FIU | FLORIDA INTERNATIONAL UNIVERSITY

COURSE SYLLABUS

ISM 6326 Information Security and Compliance

GENERAL INFORMATION

PROFESSOR INFORMATION

Instructor:	Dr. Christopher Sullivan, PhD	**Phone:**	(850) 591-2821
Office:	FIU Brickell Campus, FDBN 234	**Fax:**	(305) 348-4126
Office Hours:	Saturday, 8:00-12:30 AM	**E-mail**	cbsulliv@fiu.edu
Website:	imageresearch.com/infosec		

COURSE DESCRIPTION

This course covers the regulatory, technical and organizational aspects of privacy and security in health care settings. Information security in health care is regulated by a complex of federal and state laws and regulations, by the technical requirements of cybersecurity and by executive management decisions on dealing with risk to information technology and workforce training in security. Introducing students to this important area requires that all three security settings are addressed and integrated to demonstrate how regulatory, technical and organizational factors all impact information security and compliance.

The course will cover the three areas presented above. The first section will cover the Health Information Privacy and Portability Act (HIPAA) requirements as laid out in the HIPAA Privacy Rule and the HIPAA Security Rule. This section will also cover the role of state laws in ensuring the privacy of “super-confidential” medical records with particular attention to Florida statutes. Finally, the section will address the compliance requirements of HIPAA and state law and data breach penalties.

The second section will cover the technical issues of cybersecurity with an overview of telecommunications and computer networks, the threats created by cyber-attacks and the measures that must be taken to ensure the security of Health IT on an ongoing basis. This section will also cover guidelines for health IT security such as the Federal Information System Management Act of 2002 (FISMA), the special publications on Health IT Security from the National Institute for Standards and Technology (NIST) and information security standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The final section of the class will cover management issues of information security including determining acceptable risk levels, security training, risk analysis and risk mitigation. This part of the course will use the NIST Risk Framework to develop overall risk policies and procedures and will cover risk assessment

guidelines from NIST and CMS to introduce the concept of conducting a risk analysis within the context of a risk strategy.

COURSE OBJECTIVES

After completing this course, students will be able to

- Understand the legal requirements established in HIPAA protecting the disclosure of medical records and identify settings in which patient authorization is required and where it is not required.
- Understand the requirements for maintaining the security and confidentiality of protected health information based on HIPAA regulations and how to apply them in a health care setting.
- Explain the variety and intensity of cyberthreats facing health care computer networks and the vulnerabilities to cyber-attack that can exist,
- Identify the options available to firewall computer networks, employ cybersecurity measures and ensure proper authentication users to maintain security of the health IT infrastructure to avoid data breach.
- Recognize and explain federal and industry guidelines for information security.
- Conduct a management risk strategy assessment based on the NIST Risk Framework and certification programs for information security.
- Identify the requirements of IT security as laid out in the HIPAA Security Rule and be able to conduct a risk assessment in a health care setting.

MAJOR & CURRICULUM OBJECTIVES TARGETED

Learning Objectives: Upon completion of the course, the student should have an understanding of the vital importance of information security in Health IT, the legal requirements for maintaining confidentiality of protected health information and technical and administrative approaches to ensuring security of computer network systems in modern health care settings. This will include:

- Understanding HIPAA and state law regulations and requirements to control the disclosure of protected health information (PHI) to protect the confidentiality of medical records.
- Ensuring the security and confidentiality of electronic protected health information (ePHI) according to the regulatory requirements of the HIPAA Security Rule.
- Recognizing vulnerabilities of in health care computer networks to cyber-attacks and other event that threaten to breach the privacy protections of ePHI.
- Identifying and specifying the security approaches required to maintain security of the health IT infrastructure to avoid data breach.
- Understanding the information security guidelines established for private sector, public sector and health care information technology systems.
- Developing a risk framework strategy to address vulnerabilities of the computer network, training needs of the organization staff and ongoing assessment of risk in the health care facility.
- Familiarity with the IT security requirements in the HIPAA Security Rule and steps to conduct a risk assessment in a health care setting.

TEACHING METHODOLOGY

ISM 6326 Information Security and Compliance addresses information security of Electronic Protected Health Information in a health care setting and compliance with federal and state laws and regulations that pertain to maintaining the privacy of medical records.

The instructor's approach to the course will be to1) integrate regulatory, technical and standards-based lectures that cover information relevant information security with 2) in-class discussions and student-based

presentations that demonstrate mastery of terminology and concepts and 3) written papers that allow students to explore issues in ensuring the confidentiality of patient records and maintaining the security architecture of computer networks in a health care setting. Class lectures, presentations and discussions will include security regulations, information security standards and guidelines, technical advances in computer hardware and software that both threaten and protect medical records and approaches to assessing risk and its impact.

