College Name

College Name CIS - Tech Support Infusion Program Curriculum Health IT Module Content

Program Course Information

CIS Topics in Healthcare Security Summary
This course consists of weekly lectures, labs and online sessions. There is an emphasis on healthcare computer security, topics include identifying threats and points of vulnerability in healthcare IT systems, access control and its relation to HIPPAA, security related to patient data, workflow challenges, healthcare regulations that impact data security, and preparing various security attacks.

Course Learning Objectives

At the completion of this course the student should be able to:

- Describe the effects of HIPAA on system security in a healthcare environment.
- Recognize the potential vulnerabilities that result from the interaction of multiple systems in a healthcare environment.
- Discuss ways to employ access controls to protect patient data and meet HIPAA requirements.
- Describe ways to mitigate the challenges to system security posed by clinical workflows.
- Discuss ways to enhance the usability of security measures to encourage compliance.
- Identify potential security issues in system acquisition and implementation.
- Discuss ways to maintain security so that it meets governmental regulations.

Course Topics

- Privacy and Security laws and regulations
- Potential points of vulnerability in a healthcare IT system – covers the interfaces between systems
- Interoperability Standards and Certification
- Impact of end users on HIT security, particularly in applications
- Access control and its relation to HIPAA
- Security related specifically to patient data (influence of HIPAA, and other regulations)
- Workflows and their challenges to security
- Importance of usability to maintaining security

Module 1: Basics of HIPAA and Health IT Systems – 2 hours lecture / 2 hours lab / 4 hours online sessions

Topics, Descriptions and Objectives

a. Privacy and Security laws and regulations

In this unit students will learn about the basic structure of HIPAA and which sections apply to them as Network Engineers. The will learn to describe the effects of HIPAA and the basic security measures that need to be put into place in order to be considered HIPAA compliant.

Objectives	**Material** (Lecture/article/video/web resources/textbook and pages) – *Please include proper citation for resource*
Describe the effects of HIPAA on system security in a healthcare environment. Discuss ways to maintain security so that it meets governmental regulations.	HIPAA Overview, Lecture 1
Describe the effects of HIPAA on system security in a healthcare environment.	CAHIMS lesson 1.4 (Bellevue College CAHIMS Exam Preparation Course)
Recognize the potential vulnerabilities that result from the interaction of multiple systems in a healthcare environment.	CAHIMS lessons 2.2, 2.4, 2.5 and 2.6 (Bellevue College CAHIMS Exam Preparation Course)

Learning Activities/Assignments

Describe, in detail, the learning activities for this Week and list any materials or resources needed to complete the activity/assignment.

Activity 1—Title: *Medical Office Practical HIPAA Use*

http://www.healthit.gov/sites/default/files/cybersecure/cybersecure.html

In this activity students will make choices for the doctors and office personal. You will be presented 4 different options per question and one of them is the most HIPAA compliant, the others are not. At the end of the game you will be presented with your completion and an option to go to notes about HIPAA compliance.

Resources Needed: Internet access

Activity 2—Title: *Obscuring HIPAA Sensitive Information*

Students will practice sending information back and forth between simulated HIPAA compliant organizations. This activity gives students practice with HIPAA compliance and understanding what is considered Patient Health Information (PHI).

Resources Needed: Obscuring HIPAA Sensitive Information plan document, Practice Insurance Claim documents, GIMP2 image editor program

Claim 1, Claim 2, Claim 3, Claim 4

Discussion Questions

Discussion Question 1: After completing activity 2, what information did you choose to blur? Why did you choose to blur that information? Was there any PHI that was not blurred but should have been? What was it?

Optional Resources

GFI: HIPAA — IT compliance

4Medapproved Learning Lunch featuring Mike Semel

HIPAA 101: The Basics of HIPAA Administrative Simplification

Assessment Questions

1. What are the three main parts of HIPAA?

    a. Privacy, Accountability, Security

    b. Confidentiality, Accountability, Security

c. *Privacy, Code Sets, Security

d. Integrity, Code Sets, Privacy

Feedback: Information on this topic can be found in HIPAA Overview, Lecture 1

Objective to which this item maps: Module 1, topic a, objective 1.

