely on external consultants for all training updates
D. Limit response to affected patients only

Answer: B

Explanation: As a resource for regulatory interpretation, the privacy officer must design targeted training under HIPAA's Security Rule (45 CFR § 164.308(a)(5)) to address phishing threats, incorporating Florida's Information Protection Act mandates for proactive breach prevention training that exceed HIPAA's baselines. This includes simulations, policy reinforcement, and preemption analysis to ensure state laws' stricter employee accountability measures are applied, thereby enhancing organizational resilience and ethical stewardship of PHI in a high-risk telehealth environment.

Question: 1126

Which compliance enforcement mechanism requires prompt investigation and effective mitigation actions when monitoring reveals potential unauthorized PHI access?

A. HIPAA Security Rule audit controls provision
B. OSHA workplace safety inspections
C. FDA post-market surveillance regulations
D. CMS mandatory reporting for fraud only

Answer: A

Explanation: The Security Rule mandates audit controls to detect, investigate, and mitigate unauthorized access to PHI. OSHA and FDA regulations address different domains. CMS fraud reporting is related but not specific to technical access monitoring.

Question: 1127

A covered entity plans to release PHI for marketing purposes. What documentation is required to ensure compliance?

A. Only a patient notification, no written authorization necessary
B. An internal memo approving the marketing strategy
C. Documentation of verbal consent from the individual
D. A valid written authorization from the individual specifying the marketing disclosure

Answer: D

Explanation: HIPAA strictly requires valid, written authorization specifying the marketing purpose before PHI can be disclosed for marketing. Internal memos and verbal consents are insufficient.

Question: 1128

During an IT security assessment, it is found that no encryption is applied to laptops used by field nurses containing PHI. What technical safeguard would be most appropriate?

A. Use of complex passwords only without additional controls
B. Software firewalls installed without encryption
C. Full disk encryption on all portable devices to protect ePHI at rest
D. Encouraging nurses to carry devices only during work hours

Answer: C

Explanation: Full disk encryption protects data if the device is lost or stolen, a critical requirement for portable devices with PHI. Firewalls and passwords alone do not protect data at rest. Behavioral controls like timing do not guarantee security.

Question: 1129

Which of the following roles within an organization is most responsible for ensuring policies and procedures for breach notification comply with federal and state laws?

A. Chief Information Officer (CIO)
B. Privacy Officer or Compliance Officer
C. Director of Nursing
D. Chief Financial Officer (CFO)

Answer: B

Explanation: The Privacy Officer or Compliance Officer is primarily responsible for ensuring that policies, including breach notification, comply with applicable laws and regulations. Although CIO and other leadership may support the process, compliance roles oversee regulatory adherence. Directors of nursing and CFOs have operational and financial roles, respectively, but not primary compliance responsibilities.

Question: 1130

In 2026 research collab, DRS excludes trial data with infectious PHI. BA shares fundraising. IRB flags. What?

A. Exclude, permit share, ignore IRB.
B. Include with flags, auth share, address IRB.
C. Non-exclude, no auth.
D. Partial, delayed.

Answer: B

Explanation: Trial DRS; auth, IRB compliance.

Question: 1131

A long-term care facility in 2026, amid OCR's 2024-2026 audits, discovers resident monitoring cameras streaming ePHI-tagged videos over unsegmented IoT networks, vulnerable to Mirai-like botnets per pentest. The assessment rates IoT as emerging high-threat. What technical safeguard isolates these devices?

A. Upgrade cameras to HIPAA-compliant models with built-in encryption and automatic firmware updates.
B. Create dedicated IoT VLANs with micro-segmentation firewalls blocking outbound traffic except to secure gateways.
C. Route all streams through a secure SD-WAN overlay with traffic inspection at edge routers.
D. Assign static IPs to cameras with MAC address filtering on switch ports.

Answer: B

Explanation: Creating dedicated IoT VLANs with micro-segmentation firewalls blocking outbound traffic except to secure gateways isolates monitoring devices from core networks, preventing botnet propagation

under HIPAA §164.312(f)(1) and NPRM's network controls for IoT. Mirai variants hit 2024 healthcare 15% more. Micro-segmentation enforces zero-trust per device, surpassing upgrades' scope, and integrates physical camera mounts. For long-term care, this protects resident ePHI, aligns with audits, and enhances assessments with traffic logs, mitigating enforcement.

Question: 1132

A healthcare organization wants to balance access to electronic health records with security. Which technical safeguard aligns with regulatory compliance and facilitates this balance?

A. Assigning generic user accounts to reduce password management
B. Open access for all clinical staff without audits
C. Role-based access control with individualized audit trails
D. Disabling automatic session timeouts to improve workflow

Answer: C

Explanation: Role-based access control ensures only authorized users access data necessary for their role, while audit trails provide traceability. Open access and generic accounts breach security principles, and disabling session timeouts increases vulnerability.

Question: 1133

When conducting an environmental risk assessment for a healthcare organization, which element is MOST critical to evaluate for physical safeguards?

A. Control of facility access using badge and visitor management systems
B. Frequency of employee email usage during working hours
C. Number of software updates installed each month on laptops
D. Scheduling policies for clinical staff rotations

Answer: A

Explanation: Physical safeguards include measures to control physical access to facilities and devices, with badge and visitor management systems being essential components. Email usage and software updates relate to technical safeguards and administrative policies, respectively.

