**Topic 1: Analyze Your Pharmacy for HIPAA Compliance**

Consider your local pharmacy. What physical, technical, organizational and administrative safeguards have you observed at this pharmacy? Post your observations to the message board. Respond to other person’s posts.

Down at the CVS   Edward Jackson Email this Author   10/25/2014 2:43:39 PM

When considering HIPAA compliance, I expect patient health information and patient data to be protected at all costs. My visit down to the local CVS proved that HIPAA compliance is taken seriously by the CVS pharmacy. For example, right when I walked in the store, I noticed security cameras everywhere. The cameras are a good idea to assure all traffic to the medication area is tracked. I also noticed to get into where the medications were being stored there was a metal key punch code. This is to keep unauthorized personnel and customers out of the medication area, as well as to protect patient information located in computers and on prescription labels. One thing that I thought was a great idea is how the prepared prescriptions were being stored. They were in bins facing the front counter, but had a white plastic shield in the front of the bin to cover up the patient information on the prescription. This way, the medications were easily assessable by staff, but the patient information could not be seen from the front counter.

I’m not sure if it was intentional or not, but I could not hear anything the two people behind the counter were talking about. Not being able to hear the staff preparing the medications helps to further protect patient information from listening ears. One final thing that I thought was good was that I could easily tell the difference between non-pharmacy staff, and the regular store staff. This is good because I would not want to walk up to regular store personnel and begin talking about by health problems, and asking for certain medications (I am also sure the normal staff does not want to hear it anyways). Overall, the CVS seems to take HIPAA compliance very seriously, as they have multiple layers of security in place.

As far as what could be better, I did not see many improvements. I did notice that the prescription bags themselves had information on the front; perhaps this could be covered with some type of paper flap.

**Topic 2: Hot topics with HIPAA Compliance**

What is a hot issue this week in the security arena as it relates to this unit’s topic? Summarize one of these issues on the message board, and respond to another person’s post.

HIPAA not violated   Edward Jackson Email this Author   10/25/2014 3:40:46 PM
My article comes from Internal Medicine News and outlines a potential HIPAA violation. Gallegos (2014) discuss a HIPAA issue where a federal tort reform rule was upheld in a Florida court. The exact issue was whether state law was violating federal law when it came to giving doctors access to a patient’s records during a malpractice law suit. Basically, when a doctor is sued for some form of malpractice, the Florida law was allowing the doctor to access patient records, to provide and build a better case. A patient was saying this violated their privacy, and that the rule should be banned. However, a three-judge panel overturned the appeal, stating that the Florida law did violate any HIPAA compliance laws. I do understand both sides of this argument, but from the doctor’s perspective, they get sued for basically everything (even if the patient lies or has some pre-existing condition). I do not think it is wrong for doctors to want to obtain all the facts.

Reference


Information Security and the Health Care Industry

The Health Insurance Portability and Accountability Act of 1996 is usually called just “HIPAA.” The Privacy Rule standards address the use and disclosure of individuals’ health information — called “protected health information” by organizations subject to the Privacy Rule — called “covered entities”, as well as standards for individuals' privacy rights to understand and control how their health information is used. Within the department of Health & Human Services, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

From a security perspective there are four major areas of HIPAA compliance. They are:

- Administrative Safeguards
- Organizational Safeguards
- Physical Safeguards
- Technical Safeguards

Outcomes
After completing this unit, you should be able to:

- Evaluate the meaning of HIPAA administrative and organizational safeguards.
- Select the administrative and organizational safeguards HIPAA standards for a medical office.
- Differentiate the meaning of HIPAA physical and technical safeguards.
- Recommend the physical and technical safeguards HIPAA standards for a medical office.

Course outcome(s) practiced in this unit:

IT540-4: Assess computer networks for regulatory compliance.

What do you have to do in this unit?

- Complete assigned Reading.
- Complete the Learning Activity.
- Participate in Discussion.
- Complete unit Assignment.
- Review Program Portfolio.

Reading

Read Chapter 3: “Legal, Ethical, and Professional Issues in Information Security,” in your text.

Also, Open your textbook, peruse Chapter 7: “Security Technology: Intrusion Detection, Access Control, and Other Security Tools,” and Chapter 8: “Cryptography.”

Key Terms

existing fraud and abuse provisions, and penalties for fraud violations by health care providers

**Federal Privacy Act of 1974:** Regulates government agencies and holds them accountable if they release private information about individuals or businesses without permission.

**Electronic Communications Privacy Act of 1986:** The act was primarily designed to prevent unauthorized government access to private electronic communications.

**Financial Services Modernization Act:** Requires all financial institutions to disclose their privacy policies on the sharing of nonpublic personal information.

**Security and Freedom through Encryption Act of 1999 (SAFE):** Provides guidance on the use of encryption and provides measures of protection from government intervention.

**Sarbanes-Oxley Act of 2002:** A critical piece of legislation that affects the executive management of publicly traded corporations and public accounting firms, seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies.

**Freedom of Information Act:** Allows any person to request access to federal agency records or information not determined to be a matter of national security.