2. What are the three main sections of the Security Rule?

   a. Administrative, Physical, Technical

   b. Privacy, Code Sets, Security

   c. Viral, Physical, Software

Feedback: Information on this topic can be found in HIPAA Overview, Lecture 1

Objective to which this item maps: Module 1, topic a, objective 1.

3. What is “Creditable Coverage” as defined by HIPAA?

_____

_____

*Defined quite broadly and includes nearly all group and individual health plans such as Medicare and Medicaid.

Feedback: Information on this topic can be found in HIPAA Overview, Lecture 1

Objective to which this item maps: Module 1, topic a, objective1.

4. What is a “Significant Break” as defined by HIPAA?

_____

_____

Feedback: Information on this topic can be found in HIPAA Overview, Lecture 1

Objective to which this item maps: Module 1, topic a, objective1.

*Defined as any 63 day period without any creditable coverage.

5. What does Title II: “Administrative Simplification” cover?
    a. The Privacy Rule
    b. Transactions and Code Sets Rule
    c. Security Rule
    d. Unique Identifiers Rule
    e. Enforcement Rule
    f. *All of the above

Feedback: Information on this topic can be found in HIPAA Overview, Lecture 1

Objective to which this item maps: Module 1, topic a, objective1.

Module # 2: Fundamentals of Social Engineering, Mitigation and Interoperability Standards – 2 hrs lecture / 2 hrs lab / 4 hours online sessions and research

Topics, Descriptions and Objectives

a. Potential points of vulnerability in a healthcare IT system – covers the interfaces between systems; Impact of end users on HIT security, particularly in applications.

In this unit students will learn how to identify common forms of social engineering. Students will also learn about the different methods that they can educate their peers and how to ensure that specific security practices are being retained and followed.

Objectives	Material (Lecture/article/video/web resources/textbook and pages) – Please include proper citation for resource
Describe ways to mitigate the challenges to system security posed by clinical workflows. Discuss ways to maintain security so that it meets governmental regulations. Discuss ways to enhance the usability of security measures to encourage compliance.	Fundamentals of Social Engineering and Mitigation Lecture

b. Interoperability Standards and Certification

In this section students will learn about issues of interoperability and integrating new HIT systems with an existing network and its systems. Students will also learn about the security practices needed in order to be compliant with both internal and external standards.

Objectives	**Material** (Lecture/article/video/web resources/textbook and pages) – Please include proper citation for resource
Identify potential security issues in system acquisition and implementation. Discuss ways to maintain security that it meets governmental regulations.	CAHIMS Lessons 4.1 and 4.3 (Bellevue College CAHIMS Exam Preparation Course)

Learning Activities/Assignments

Activity 1—*Spotting the HIPAA Violations*

This exercise will help you see the different choices that may be presented in a work environment. These choices will have different impacts on how customers respond and how as a company you are required to be HIPAA compliant.

Resources Needed: Spotting the HIPAA Violations Document, Internet Access

Activity 2 – *Security Breaches in the Health Field* (Students can write their responses or have discussions about the issues.)

Students will research and investigate three recent breaches of security in the medical field. They will provide a summary of the incident along with proper citation of the article and then discuss if this was breach was preventable and what security precautions should be taken in order to ensure that such a breach does not occur again.

Resources Needed: Security Breaches in the Health Field Document, Internet Access

Activity 3 – CAHIM 4.1 Quiz (Education College CAHIMS Exam Preparation Course)

This activity will test the students to ensure that they understand the content that was covered. They should be able to answer questions related to systems selection and

evaluation process, Interoperability and integration assessment and systems certification and validation.

Resources Needed: Internet Access

Activity 4 – CAHIM 4.3 Quiz (Education College CAHIMS Exam Preparation Course)

This activity will test the students to ensure that they understand the content that was covered. They should be able to answer questions related to standards for health IT, IOM report on health IT and patient safety, changes with the HITECH Act, and systems compliance.

