F12-90820 Health Care Information Security  
Mondays, 5:30–8:20 PM  
August 29 – December 12, 2012  
Instructor: Greg Porter

Course Description

This 12-unit course is designed to provide graduate students with an introduction to current and emerging issues in health care information security, privacy and regulatory compliance. Health Care Information Security (HCIS) is an elective course within the Master of Science in Health Care Policy and Management (HCPM) program but is open to other students throughout the Heinz College programs, both technical and non-technical alike, with an interest in health information related security. The goal of the HCIS class is to provide the student with a substantive overview and analysis of relevant information security subject matter that is having a direct and material impact on the U.S. health care system.

The learning objectives of this course are to:

- Gain an understanding of foundational information security concepts, such as the purpose and components of policy, the principles of confidentiality, integrity, and availability, common security threats and the application of appropriate risk management concepts;
- Understand current & emerging health care legislation including the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, Meaningful Use, and the Department of Health and Human Services (HHS) Breach Notification Rule;
- Develop an understanding of the HIPAA Security Rule and how it directly impacts the protection of health care information and systems;
- Describe risk based health care governance models and recognized practices to comply with the intent of HIPAA and other regulatory demands. Review frameworks that can be used to manage the security of medical information such as those created by the International Organization for Standardization (ISO), SEI-CERT, and HITRUST;
- Review the breach notification requirements as implemented by the HITECH Act;
- Review current and emerging threats to health care information security such as those introduced by unbounded networks and mobility, social networking, the criminal underground, insider threats, web based technologies, and insufficiently governed operations;
- Gain a fundamental understanding of encryption technologies, why they are required (or not) and considerations for implementation;
- Examine the relationship between HHS, the Centers for Medicare & Medicaid Services (CMS), and the Office for Civil Rights (OCR) and how regulatory compliance is being enforced;
• Review aspects of information security within Health Information Technology (HIT), the role of HHS and the Office of the National Coordinator (ONC), federal HIT standards issues, including electronic health record (EHR) certification criteria and implementation specifications for the meaningful use of EHR's for the Medicare and Medicaid EHR Incentive Programs.
• Obtain familiarity with reasonable and appropriate protected healthcare information (PHI) administrative, physical, and technical safeguards;

Course Text
Course Structure

The course material will be separated into four modules covering a related series of topics:

- Module One: Health Care Information Security Fundamentals
- Module Two: Health Care Information Security Regulatory Landscape
- Module Three: Risk Based Governance & Compliance
- Module Four: HIT, EHR’s and Maintaining and Monitoring Compliance Through Administrative, Physical & Technical Controls

Generally, each module will be covered over the course of 3 weeks. Each week, classes will be broken into two sessions separated by a fifteen minute break:

- Session 1: 5:30 PM – 6:45 PM
- Break: 6:45 PM – 7:00 PM
- Session 2: 7:00 PM – 8:20 PM

Course Requirements

Four key components will be used to evaluate student performance during the course:

- Participation 10%
- Quizzes (3) 35%
- Group Project 20%
- Final Exam 25%

Participation: This course is designed to engage the student, requiring that both the students and the instructor come to class prepared. Students are expected to read the assigned text and writings prior to class so that you are prepared to discuss relevant subject matter. Students are expected to attend every class; planned absences should be discussed in advance with the instructor.

Quiz: Two quizzes will be given during the semester, one following module 2 and one following module 3. The quizzes will cover key areas covered in modules one, two and three respectively. Additional details will be provided to students at least one week prior to the quiz.

Group Project: The ability to collaborate is an essential element to a successful career in health care. In the second half of the semester, students will be assigned to work groups consisting of 3-4 individuals. The group project will require students to address a pertinent health care information security area based on an assigned topic. Additional details about the group project will be provided in class.

Final Exam: There will be a cumulative closed book final exam at the end of the class. Although subject to slight alterations, the final exam will contain a mixture of multiple choice and short essay questions.

Grading Scale

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>98-100%</td>
</tr>
<tr>
<td>A</td>
<td>93-97%</td>
</tr>
<tr>
<td>A-</td>
<td>90-92%</td>
</tr>
<tr>
<td>B+</td>
<td>87-89%</td>
</tr>
<tr>
<td>B</td>
<td>83-86%</td>
</tr>
<tr>
<td>B-</td>
<td>80-82%</td>
</tr>
<tr>
<td>C+</td>
<td>77-79%</td>
</tr>
<tr>
<td>C</td>
<td>73-76%</td>
</tr>
<tr>
<td>C-</td>
<td>70-72%</td>
</tr>
</tbody>
</table>