**Graduate/Undergraduate Syllabus Template**

**[Course Number]**

**Critical Issues in Cybersecurity and Medicine**

|  |  |
| --- | --- |
|  |  |

[University]

[Semester]

[Instructor]

[Email]

[Office]

[Office Hours]

**Course Description**

This five-week, modular course is designed to provide students in a variety of disciplines with knowledge on the technological, ethical, legal, and social issues associated with implantable medical devices. The division of the five weeks into discreet sub-units allows portions of these courses to be individually adopted in a variety of courses. The course is designed to create a pipeline of cognizant and prepared professionals to address the present and future challenges of this proliferating technology. The courses will feature two weeks dedicated to uncovering the technology behind implantable devices, including an overview of the medical uses and potential existing security vulnerabilities. The remaining weeks will be dedicated to examining the ethical, legal, and social implications of the associated security and privacy risks.

**Learning Outcomes**

Course level outcomes:

1. Demonstrate basic knowledge of the technology underlying networked medical devices.
2. Be aware of the security and privacy implications of these devices.
3. Understand the various attack motives and tactics to compromise security and privacy.
4. Understand the ethical, legal, and social implications of security and privacy risks.
5. Be able to design security-conscious and appropriate policies governing these devices.

Course learning outcomes will be measured in several ways:

1. Weekly exercises and activities designed to allow students to demonstrate and deepen understanding of the topics.
2. Input in interactive learning prompts embedded within course materials, such as surveys and writing, to monitor student learning and ensure students engage with all relevant materials.
3. Participation in (online) discussions that are based on assigned readings and encourage active reflection on and application of the materials.

**Required Course Readings**

All required and recommended readings are listed in the schedule section of this syllabus under the relevant topic.

**Assignments and Assessments**

**Weekly Exercises and Assignments**

[include specific expectations, grading rubrics, due dates, late policies, and other details]

**Embedded Interactive Learning Prompts**

Weekly course materials will be embedded with interactive activities such as questions which require responses with independent research, surveys, and quizzes. This will ensure students are: (1) actively understanding of the materials presented, (2) informed and engaged enough to give critical feedback, and (3) able to find and present relevant published research.

[include specific expectations, grading rubrics, due dates, late policies, and other details]

**Discussion Contributions**

[include specific expectations, grading rubrics, due dates, late policies, and other details]

**Grades:** All grades and comments will be posted [insert platform]. The breakdown of the course grade is as follows:

Weekly exercises and assignments: [insert %]  
Embedded Interactive Learning Prompts:  [insert %]  
Discussion Contributions:  [insert %]

**Grading Thresholds (in percentages):**

            97+      A         77-79   C+  
            94-96   A         74-76   C  
            90-93   A-        70-73   C-  
            87-89   B+       69 and below  F  
            84-86   B           
            80-83   B-       

**Course policies**

**Grade Disputes**

Only legitimate reasons will be considered for any grade adjustments, such as calculation mistakes.  Being close to a higher grade or the need to pass the class, for example, is not considered a valid reason.  If you are struggling in the course, please see the instructor for help and do so as early as possible. Realizing that you are heading towards a bad grade during the last week of the semester will likely not change the outcome. Please note that no individual extra credit will be given to “fix” bad grades! You have plenty of opportunities to make up for one bad assignment grade in this course.

**Make-up, Extra-Credit, and Late Assignment Policies**

Only in rare instances where you missed class due to documented illnesses, documented immediate family emergencies, or for athletic or other university approved absences will you be given the opportunity to make-up missed exercises and assignments.

The course provides frequent assessments of your progress. Maintaining a good grade is fairly easy provided that you fulfill the minimum requirements (assignments, reading assigned texts).

Barring extraordinary circumstances, all assignments must be turned in or taken on the scheduled date. Late assignments will automatically be downgraded one letter grade for each day they are late. If you cannot turn in an assignment or take an exam on the assigned date, please let me know as soon as possible. You may turn in the assignment before the scheduled day. Late assignments or make-up exams will only be given under extraordinary circumstances and only to students who have a legitimate excuse and provide official documentation explaining the absence. Emails without official documentation attached or phone messages do not constitute official documentation.

