School of Healthcare Business

Course Syllabus
HIN.740 – Health Data Security and Ethics
[semester] 202x

Faculty Information:
Name:
Phone:
MCPHS Email:
Office:
Office Hours:

Course Information:

HIN.740 – Health Data Security and Ethics - Credits: 3
This is an online course. Students may review each weekly lesson at a time convenient to their individual schedules within the week, but must remain current by completing each lesson and/or assignment within the timeframe indicated in this document.

Course Description:
This course focuses on privacy, security, and compliance issues associated with health care informatics as well as the moral and ethical concepts of information security. The course covers creation and storage of healthcare data, enterprise risk management, regulatory compliance measures pertaining to healthcare data, and confidentiality and privacy of patient data. Students are introduced to cybersecurity and threat actors and what organizations need to do in event of a data breach and the unauthorized disclosure of PHI. Importance is placed on understanding and demonstrating the relationship between technology, regulatory affairs, and organizational factors and their impact on healthcare data security and ethics.

Text/ Primary Course Materials:
Required Text:
1. Webster, M. (2021). *Do No Harm: Protecting Connected Medical Devices, Healthcare, and Data from Hackers and Adversarial Nation States*. John Wiley & Sons.
2. Curtis, E., & Drennan, J. (2013). *Quantitative health research: issues and methods: issues and methods*. McGraw-Hill Education (UK). [selected chapters provided on Blackboard, https://ebookcentral-proquest-com.ezproxymcp.flo.org/lib/mcphs/detail.action?docID=1336598]
3. Morrison, E. E. (2009). *Health care ethics: Critical issues for the 21st century*. Jones & Bartlett Learning. [selected chapters provided on Blackboard]
4. Supplemental articles and readings as assigned

Recommended Text:
1. American Psychological Association. (2019). *Publication manual of the American Psychological Association* (7th ed.). Washington, DC: American Psychological Association.

Other Resources:
1. Useful website for APA style guidelines from the [Purdue Online Writing Lab](#)

Course Objectives:
1. Explain the risks and benefits of having personal and enterprise medical devices interconnected on the internet,
2. Analyze the types and sources of medical and non-medical data that medical devices and healthcare information systems may generate,
3. Review organizational security plans and protocols and identify areas for improvement,
4. Differentiate between the various types of threat actors and vectors commonly used to target healthcare organizations,
5. Understand the Common Vulnerability Scoring System (CVSS) and its use and purpose in the cybersecurity field,
6. Apply the data governance lifecycle to existing organizational processes for improvement purposes,
7. Formulate data breach investigation plans using the incident response framework,
8. Apply the principle ethical theories to the storage and security of healthcare data,
9. Propose ethical arguments to organizational decisions before they are made,
10. Take part in ethical discussions pertaining to the creation, collection, use, and storage of healthcare data, and
11. Ethically evaluate the secondary use of research data for additional purposes unrelated to its original collection.

School of Healthcare Business

Assessment of Student Learning and Teaching Effectiveness:
This course will be offered online using Blackboard as the course learning management system. Narrated PowerPoint slides will be posted to Blackboard weekly to present each topic. Students will read the assigned *Readings* outlined in the course calendar for each topic prior to viewing the PowerPoint presentation for that topic. After reviewing the PowerPoint presentation(s), students will participate in associated discussion board activities to promote learning via reflection. A final research paper as well as various other assignments will be used to assess the course objectives.

Course Requirements:
1. **Course Assignments:**   xx%

2. **Data Breach Project:**   xx%

3. **Participation/Discussion Board:**   xx%
    ▪ Active learning is essential. Students will participate via *Blackboard* in all posted discussion topics. Participation is mandatory with a minimal requirement of 2 postings per week to the discussion board. Students are required to post twice each week, once by Thursday of the week stating their views and once, by Sunday of the week, with a thoughtful reflection commentary after reading the views of classmates.
    ▪ Weekly lessons and assigned readings will be the source of the discussion topics. Questions will be posed at the beginning of each week to initiate discussion
    ▪ Each discussion, unless otherwise stated, will be open for one (1) week with no contributions to the topic accepted thereafter. (This means postings must be completed by 12 midnight EST Sunday of each week; if both postings are not done, a grade of zero is assigned).
    ▪ The faculty member will not comment on each posting, but may comment to provide direction to the discussion as postings accumulate.
    ▪ "Chatter" in the discussion sessions should be avoided; responses to colleagues should advance the conversation and not simply provide praise.

Assignments and Grading

Citations - All assignments, papers, discussion boards, or otherwise will follow American Psychological Association (APA) style guidelines 7th edition. **There are no exceptions.** The APA Guidelines set forth the standards for writing style as well as recognition of sources, evidence, etc.

Plagiarism Software and Review - Students are expected to abide by the University Academic Honesty Policy as explained in the Student Handbook and University Catalog. Plagiarism is considered a violation of this policy. To deter plagiarism and ensure the appropriate use of resources, the University subscribes to verification services like Turnitin. Students must submit their written work via Blackboard where similarity checking is carried out and authenticity verified. **Note:** When the submission is complete, a confirmation email is automatically sent to your MCPHS email.

School of Healthcare Business

Assignment Due Dates

- All assignments must be submitted on the due date indicated.
- Submissions are required by 11:59 p.m. EST by default unless your instructor indicated an alternative date/time.
- Assignments are submitted via Blackboard (see the assignment for the specific method).