Resources Needed: Internet Access

Discussion Questions

Discussion Question 1

Give some examples of “red flags” when in the middle of a potential social engineering attack. What methods can we use to teach our co-workers about social engineering and how can we ensure that these practices are being followed?

Optional Resources

None needed

Assessment Questions

1. A fake email sent to an employee in an attempt to steal information is what type of social engineering attack?

    a. *Phishing

    b. Fishing

    c. Spear Hunting

    d. Pretexting

Feedback: Information on this topic can be found in Fundamentals of Social Engineering and Mitigation Lecture

Objective to which this item maps: Module 2, topic a, objective 1.

2. What step or steps will help to prevent incidents of dumpster diving? (Circle all that apply)

   a. *Shredding documents

   b. Leave dumpsters out on the sidewalk

   c. *Leave dumpsters on private property

   d. Set it and forget it

Feedback: Information on this topic can be found in Fundamentals of Social Engineering and Mitigation Lecture

Objective to which this item maps: Module 2, topic a, objective 1.

3. When in a crowded area what issue is a typical problem for employees?

   a. Pretexting

   b. *Public Disclosure

   c. Shared Information

   d. Shoulder surfing

Feedback: Information on this topic can be found in Fundamentals of Social Engineering and Mitigation Lecture

Objective to which this item maps: Module 2, topic a, objective 1.

4. List one defensive tactic that helps prevent social engineering.

   _____

*Possible answers can be: Utilize Defense-in-Depth, Develop policies and procedures to address possible threats, Ensure that employees understand legal requirements and recourses.

Feedback: Information on this topic can be found in Fundamentals of Social Engineering and Mitigation Lecture

Objective to which this item maps: Module 2, topic a, objective 1.

5. In a company who can be a potential target of a social engineering attack?

   a. Receptionist

   b. CEO

   c. Intern

   d. Janitor

   e. *All of the above

Feedback: Information on this topic can be found in Fundamentals of Social Engineering and Mitigation Lecture

Objective to which this item maps: Module 2, topic a, objective 1.

Health IT Module 3: Network and Systems Implementation – 2 hrs lecture / 2 hrs lab / 4 hours online sessions and research

Topics, Descriptions and Objectives

a. Access control and its relation to HIPAA

This unit focuses on how to set up access controls, select components and upgrade a network to meet HIPAA requirements. Students will understand the potential security risks that can accompany interaction of multiple systems in a healthcare environment.

Objectives	**Material** (Lecture/article/video/web resources/textbook and pages) – Please include proper citation for resource
Discuss ways to employ access controls to protect patient data and meet HIPAA requirements Recognize the potential vulnerabilities that result from the interaction of multiple systems in a healthcare environment. Identify potential security issues in system acquisition and implementation.	Upgrading a Theoretical Network Lecture

b. Workflows and their challenges to security

In this unit students learn how to look at an HIT system and the steps involved in an implementation process. They will learn about HIT best practices and compliance in regards to monitoring and basic maintenance of HIT systems. Students will learn about issues that end users may run into and tactics on how to support and train them.

Objectives	**Material** (Lecture/article/video/web resources/textbook and pages) – Please include proper citation for resource
Discuss ways to maintain security so that it meets governmental regulations. Discuss ways to employ access controls to protect patient data and meet HIPAA requirements.	CAHIMS Lessons 5.1, 5.2 and 5.3 (Bellevue College CAHIMS Exam Preparation Course)

Learning Activities/Assignments

Activity 1 – *Research and Design a Network Topology*

This activity will have students researching HIPAA compliant networks; they will then use that research to help them design their own HIPAA compliant network topology.

Resources Needed: Microsoft Visio, Internet Access

Activity 2 – CAHIM 5.2 Quiz (Bellevue College CAHIMS Exam Preparation Course)

This activity will test the students to ensure that they understand the content that was covered. They should be able to answer questions related to end user training and support.

Resources Needed: Internet Access

Discussion Questions

Discussion Question 1

What are some of the challenges when upgrading a network? How can we ensure that our network stays HIPAA compliant? What are some ways to ensure that we are able to train and support our end users effectively?