The instructor intends to split the class time among lectures, in-class discussion on course-relevant information and concepts and student presentations on assignments and research projects. Students are expected to come to class fully prepared to engage in class discussions, make assigned presentations and assist class members in understanding class content. The instructor's approach will be highly interactive and is intended to promote articulate dialogue on the implications information security in the health care system. The class will draw heavily upon the professional experiences of both the students and the instructor.

The instructor plans to invite several security professional as guest lecturers to the class.

ASSURANCE OF LEARNING

The College of Business cares about the quality of your education. More on the College's commitment to Assurance of Learning can be found at the following link:

http://businessonline.fiu.edu/course_addons/Learning_Commitment.pdf

POLICIES

Please review the policies page as it contains essential information regarding guidelines relevant to all courses at FIU and additional information on the standards for acceptable netiquette important for online courses.

TECHNICAL REQUIREMENTS/SKILLS

One of the greatest barriers to taking an online course is a lack of basic computer literacy. By computer literacy we mean being able to manage and organize computer files efficiently, and learning to use your computer's operating system and software quickly and easily. Keep in mind that this is not a computer literacy course; but students enrolled in online courses are expected to have moderate proficiency using a computer. Please go to the "What's Required" page to find out more information on this subject.

This course utilizes the following Blackboard tools as complements to the in-class discussions:

1. Discussion Forum
2. Content Tool
3. Email and Blackboard Messages

For detailed information about the technical requirements, please **click here**.

ACCESSIBILITY AND ACCOMODATION

For detailed information about the specific limitations with the technologies used in this course, please visit http://online.fiu.edu/app/webroot/html/blackboardlearn/mastertemplate/accessibility/.

For more information about Blackboard's Accessibility Commitment, please visit http://www.blackboard.com/Platforms/Learn/Resources/Accessibility.aspx.

For additional assistance please contact our http://drc.fiu.edu/.

COURSE PREREQUISITES

There are no course prerequisites for this course.

TEXTBOOK

The texts in this course will be collected from current, available documents related to the information security published by credible sources such as the *Office of the National Coordinator for Health IT (ONC)*, the *Centers for Medicare and Medicaid Services (CMS)*, the *National Institute for Standards and Technology and other.*

All course documents will be provided electronically to reduce the cost of purchasing an expensive textbook. A list of course documents for each week of instruction will be provided in Blackboard before the start of class and to each student on the day of class.

An example of the text resources provided to the class is given below:

Matthew Scholl, Kevin Stine, Joan Hash, Pauline Bowen, Arnold Johnson, Carla Dancy Smith, and Daniel I. Steinberg (2008) NIST Special Publication 800-66 Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

EXPECTATIONS OF THIS COURSE

This is a classroom course with the capability to use Blackboard for online discussion and instruction. Expectations for student performance online are the same as for the classroom days. The online discussion forums allow for an exchange of ideas between students and instructor based on a written dialogue on specific topics. The online Blackboard aspect of the course requires a degree of self-motivation, self-discipline, and technology skills that can make it somewhat more demanding than the in class meetings but rewarding at the same time.

Students are expected to:

- Review the how-to-get-started information located in the course content.
- Ensure that your computer is compatible with Blackboard.
- Interact online with instructor/s and peers.
- Log in to the course regularly over the course of the eight weeks.
- Respond to discussion boards, blogs and journal postings within the week.
- Respond to emails within a reasonable timeframe.
- Submit assignments by the corresponding deadline.

The instructor will:

- Log in to the course regularly.
- Respond to discussion boards, blogs and journal postings daily.
- Respond to emails within 48 hours.
- Grade assignments within two weeks of the assignment deadline.

COURSE COMMUNICATION

Communication in this course will take place via interpersonal contact, email and Blackboard messages.

Messages are a private and secure text-based communication that occurs within a Course and among Course members. Users must log on to Blackboard to send/receive/read messages. The Messages tool is located on the left side Course Menu (Blackboard user interface). It is recommended that students check their messages routinely to ensure up-to-date communication.

The Email feature is an external communication tool that allows users to send emails to users enrolled within the course including the instructor and other students. Emails are sent to the students' FIU email on record. The Email tool is located on the left side Course Menu (Blackboard user interface).

For more information on professional writing and technical communication visit this link: http://online.fiu.edu/app/webroot/html/blackboardlearn/resources/writing_resources/.

