



Security-Related Questions

GENERAL SECURITY

(Multiple Choice) If there is a violation of CHS' Security policies or standards, which of the following is a possible consequence? *Correct Answer: E*

- a. Loss of access privileges to CHS resources
- b. Disciplinary action
- c. Termination of employment
- d. Civil or criminal penalties, fines and imprisonment
- e. All of the above

(Multiple Choice) Why is electronic security being emphasized at CHS? *Correct Answer: D*

- a. CHS must comply with the Health Insurance Portability and Accountability Act (HIPAA) because it is a federal law and CHS' systems contain patient information.
- b. CHS has confidential or proprietary company information, including employee payroll information, which must be protected from unauthorized access.
- c. CHS relies on information integrity to perform its patient care and business functions.
- d. All of the above.

(True/False) After I leave CHS, I am no longer obligated to uphold any of their policies and procedures.

Correct Answer: False

(Multiple Choice) If I suspect there has been a security violation, I should: *Correct Answer: D*

- a. Not tell because I don't want to be associated with the violation or betray a friend
- b. Contact the Facility Security Officer or Corporate Security Officer
- c. Contact my manager or department head
- d. Either B or C are acceptable
- e. Write up a report and store it in a safe place in case it is needed later

(Multiple Choice) Confidential Information includes all the following except: *Correct Answer: D*

- a. Human Resources information
- b. Patient's health information
- c. Communications with business partners
- d. Marketing brochures for my facility

(True/False) Anything I may access, create, store, send or receive on CHS computer systems may be monitored, accessed or reviewed without my consent or knowledge. *Correct Answer: True*

(Multiple Choice) Who is the designated person in my facility ultimately responsible for implementation of the security compliance program and for all security-related issues? *Correct Answer: B*

- a. The Chief Nursing Officer
- b. The Facility Security Officer
- c. The IS Director
- d. The CEO

(Multiple Choice) What is the length of time that HIPAA-compliance documents and policies must be retained?

Correct Answer: D

- a. Only as long as they are applicable, then they should be destroyed.
- b. For 1 year past the date they expired or are no longer applicable.
- c. For 3 years if electronic, or for 5 years if on paper.
- d. For 6 years from the date of creation or the date when it last was in effect, whichever is later.
- e. There is no legal requirement to keep policies, only for keeping patient information.

(True/False) Rebecca does not work in the information technology department, so she does not worry about or take any responsibility for disaster preparedness or emergency operations; she is confident that the IT department is taking care of all that. *Correct Answer: False*

(Multiple Choice) Which of the items below are examples of social engineering? *Correct Answer: E*

- a. A person you do not recognize says he is an employee and left his key/badge in his other jacket and asks that you let him in.
- b. A housekeeping worker appears to be rummaging through the trash.
- c. A phone call from Corporate Information Security saying there is an update they are applying to the network. He asks you for your user ID and password so the update to your account can proceed.
- d. An email claiming you have a tax refund coming to you, and directs you to the official site to claim it. On that site, it asks you to enter your name, social security number, and birth date, so they can verify it is you, and your address so they know where to send the check.
- e. All of the above.

EMAIL & INTERNET

(True/False) All email sent from your CHS email account is considered private and no one else can access messages sent and received. *Correct Answer: False*

(True/False) When using company email, as long as I delete messages, and empty the deleted items folder, there is no trace of my deleted messages. *Correct Answer: False*

(True/False) I should not use inappropriate language or topics that may be considered offensive to others in my email messages or Internet postings. *Correct Answer: True*

(True/False) It is okay to send out non-work-related broadcast messages to other CHS email accounts. *Correct Answer: False*

(True/False) It is okay for me to visit non-work-related websites or send personal emails with sexual, religious or political messages from work, as long as I do it on my own time and it does not interfere with my work. *Correct Answer: False*

(True/False) It is okay to download music files from the Internet onto my work computer for my own use, so long as I do not distribute them. *Correct Answer: False*

PASSWORDS/ACCESS

(True/False) If two users share the same workstation, it is okay for them to share the same user ID and password, too. *Correct Answer: False*

(Yes/No) Karen is home sick, and Alice calls her asking about an important change to a document that Karen made the previous day. Since Alice has a deadline to meet, worth a considerable amount of money to the company, can Karen give Alice her CHS network ID and password, so that Alice can complete the document on time? *Correct Answer: No*

(Multiple Choice) When Jim started work at CHS, he was given access to the financial system. However, Jim's job duties have changed in recent months and have become more clinical. Now, he never has a need to access the financial systems in the course of his normal workday. What should Jim do? *Correct Answer: B*

- a. As long as Jim has access to the clinical systems he needs to do his job, Jim doesn't need to do anything.
- b. Jim should alert his manager and/or the IS Director, so that his privileges on the financial systems can be revoked.
- c. Since another person is now performing Jim's old financially-related duties, Jim should give them his user ID and password so they can do their job.