**General Class Behavior**

A classroom, whether online or offline, is meant to be an environment of mutual respect.  It is an open environment for sharing and discussing issues which are oftentimes sensitive in nature.  Disruptive behavior such as inappropriate language, personal attacks, and threats etc. is detrimental to the learning environment.  Should this type of behavior become an ongoing problem, you will be banned from discussion boards and this activity will adversely affect your grade.

**Grade Posts**

All scores and grades will be posted on [insert platform].

**Policies**

**Academic Misconduct**

[insert misconduct policy]

**Disabilities**

[insert disabilities policy]

**Instructor Information and Office Hours**

[insert: how to get in contact, email policy, etc.]

**Schedule of Topics and Assignments**

**([insert dates]) Week 1 Module 01: Introduction to “Smart” Medical Devices & Technical Issues Part 1**

Read Module 01

Read the following chapters:

[Security and Privacy for Implantable Medical Devices](https://spqr.eecs.umich.edu/papers/b1kohFINAL2.pdf) by Halperin et al. IEEE Pervasive Computing, Special Issue on Implantable Electronics 7(1), January 2008.

* Pp. 30: Article presents a general framework for evaluating the security and privacy of next-generation wireless IMDs
* Pp. 32: Helpful graphic for illustrating Web access of cardiac defibrillators

Pp. 35: Beginning discussion on classes of adversaries, tension between security vs. accessibility

Read the following articles:

Reel, M., & Robertson, J. (2015, November). *It’s way too easy to hack the hospital: Firewalls and medical devices are extremely vulnerable, and everyone’s pointing fingers.* Retrieved from <http://www.bloomberg.com/features/2015-hospital-hack/>

<http://losangeles.cbslocal.com/2016/02/17/la-hospital-paid-17k-ransom-to-hackers-of-its-computer-network/#.VsUaL_n4iMI.twitter>

* Malware attack (ransomeware, extortion)
* Hospital paid in Bitcoin
* FBI still investigating
* Hospital claims patient care and data not compromised

Article from *The Telegraph*, titled “Terrorists could hack pacemakers like in Homeland, say security experts,” retrieved from <http://www.telegraph.co.uk/news/science/science-news/11212777/Terrorists-could-hack-pacemakers-like-in-Homeland-say-security-experts.html>

Watch the following video:

[Cybersecurity expert interview with David Kennedy](https://www.youtube.com/watch?v=XXHn6LsBRWQ) – 3:52 min

View the following infographic:

Infographic: An Overview of the Internet of Things. Retrieved from <http://postscapes.com/what-exactly-is-the-internet-of-things-infographic>

Complete the following activities [insert activity and due date]

**([insert dates]) Week 2 Module 02: Technical Issues Part 2**

Read Module 02

Read the following articles:

Naone, E. (2009, November 10). *Keeping pacemakers safe from hackers.* Retrieved from <https://www.technologyreview.com/s/416214/keeping-pacemakers-safe-from-hackers/>

* Beginning pp. 1: Introduces scheme to protect IMD against wireless attacks: ultrasound waves (to be used in addition to radio signals)
* Pp. 3: Discussion of how medical devices need a microphone in order to detect the ultrasound
* Pp. 4: Prototype is now mature enough to begin development

Storm, D. (2015, June 8). *MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks.* Retrieved from <http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html>

* Introduces hospital lab blood gas analyzer attack (pp. 2)
* Includes 2 large graphics that might be useful illustrations
* Discusses malware-infected X-Ray systems (p. 5)
* Overall: Article provides an entry-level introduction to other types of attacks on different types of medical equipment

Independent Security Evaluators. (2016, February 23). *Securing hospitals: A research study and blueprint.* Retrieved from <https://securityevaluators.com/hospitalhack/securing_hospitals.pdf>

Watch the following video:

[Problems with a syringe pump](http://www.youtube.com/watch?v=brNbDWnHDVs&feature=player_embedded) (Harold Thimbleby's video) – 1:48 min

View the following presentation:

Ransford, B. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero power defenses. Presentation at 2008 IEEE Security & Privacy conference. Retrieved from: <http://www.halper.in/pubs/imdsecurity_slides_ransford_oakland08.pdf>

* Beginning Slide 11: Outlines different types of possible attacks on IMD
* Beginning Slide 24: Outlines defensive directions
* Slide 35: Non-technical challenges

Complete the following activities [insert activity and due date]

