SECURITY

The Manta Group

A Technology Consulting Firm

Name _____

Practice _____

Date _____

Security Rule Test

Q1 – The Facility Security Plan indicates

A. Access within our organization is controlled by a Key system.
B. Access is limited to one employee in the foyer areas at any given time.
C. Access within our organization is allowed if you tailgate another employee.
D. Our organization does not have a Facility Security Plan at this time.

Q2 – The Access Control and Validation Policy indicates

A. When employment ends, the access key need not be returned immediately.
B. Our Organization has no Access Control and Validation Policy.
C. A key marked "Do Not Duplicate" will be issued to each employee to access the facility.
D. Each access badge will contain the team member's nickname and no photograph.

Q3 – The Sanction Policy

A. Outlines specific actions be taken if an employee inadvertently leads to the compromising or breach of ePHI.
B. Sanction policy does not include suspension or other actions up to and including termination of employment if violations of the rule occur.
C. Requires no action be taken if an employee inadvertently leads to the compromising or breach of ePHI.
D. Our organization has no Sanction Policy.

Q4 – According to the Media Re-Use Policy

A. Since we do not deal with any ePHI on any of our computers, this does not apply.
B. I do not know what media means so this does not apply to me.
C. Prior to making storage devices and removable media available for reuse, we must ensure the device does not contain any ePHI
D. We do not have a Media Re-Use Policy.

Q5 – In accordance with the Workstation Use and Workstation Security Policies

A. All employees will implement workstation locking with screensavers on all our company computers.
B. Our organization has no Workstation Use and Security Policies.
C. In that we are behind closed doors, we do not need to use workstation locking with screen savers on all our computers.
D. In that we have more than one person sometimes using a computer, those computers are exempt from the Workstation Use and Workstation Security Policies.

Q6 - The Unique User Identification Policy indicates

A. Our organization has no Unique User Identification Policy.
B. Many users are not required to login to systems before usage is granted. Many users need not login with unique username and password.
C. Usernames should not be identifiable to individuals such as: Jsmith for John Smith.
D. All users are required to login to systems before usage is granted. All users must login with unique username and password.

Q7 – The HIPAA Security Rule Timeline requires health providers to

A. To be compliant by April 21, 2005 with an extra year for small payers – below $5 million, until April 21, 2006.
B. Hope that the legislation will be changed by the Federal Government.
C. Do nothing at the present time.
D. Sometime in the future work on getting ready, but not until after April 2005.

Q8 – The Access Authorization Policy

A. Contains access control features, where available, that must be implemented to allow users access to only data and functions required to perform their duties.
B. Our organization has no Access Authorization Policy.
C. Do not control access to information based on an individual's job responsibilities.
D. Authorizes all employees' access to any folder and data on all of our computers and or servers, regardless of where one works, etc.

Q9 – HIPAA Security Standards Rule

A. Adopts standards for the security of electronic protected health information to be implemented by health providers.
B. Is not going to be approved by the Office of Health and Human Services (HHS)
C. Has no standards or requirements for health providers.
D. Will not become effective until the year 2010.

Q10 – What are some of the possible impacts of not complying with the Security Final Rule?

A. Loss of public confidence in our organization is not considered an impact on not complying with the Security Final Rule.
B. Not complying with the Security Final Rule should have no impact on any covered entity.
C. The impact is not known at this time and thus should be of no concern to our organization.
D. Penalties could include Civil monetary for each violation of a standard, and possible criminal actions for wrongful disclosure of PHI, just to name two.

Q11 – According to the Access Control and Validation Procedures

A. An employee's access badge must be carried in their wallet or purse while on company property.
B. An employee must use a key and/or an alarm code to access company property.
C. When an employee's employment ends. They are allowed to take their access badge with them.
D. There is no Access Control and Validation Procedures at this time.

Q12 - The Security Standards rule

A. Adopts national standards for safeguards to protect non ePHI only.
B. Is to adopt national standards for safeguards to protect the confidentiality, integrity and availability of ePHI.
C. Is not going to affect our organization until the year 2015.
D. Doesn't adopt any standards that impact the way we handle ePHI.

Q13 – What will the enforcement process look like?

A. The enforcement process for HIPAA Security Rule will be both complaint-driven and random audits.
B. CMS would not notify the provider of the complaint.
C. The provider would not have the opportunity to demonstrate compliance, or submit a corrective action plan.
D. If the provider does nothing to correct a violation, CMS will have no authority to impose penalties.

Q14 – The Security rule gives this guidance about policies and procedures

A. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, etc. of the rule.
B. Requires no policies and procedures be written and implemented.
C. The rule doesn't give clear guidance on what policies and procedures should be written or developed to reasonably meet the requirements of the rule.
D. There is only one or two policies and procedures required to meet the standards of the rule.

Q15 - Concerning Addressable Implementation Specifications under the HIPAA Security Rule

A. The need to address these implementation specifications can be deferred up to two years after the Security Rule becomes effective in April of 2005.
B. If the implementation specification is determined to be reasonable and appropriate, the covered entity must implement it.
C. If the implementation specification is identified as addressable we need not be concerned with it at this time.
D. There are no Addressable Implementation Specifications under HIPAA Security Rule, they are only part of the Privacy Rule.

Q16 – The Accountability Policy states

A. We are each accountable for how we spend our weekends and a full report must be given to our supervisors each Monday.
B. We are allowed to move any computer hardware anytime, without contacting the appropriate department.
C. The practice has policies designed to safeguard PHI data as applicable to the practice.
D. We currently do not have an Accountability Policy.

Q17 - The Encryption Policy states that

A. Since I don't know how to encrypt files, this policy does not apply to me.
B. All files that may contain ePHI that are sent over public networks will be encrypted.
C. We see no need here at our organization to use encryption, because we trust no one will try to hack into our system or transmissions.
D. All files containing ePHI that are sent over the network by anyone in our organization need not be encrypted per our policy.

Q18 – What is one of the differences between Privacy and Security under HIPAA?

A. Security requires minimum level of documentation that must be retained for one year.
B. Security standards do not extend to the personnel of a covered entity's workforce even if they work at home.
C. Security Rule covers only ePHI, while the Privacy Rule applies to PHI in paper, oral and electronic form.
D. Privacy applies only to electronic data, Security applies only to people.

Q19 – The Password Management Policy indicates that

A. Passwords must be chosen by the individual's supervisor and kept in confidence.
B. A User's identity will only be authenticated by the use of a password if the appropriate department determines it will be beneficial.
C. A unique User ID must be assigned to each individual User on all company systems.
D. Regardless of the circumstances, passwords must be shared or revealed to anyone else who requests them.

Q20 – The Security Incident Policy requires

A. An employee who becomes aware of unintentional or intentional release of ePHI should immediately notify their HIPAA Compliance Officer.
B. An employee to ensure that all their friends are made aware of a breach of security the moment that it happens.
C. Our organization has no Security Incident Procedures.
D. An employee is to keep all security incidents to themselves and let no one else know about it.