ASSIGNMENTS

The Instructor will provide clear guidelines for each assignment

There will be three types of assignments in this course: Individual in-class presentations, Group in-class presentations Research Papers. The online discussion forum will be used for class interaction between Saturday sessions.

- *In-class presentations will address information covered in each chapter of the class text book with additional outside research on health information technology applications. Presentations can be individual or group, as preferred.*
- *The online forums will be used to provide a forum for students to research the usability and functionality of the EHRs that they are working with.*
- *Specifications for papers will be distributed at least two weeks before the paper is due. All papers will be evaluated within two weeks of the due date.*

DISCUSSION FORUMS

Keep in mind that forum discussions are public, and care should be taken when determining what to post.

Instructor

Instructor will provide clear guidance on the expectations and requirements of assignments.

- Students will receive specifications for in-class presentations during the first day of class. Specifications will include expected breadth of topic, depth of content and grading criteria.
- Students will be evaluated on the extent and quality of their classroom discussions.
- Online discussion topics will be communicated one week ahead of the online discussion. Students will be evaluated on the number of entries they post in the discussion forum and on the quality of their posts. Minimum expectations are for three posts within the week.
- Specifications for research papers will be distributed two weeks before papers are due. Online discussion topics will be selected that feed into the research papers and give students a chance to discuss the research topic and gather background materials. Criteria for evaluating the papers will be included in the specification sheets.

WEEKLY SCHEDULE

All classes will be held at the FIU Brickell Campus

Class Date	Class Discussion	Presentation Content	Assignment
Week 1 Saturday, Aug 23, 2014	Introduction to issues in Cybersecurity - HIPAA Privacy Rule and State Privacy Laws	General introduction to cybersecurity, review of HIPAA Privacy Rule and authorization requirements for the disclosure of Protected Health Information (PHI) and overview of State laws that protect disclosure of "super-confidential" patient records.	N/A
Week 2 Saturday, Aug 30, 2014	HIPAA Security Rule and requirements for security compliance	Introduction to the HIPAA Security Rule and overview of US Government requirements for ensuring the confidentiality and security or Electronic PHI (ePHI).	Team Presentation #1
Week 3 Saturday, Sept 6, 2014	Health care IT networks – cyberthreats and vulnerabilities	Technical overview of health care IT, telecommunications and computer networks and discussion of potential vulnerabilities from human and technical perspectives and the external threat of cyber-attack and data breach.	Individual interactive discussions
Week 4 Saturday, Sept 13, 2014	Health care IT networks - cybersecurity provisions	Technical review of security measures that are available to protect health care IT, telecommunications and computer networks and ensure the confidentiality and security of health care data.	Individual interactive discussions Paper #1 Due
Week 5 Saturday, Sept 20, 2014	Guidelines for Health IT security – IT industry and government standards	Overview of federal and industry standards and guidelines for information security management as published by NIST and ISO/IEC and presented in FISMA.	Team Presentation #2
Week 6 Saturday, Sept 27, 2014	Creating the security culture – NIST Risk Framework	Overview of the NIST Risk Framework for developing organizational risk strategies, training techniques for developing security awareness and approaches to drafting a privacy and security policy and procedures manual.	Individual interactive discussions
Week 7 Saturday, Oct 4, 2014	Risk assessment and mitigation of risk in Health IT systems	Review of the role of the HIPAA Risk Assessment, comparison of risk assessment tools, how the risk analysis fits within the Risk Framework and methods for developing a risk mitigation plan.	Individual interactive discussions Paper #2 Due
Week 8 Saturday, Oct 11, 2014	Summarizing legal, technical and management approaches to information security	Review of the legal, regulatory, technical, standards and organizational issues that are part of an integrated information security strategy and projection of future security threats and requirements.	Team Presentation #3

GRADING

Assignments will be evaluated according to the weights given below:

	Number	Per Unit	Total	Cumulative
Research Papers	*2*	*25%*	*50%*	*50%*
In-Class Group Report	*3*	*10%*	*30%*	*80%*
In-Class Discussion Lead	*1*	*12%*	*12%*	*92%*
In-Class Individual Participation	*8*	*1%*	*8%*	*100%*
		Total	*100%*	*100%*

Grades will be assigned according to the percentage totals given below:

Letter Grade	Range
A	93% - 100%
A-	91% - 92%
B+	87% - 90%
B	84% - 86%
B-	81% - 83%
C+	77% - 80%
C	74% - 76%
C-	71% - 73%
D+	67% - 70%
D	64% - 66%
D-	61% - 63%
F	Less than 61%