**([insert dates]) Week 3 Module 03: Legal & Regulatory Aspects**

Read Module 03

Read the following government report:

U.S. Food and Drug Administration. (2015, August 24). National medical device postmarket surveillance plan. Retrieved from <http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/ucm301912.htm> (site includes links to pdf downloads of several related FDA reports; TBD which reports are most valuable to download & post to course website)

Read the following news article:

Talbot, D. (2012, October 17). *Computer viruses are “rampant” on medical devices in hospitals.* Retrieved from <https://www.technologyreview.com/s/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/>

* Pp. 2: Discusses how malware slowed down fetal monitors used on women with high-risk pregnancies being treated in intensive-care wards
* Beginning pp. 3: Introduces botnets
* Pp. 14: Discusses how malware problems on hospital devices are rarely reported to state or federal regulators (partly because hospitals believe they have little recourse)
* Includes comments from FDA, hospital Chief Technology Officers, and officials

Read the following sites:

McGee, M. K. (2012, September 14). *Monitoring medical devices: An update.* Retrieved from <http://www.healthcareinfosecurity.com/monitoring-medical-devices-update-a-5109>

* Pp. 1: Introduces FDA’s 2012 report, “Strengthening Our National System for Medical Device Post-Market Surveillance”
* Beginning pp. 1: Criticism of FDA from UMass-Amherst, Harvard Medical School, and Beth Israel Deaconess Medical Center
* Pp. 2: Dale Nordenberg advocates for a unique ID for all medical devices but Rick Hampton doesn’t think that will help much
* Pp. 3: Discusses FDA’s current Sentinel System

Olson, M. (2012, September 24). *Medical device security: A call to action.* Retrieved from <http://www.healthcareinfosecurity.com/blogs/medical-device-security-call-to-action-p-1360/op-1>

* Pp. 2: Introduces medical care devices classes I, II, and III and FDA 501K certification
* Opinion piece addresses FDA shortcomings and what should be done to remedy unnecessary risks (a call to action written by the Chief Information Security Officer at Beth Israel Deaconess)

Complete the following activities [insert activity and due date]

**([insert dates]) Week 4 Module 04: Ethical Aspects**

Read Module 04

Read the following chapters:

"Wounds That Don't Heal: Nurses' Experience with Medication Errors" Chapter 9 by Linda A. Treiber and Jackie H. Jones from *First Do Less Harm* by editors Ross Koppel and Suzanne Gordon, Cornell University Press, 2012. (pp. 180-195)

"The Economics of Cybersecurity" Chapter 9 from *Security in Computing* by Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice-Hall, 2007. (pp. 571-602)

"The Food and Drug Administration" Chapter 3 from *Reliable Design of Medical Devices* by Richard Fries, CRC Press, 2006. (pp. 25-51)

Complete the following activities [insert activity and due date]

**([insert dates]) Week 5 Module 05: Policy Implications & Future Directions**

Read Module 05

Read the following chapter:

"Managing Safety and the Safety Culture" Chapter 13 from *Engineering a Safer World: Systems Thinking Applied to Safety* by Nancy G. Leveson, MIT Press, 2011. (pp. 415-443)

Read the following article:

[Optimal Policy for Software Vulnerability Disclosure](http://mansci.journal.informs.org/content/54/4/642.short) by Arora et al. In Journal of Management Science, 54(4), April 2008, pp. 642-656.

Read the following workshop publication:

Association for the Advancement of Medical Instrumentation. (2012). *Advancing Safety in Medical Technology: Healthcare technology in a wireless world.* Retrieved from <http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/Summits/2012_Wireless_Workshop_publication.pdf>

* Beginning pp. 6: Good overview of the explosion of wireless devices in healthcare
  + Quote: “I do not think that the wireless waves I have discovered will have any practical implication” – Heinrich Hertz, 19th century German physicist
  + List of wireless technology applications
* “Data Points” box on pp. 8
* Safety and Security issues: beginning pp. 12
* Box on pp. 18: Characteristics of a High-Reliability Infrastructure in a Healthcare Organization + Top Obstacles to Building a High-Reliability Infrastructure
* Pp. 23: Regulatory Perspective – Key Considerations for Wireless Medical Devices
  + Pp. 28-29: What Medical Device Manufactures & Hospitals Can Do

Complete the following activities [insert activity and due date]