Optional Resources

None

Assessment Questions

1. List at least one issue with having multiple directory services (such as Active Directory) for your users.

   _____

   _____

   *Possible answers may include but are not limited to, multiple ID's and passwords which increase likelihood of end users forgetting their passwords. Also poses a security risk to the network.

Feedback: Information on this topic can be found in Upgrading a Theoretical Network Lecture

Objective to which this item maps: Module 3, topic a, objective 1.

2. List at least one security benefit for implementing Blackberry devices for employees.

   _____

   _____

   *Possible answers may include but are not limited to, encrypted traffic from blackberry device and company network, ability to remotely wipe device should it be stolen or lost.

3. List at least one Con for users when building and implementing a new network.

   _____

   _____

*Possible answers may include but are not limited to, migration of email; some users may need to learn new applications; compatibility with non-Windows users, some users are adverse to change.

Feedback: Information on this topic can be found in Upgrading a Theoretical Network Lecture

Objective to which this item maps: Module 3, topic a, objective 1.

4. List at least one Con for us as network administrators when building and implementing a new network.

_____

_____

*Possible answers may include but are not limited to, migration costs of new hardware and software, mono-configuration issues, and the pressures of changing and maintaining a new network.

Feedback: Information on this topic can be found in Upgrading a Theoretical Network Lecture

Objective to which this item maps: Module 3, topic a, objective 1.

5. List one reason why it is important to have a well-documented and updated network topology.

_____

*Possible answers may include but are not limited to, it is required by HIPAA, it is a useful troubleshooting tool should there be a network error.

Feedback: Information on this topic can be found in Upgrading a Theoretical Network Lecture

Objective to which this item maps: Module 3, topic a, objective 1.

Health IT Module 4: HITECH Act - Implementation and Security– 2 hour lecture / 2 hour lab / 3 hours online sessions and research

Topics, Descriptions and Objectives

a. Security related specifically to patient data (influence of HIPAA and other regulations)

This unit presents an overview of information exchange systems and the standards that impact privacy and security of data.

Objectives	Material (Lecture/article/video/web resources/textbook and pages) – Please include proper citation for resource
Discuss ways to employ access controls to protect patient data and meet HIPAA requirements. Describe ways to mitigate the challenges to system security posed by clinical workflows Discuss ways to maintain security so that it meets governmental regulations Describe the effects of HIPPA on system security in a healthcare environment	Whatcom HInet Lecture (Whatcom HInet, Guest Lecturer Lori Nichols)

b. Security related specifically to patient data (influence of HIPAA and other regulations)

In this unit students learn strategies, best practices and tools used in the healthcare industry to identify and assess data security risks. Students will learn about the elements involved in internal and external audits.

Objectives	Material (Lecture/article/video/web resources/textbook and pages) – Please include proper citation for resource
Discuss ways to maintain security so that it meets governmental regulations	CAHIMS Lessons 7.2 and 7.3 (Bellevue College CAHIMS Exam Preparation Course)

Learning Activities/Assignments

Describe, in detail, the learning activities for this Week and list any materials or resources needed to complete the activity/assignment.

Activity 1 – CAHIM 7.2 Quiz (Bellevue College CAHIMS Exam Preparation Course)

This activity will test the students to ensure that they understand the content that was covered. They should be able to answer questions related to best practices, tools used in the healthcare industry to identify and assess data security risks. Students should also be aware of what is involved in internal and external audits.

Resources Needed: Internet Access

Activity 2 – CAHIM 7.3 Quiz (Bellevue College CAHIMS Exam Preparation Course)

This activity will test the students to ensure that they understand the content that was covered. They should be able to answer questions related to management of both physical and digital access to data and systems and the security that is required in a healthcare setting.

Resources Needed: Internet Access

Discussion Questions

Discussion Question 1:

What benefits and reasons are there to convert to EHR? What are the challenges and benefits of the HITECH Act?

Optional Resources

None

Assessment Questions

No Assessment Questions at this time.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration, Grant #TC-23745-12-60-A-53. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites and including, but not limited to, accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.