(Multiple Choice) Leonard has an employee, Myra, who is about to go on maturity leave. What should he do? *Correct Answer: B*

- a. Request that Myra give him her user ID and Password so he can give them to the temp who will be filling in for Myra in her absence.

- b. Submit an access change request to the Service Desk, requesting that Myra's user IDs be inactivated during her leave of absence.
- c. Since user IDs are automatically inactivated after 30 days of non-use, and since Myra will be on leave for 3 months, Leonard doesn't need to do anything.

(Yes/No) The lock to the file storage room has been jamming, and it seems to take forever jiggling the key in it and holding the door "just right" to get it unlocked. This has begun to impede normal business functions, so the file room supervisor taped over the lock so it would no longer jam. Even though the door is not locked now, it has a sign on it saying "Authorized Personnel Only" in order to keep non-authorized people out. Has a serious security infraction been committed under these circumstances? *Correct Answer: Yes*

(Multiple Choice) What is the target of social engineering? *Correct Answer: A*

- a. To gain unauthorized access, either physically or electronically.
- b. To document human behavior so it can be applied to social welfare.
- c. To engineer cultural boundaries within society.
- d. To apply engineering principles and mathematical analysis to social issues.

USE OF CHS RESOURCES

(True/False) If the company has provided equipment for me to use, such as a laptop, Blackberry or printer, I can use it as much as I want for personal use for free. *Correct Answer: False*

(True/False) After I leave the company, if I do not return all CHS provided equipment in good condition, the cost of the equipment and/or its repair could be charged to me. *Correct Answer: True*

(Yes/No) Jane has a neat program she found on the Internet that draws pictures. She downloaded the program at her home, with no bugs or viruses popping up, and has been using it without problems. Now she wants to go ahead and download it to her PC at CHS. Can she? *Correct Answer: No*

(Multiple Choice) Where should important company data be stored on the network? *Correct Answer: B*

- a. "Z" Drive
- b. "H" Drive
- c. USB Drive
- d. "P" Drive

(Multiple Choice) If you have a CHS-owned laptop or Blackberry which is stolen, or is lost or damaged as a result of a crime (auto-theft, home invasion, etc.), which of the following should you do? *Correct Answer: C*

- a. Report the incident to the police.
- b. Report the incident to the CHS Service Desk
- c. All of the above
- d. None of the above

(Multiple Choice) Richard leaves his desk to go to lunch without locking his PC (he did not press Ctrl-Alt-Del and select 'Lock Computer'). Is this a security violation? *Correct Answer: A*

- a. Yes, because someone else could access his email and files.
- b. No, because after 15 minutes, the screen-saver will kick in.

(True/False) It is okay for PHI to reside on a USB drive (thumb drive) or a CD/DVD or floppy disk, as long as I keep it in my possession all the time. *Correct Answer: False*

(Multiple Choice) Which of the following should never be sent via email: *Correct Answer: E*

- a. PHI
- b. User IDs and passwords
- c. Social security numbers
- d. Credit card or billing information
- e. All of the above

(True/False) If a piece of equipment - like a computer monitor, hard drive or a Blackberry - is non-operational (broken, not working) I must return it to the IS Department, because it is illegal to dispose of it in the trash.
Correct Answer: True

(Multiple Choice) Alex has a CHS-issued laptop which he uses as his desktop. He leaves it on his desk overnight and only takes it with him when he is traveling or occasionally on weekends. Alex is sure to log off the network before leaving for the day, and never stores PHI on his laptop's local drive, but what is Alex forgetting? *Correct Answer: A*

- a. Laptops are easy targets for theft and so it must be locked up when not in use (such as in a locked cabinet) or it must be secured with a locking tether cable.
- b. Alex must also power off the device or unplug it.

(Multiple Choice) Which if the following items should NOT be disposed of in the secure shred trash bins.
Correct Answer: D

- a. Hospital census info showing patients names, room numbers, and doctor.
- b. Printouts of source code and/or system configurations
- c. Company org charts and/or phone lists
- d. Coupons redeemable for a free drink with purchase at a local restaurant.
- e. Unused (blank) company letterhead