Question: 1134

In a scenario where a research institution, acting as a covered entity, receives a subpoena for PHI from a law enforcement agency investigating a multi-state fraud ring involving business associate pharmacies, the privacy officer must verify the requester's authorization. Complicating this, the subpoena includes SUD records under the 2024 Part 2 updates allowing HIPAA-like disclosures with court orders. What verification process best applies the minimum necessary standard while addressing legal enforcement?

A. Disclose the full patient file upon subpoena validation, as law enforcement overrides minimum

necessary for fraud probes.
B. Require patient authorization before any disclosure, citing Privacy Rule patient rights.
C. Forward the subpoena to the business associate for direct response, avoiding entity involvement.
D. Validate the subpoena's authenticity via the issuing court, limit disclosure to fraud-relevant PHI excerpts, and document the rationale per minimum necessary policies.

Answer: D

Explanation: HIPAA Privacy Rule § 164.512(f) permits disclosures to law enforcement with valid legal process like subpoenas, but § 164.502(b) mandates minimum necessary limitations to protect against over-disclosure. The 2024 Part 2 final rule harmonizes SUD records with HIPAA, permitting court-ordered disclosures without separate consent but still requiring verification and minimization. In this fraud scenario, authenticating the subpoena (e.g., via docket checks) and redacting irrelevant PHI (e.g., unrelated treatment history) ensures compliance, with documentation supporting audit defense under OCR enforcement. This balances legal obligations with privacy program administration, unlike blanket disclosures or unauthorized patient involvement.

Question: 1135

A healthcare organization wants to verify that IT technical safeguards meet HIPAA requirements. Which process is most effective?

A. Outsource all IT functions to a third party without internal oversight
B. Focus only on physical safeguards and ignore software controls
C. Conduct a comprehensive risk assessment focusing on authentication, encryption, and audit controls
D. Rely only on vendor self-attestation of compliance

Answer: C

Explanation: A comprehensive risk assessment evaluating technical safeguards such as authentication, encryption, and audit controls ensures compliance with HIPAA security rules. Outsourcing requires oversight, physical safeguards complement but do not replace IT safeguards, and vendor self-attestation is insufficient without independent verification.

Question: 1136

A long-term care facility integrates a new RFID tracking system for resident ePHI badges, but the readers in communal areas are susceptible to signal jamming from unauthorized devices smuggled by staff. With NPRM proposals for anti-jamming in access controls and 2024 enforcement on monitoring failures, how should the risk assessment classify this for physical safeguards?

A. Disable RFID during communal hours
B. Low risk, as jamming is rare, and add basic shielding
C. High criticality for jamming enabling badge cloning, deploy encrypted RFID with jamming detection alerts and staff screening
D. Audit badge usage post-incident only

Answer: C

Explanation: Contingency operations under § 164.310(a)(2)(ii) require procedures for physical access during emergencies, extending to anti-tampering like jamming. The NPRM proposes detection mechanisms for physical threats, per rising insider risks. Jamming allows cloning, compromising all ePHI access. Low classification (B) underestimates; disabling (C) impairs tracking; post-audits (D) miss prevention. Encrypted RFID with alerts enforces unique identification (§ 164.312(a)), screening limits introduction, and high criticality drives remediation in risk analysis, aligning with OCR's $1M+ fines for access control lapses.

Question: 1137

A patient requests a copy of their PHI in electronic format. According to HIPAA, which response complies with their rights?

A. Refuse electronic copies and only provide paper versions to ensure security
B. Provide the PHI promptly in the requested electronic format if readily producible
C. Charge a flat fee regardless of labor or costs involved in producing the copy
D. Deliver the electronic copy only after patient authorization from a notary public

Answer: B

Explanation: HIPAA requires covered entities to provide PHI in the form and format requested by the patient if readily producible. Refusing electronic copies or requiring notarization beyond standard authorization is not compliant. Any fees charged must be reasonable and cost-based.

Question: 1138

A clinic's 2026 drone-delivered med kit includes ePHI trackers without encrypted external syncs, risking interception. Physical handling unverified. What safeguard gap per CPGs, and enforcement?

A. Disposal of devices, recycling.
B. Media safeguards, wipes.
C. Workstation use, geo-fencing.
D. Transmission and physical protections under 45 CFR §164.312(e) and §164.310, enforced via encrypted syncs and chain-of-custody.

Answer: D

Explanation: CPGs target emerging tech like drones with dual safeguards against interception. Enforcement demands encrypted protocols, custody verifications, and risk evals to cover innovative external uses without breaches.

Question: 1139

A patient submits a written request to opt out of all fundraising communications involving their PHI. What must the healthcare organization do to comply?

A. Cease all future fundraising communications involving that patient's PHI
B. Continue fundraising communications but without PHI references
C. Obtain patient's authorization before further fundraising communications
D. Inform the patient that fundraising communications are exempt from opt-outs

Answer: A

Explanation: HIPAA requires covered entities to honor opt-out requests for fundraising communications promptly and refrain from sending further communications that include PHI to that individual.

KILLEXAMS.COM

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*