**Vocabulary provided by:** Free dictionary.com/HIPAA

---

**Unit 6 Assignment**

**Outcomes addressed in this activity:**

- Evaluate the meaning of HIPAA administrative and organizational safeguards.
- Select the administrative and organizational safeguards HIPAA standards for a medical office.
- Differentiate the meaning of HIPAA physical and technical safeguards.
- Recommend the physical and technical safeguards HIPAA standards for a medical office.
Outcomes addressed in this activity:

- Evaluate the meaning of HIPAA administrative and organizational safeguards.
- Select the administrative and organizational safeguards HIPAA standards for a medical office.
- Differentiate the meaning of HIPAA physical and technical safeguards.
- Recommend the physical and technical safeguards HIPAA standards for a medical office.

Course outcome:
IT540-4: Assess computer networks for regulatory compliance.

Instructions:
Note: All written assignments should be completed using APA format, unless otherwise noted in the instructions.

Read the following information about a typical dental practice:

- Family Dental has two offices in the same city — the North office and the South office. These offices offer the same dental services to patients. Patients can make appointments to either office at their convenience to see the dentist of their choice. Both offices are similarly equipped.
- The professional staff includes the dentists, hygienists, dental mechanics, and administrative staff (receptionist, billing clerk, and office manager).
- Each Family Dental office has a waiting area served by a receptionist who uses a computer to check in patients, schedule one of the examination rooms, and answer the phone. The waiting room has a door opening to the outside. A second door admits patients into the rest of the facility. Background music plays inside the waiting area. There is also a large aquarium on display.
- Each examination area is partitioned off from the adjacent ones. Each has a computer and LCD screen used to pull up patient information and record new dental data such as x-ray interpretations, examination and test results, and procedures done for the patient. A low level sound masking system is installed in this area.
- After their treatment the patient visits the billing clerk’s desk, which of course has a computer and a printer. Here patients pay (cash co-pay, credit card, or check), insurance information is verified, and an appointment is made. This clerk also mails out postcard appointment reminders, and answers the phone.
- The Family Dental dentists share a private office that has a computer and a printer. Here they can review patient data, access the Internet, and exchange email with their patients, colleagues, and acquaintances.
- A database server containing patient data sits in a closet, next to a small tape library used for backup. Next to it sits a VPN server, firewall/router, and DSL modem connected to the Internet. The VPN server accepts incoming connections from the dentist’s home computers. It also provides a permanent VPN connection between the North and South Offices. In this way, all patient data is available at all times at either office.
- Most patient data is stored electronically on the database server, but some data such as x-rays and third party labs results are still in physical form. Family Dental also depends on third party service providers to build crowns, braces, false teeth, soft dental protectors, and such. Information is exchanged with service providers using telephone, fax, letter, and email.
- The network infrastructure’s management and maintenance is outsourced.
Family Dental also maintains an informative web site to advertise its practice. The site is remotely hosted. Answer the following questions in essay style. Make any sensible assumptions necessary in order to continue your analysis. Feel free to use the Discussion board to share your assumptions with others in the class:

Q1 What is all the electronic and non-electronic private health information (ePHI) that is stored, processed, and transmitted at the Family Dental’s two offices?
Q2 Assess the practice’s organization. Where is it most likely HIPAA compliant? What changes should be made to move the practice closer to compliance?
Q3 Assess the practice’s physical and technical safeguards. Where is it most likely HIPAA compliant? What changes should be made to move the practice closer to compliance?
Q4 Family Dental exchanges data with service providers and uses a third party to manage its IT infrastructure. What administrative and organizational safeguards should the practice expect these providers to adhere to?

Assignment Requirements:
Submit your Assignment in the usual double-spaced APA-styled report. Content should be a minimum of four double spaced pages, APA style followed (title page, abstract, table of contents, and references section) to meet expectations.

- Answers contain sufficient information to adequately answer the questions
- No spelling errors
- No grammar errors

*Two points will be deducted from grade for each occurrence of not meeting these requirements.
For more information and example of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.
Also review the KU Policy on Plagiarism. This policy will be strictly enforced on all applicable assignments and discussion posts. If you have any questions, please contact your professor.
Review the grading rubric below before beginning this activity.

Assignment Grading Rubric

Course: IT540 Unit: 6 Points: 136
Copyright Kaplan University
Assignment grading rubric = 136 points
Assignment Requirements Points
Possible Points Earned
Q1. Electronic and non-electronic private health information is identified at Family Dental’s two offices. 0–34
Q2. Areas where Family Dental’s organization is in HIPAA compliance are identified. Measures to bring Family Dental closer to compliance are described. 0–34
Q3. Areas were Family Dental is in
HIPAA compliance with physical and technical safeguards are identified. Measures to bring Family Dental closer to compliance are described.

Q4. Administrative and organizational safeguards that service providers must adhere to are described.

Column Total 0–136
Less deduction taken for spelling, grammar and APA errors. Plagiarism is totally unacceptable

New total after deductions