HIPAA

Exam HIO-301

Certified HIPAA Security Specialist

Version: 6.0

[Total Questions: 120]

Question No : 1

This is a self-contained program that uses security flaws such as buffer overflow to remotely compromise a system and then replicate itself to that system. Identify this program (threat):

A. Trojan horse
B. Trapdoor
C. Master book sector virus
D. Cracker
E. Worm

Answer: E

Question No : 2

The objective of this implementation specification is to conduct an accurate and thorough assessment of the potential vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity.

A. Risk Analysis
B. Network Management Policy
C. Security Policy
D. Access Controls
E. Audit Controls

Answer: A

Question No : 3

The Contingency Plan standard includes this addressable implementation specification:

A. Access Authorization Procedure
B. Testing and Revision Procedures
C. Virus Protection Plan Procedure
D. Sanctions Policy and Procedure
E. Authentication Procedures

Answer: B

Question No : 4

This is a documented and routinely updated plan to create and maintain, for a specific period of time, retrievable copies of information:

A. Disaster Recovery Plan
B. Data Backup Plan
C. Facility Backup Plan
D. Security Plan

Answer: B

Question No : 5

The objective of this standard is to perform a periodic review in response to environmental or operational changes affecting the security of electronic protected health information.

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

Answer: D

Question No : 6

The HIPAA security standards are designed to be comprehensive, technology neutral and:

A. Based on NIST specifications
B. Based on ISO specifications
C. Reasonable
D. Scalable
E. Implementable

Answer: D

Question No : 7

Risk Management is a required implementation specification of this standard:

A. Security Incident Procedures
B. Technical Safeguards
C. Security Management Process
D. Information Access Management
E. Security Configuration Management

Answer: C

Question No : 8

The Security Incident Procedures standard includes this implementation specification:

A. Prevention Procedures
B. Alarm Device
C. Threat Analysis Procedures
D. Detection Procedures
E. Response and Reporting

Answer: E

Question No : 9

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

A. Business Associate Contracts and Other Arrangements
B. Security Incident Procedures
C. Chain of Trust Contract
D. Trading Partner Agreement
E. Assigned security responsibility

Answer: A

Question No : 10

The Security Management Process standard includes this implementation specification:

A. Risk Reduction Policy
B. Audit Control
C. Risk Management
D. Detection Procedures
E. Training

Answer: C

Question No : 11

This addressable implementation specification is about procedures for “overseeing” workforce members that work with electronic protected health information or in locations where it might be accessed.

A. Risk Management
B. Sanction Policy
C. Authorization and/or Supervision
D. Unique User Identification
E. Integrity Controls

Answer: C

Question No : 12

“Evaluation” is a standard within:

A. Administrative Safeguards
B. Physical Safeguards
C. Technical Safeguards
D. Privacy Safeguards
E. Electronic Signatures

Answer: A

Question No : 13

This is a program that is a type of malicious code. It is unauthorized code that is contained within a legitimate program and performs functions unknown to the user.

A. Trojan horse
B. Distributed Denial of Service
C. Stealth virus
D. Polymorphic virus
E. Denial of Service

Answer: A

Question No : 14

Documented instructions for responding to and reporting security violations are referred to as:

A. Business Associate agreement
B. Security Incident Procedures
C. Non-repudiation
D. Sanction Policy
E. Risk Management

Answer: B

Question No : 15

A required implementation specification of the contingency plan standard is:

A. Chain of Trust Agreement
B. Applications and Data Criticality Analysis
C. Security Training
D. Disaster Recovery Plan
E. Internal Audit

Answer: D

Question No : 16

This standard addresses restricting physical access to electronic PHI data through interface devices to authorized users:

A. Facility Security Plan
B. Person or Entity Authentication
C. Workstation Security
D. Contingency Plan
E. Access Control

Answer: C

Question No : 17

An addressable Implementation Specification of Facility Access Controls is:

A. Unauthorized Access
B. Security Configurations
C. Accountability
D. Maintenance Records
E. Media Disposal

Answer: D

Question No : 18

This HIPAA security category covers the use of locks, keys and administrative measures used to control access to computer systems:

A. Technical Safeguards
B. Technical Services
C. Physical Security Policy
D. Administrative Safeguards
E. Physical Safeguards

Answer: E

Question No : 19

Media Re-use is a required implementation specification associated with which security standard?

A. Facility Access Controls
B. Workstation Use
C. Workstation Security
D. Device and Media Controls
E. Access Control

Answer: D

Question No : 20

This is a standard within Physical Safeguards

A. Contingency Operations
B. Workstation Use
C. Security Incident Management
D. Disaster Recovery E. Disposal

Answer: B

Question No : 21

This is a type of a data backup method.

A. Incremental
B. DES
C. Bluetooth
D. IEEE8O2.11 E. WEP

Answer: A