

Common Course Outline for: HCST 2200 Privacy and Security in HCST

A. Course Description

1. Number of credits: 2
2. Lecture hours per week: 2
3. Lab hours per week: *None*
4. Prerequisites: HCST 2100
5. Co-requisites None
6. MnTC Goals None

This course will develop an understanding of the need for privacy and security in the health care industry. This course will emphasize government mandated privacy and security requirements, the importance of compliance, and ways to implement privacy and security during software development.

B. Date last revised: March, 2014

C. Outline of Major Content Areas

Fundamental of Privacy and Security in Healthcare industry
Government mandated privacy and security compliance requirements
Software development and privacy and security compliance
Privacy and security best practices

D. Course Learning Outcomes

Upon successful completion of the course, the student will be able to:

1. Understand the fundamentals of security and privacy, current issues, recent statistics related to healthcare industry
2. Define the Electronic Medical Records and its functions in clinics and hospitals
3. Define Government mandated privacy and security regulations and consequences of non-compliance
4. Understand types of Internet access and the usage policies, the security risks, such as, Virus, Worms, Hacker attacks, cookies, web bugs, web site log analyzer
5. Understand both hardware and software Firewalls and their roles in privacy and security
6. Understand Email Issues such as Imbedded gifs, Spam, scams, hoaxes, viruses, attachments; risks associated with running other applications such as Chat, IM, File Sharing, online gaming, and other peer-peer applications, media streaming
7. Understand user actions to protect security and privacy such as installing operating system updates, use of passwords, local file encryption, passwords and industry standards
8. Define security policies regarding network security, including definitions of authentication, VPN, Intrusion detection, Virus Software, and Firewalls

9. Understand future techniques such as biometric identification, legislative trends, security of other online devices (smart phones, PDA's)

E. Methods for Assessing Student Learning

The instructor will choose from among various classroom evaluation techniques including – but not limited to – in-class testing, take-home testing, assignments, quizzes, attendance, group or individual projects, peer evaluation and research. The instructor will also choose a method for end-of-the-semester evaluation.

F. Special Information *None*