If you experience an illness or other excusable absence, contact your instructor immediately. Your instructor will provide guidance. **Please note**: to receive a Documented Absence it must be submitted within 5 days of the first absence ([see Documented Absence Policy](#)). Without proper documentation from the Dean of Students, or exception granted by your instructor, no exceptions will be made for late assignments.

Please note:

- If you have questions or concerns about an assignment, contact your instructor **prior** to the due date.
- You are encouraged to maintain copies of all assignments, projects, proposals, and discussion posts submitted for your own records. Courses may not be available to you after the semester concludes.
- After you submit your assignment, you are encouraged to double-check to make sure that it has been received/recorded.
- Writing assignments are submitted via Turnitin. When the submission is complete, a confirmation email is automatically sent to your MCPHS email.

Late Assignments

A late assignment is any assignment submitted after the stated due date without a documented absence granted by the Dean of Students Office, or confirmation of an exception granted by your instructor. Late assignments without documented absence, or granted exception will be graded according to the following scale:

- Submitted within 1 day / 24 hours – 20% penalty
- Submitted within 2 days / 48 hours – 35% penalty
- Submitted within 3 days / 72 hours – 50% penalty
- After 72 hours, assignments will not be accepted and marked as a 0

Assignment Grading

- Grades for the course assignments/requirements will be posted via the Blackboard Grade Center.

HIN.740 – Health Data Security and Ethics

- Any questions about grades should first be sent to your instructor in writing from your MCPHS email address.
- Any exception to the due dates or late submissions (see above) must be discussed with your instructor and confirmed in writing.

Academic Honesty and Plagiarism

The School of Healthcare Business faculty believes in honesty and integrity in all educational pursuits. We are steadfast in our commitment to academic integrity and the standards identified in the Student Handbook and University Catalog. All students are expected to abide by these policies. Students must uphold the highest standards of academic integrity, including presenting all work, writing assignments, discussion posts, etc., without any instance of plagiarism, intentional or otherwise. Plagiarism is defined as submitting another person's work as one's own without proper acknowledgment or using the words or ideas of others without crediting the source of those words or ideas. If an incident of plagiarism is identified it will be addressed as follows:

The First Incidence of Plagiarism/Academic Dishonesty - Students will be notified via their MCPHS email of the identified offense and required to discuss the situation with the instructor, program director, or Dean. To receive credit, a revised submission is required within seven (7) days, or no points will be awarded.

- A penalty of 20% will be applied to the revision.
- Any further plagiarism or academic dishonesty in the revised submission will constitute the second incidence of plagiarism (see below).
- Student Affairs will be notified of the first incident and the academic penalty that has been imposed. Please note - The DOS/Student Affairs may impose additional penalties.

The Second Incidence of Plagiarism/Academic Dishonesty Students will be notified via their MCPHS Email of the identified offense and required to discuss the situation with the instructor, program director, or Dean. To receive credit, a revised submission is required within seven (7) days, or no points will be awarded.

- A penalty of 40% will be applied to the revision.
- Any further plagiarism or academic dishonesty in the revised submission will constitute the third incidence of plagiarism (see below).
- Student Affairs will be notified of the second incident and the academic penalty that has been imposed. Please note - The DOS/Student Affairs may impose additional penalties.

The Third Incidence of Plagiarism/Academic Dishonesty - Students will be notified via their MCPHS Email of the identified offense and required to discuss the situation with the instructor, program director, or the Dean.

HIN.740 – Health Data Security and Ethics

School of Healthcare Business

- No revisions are accepted.
- The assignment will be automatically graded with a 0 (zero).
- Students may be required to repeat the course (see grading section)
- The DOS/Student Affairs will be notified of the incident and the academic penalty that has been imposed. Please note – The DOS/Student Affairs may impose additional penalties.

Please note:

- Each incidence of plagiarism or academic dishonesty, is <u>cumulative</u> while enrolled as a student in the School of Healthcare Business.
- All incidences of plagiarism or academic dishonesty, either intentional or unintentional, will be reported to the DOS/Student Affairs as outlined above.
- University level consequences related to plagiarism may be applied to each incidence as determined by the DOS/Student Affairs.
- After three incidences the DOS/Student Affairs will be notified by the Dean with a recommendation for dismissal.

Grading

Grades for the course assignments/requirements listed above will be posted via the Blackboard Grade Center. Students are strongly encouraged to maintain copies all assignments, projects, proposals, and discussion posts submitted for your own records and so your work can be resubmitted if there is a posting or transmission error.

Grading Scale

Please note that the graduate grade scheme does not include the grades that are Bolded. Students receiving below a passing grade in graduate level courses will be graded with an F, regardless of the letter grade. Check the grading policies for your program in the University Catalog.

Students enrolled in the DHA and DScPAS programs must pass the course with a minimal grade of 83%/B
Students in the MBA and MSCM programs must pass the course with a minimal grade of 80%/B-

A	100-93	*C+*	*79-78*
A-	92-90	*C*	*77-73*
B+	89-88	*C-*	*72-70*
B	87-83	**D**	**69-60**
B-	*82-80*	**F**	**<60**

Course Policies

Any issues arising from the syllabus or course requirements should be addressed to the course faculty immediately. If changes to the syllabus are required the faculty member will notify students of the changes.

Reuse of Your Own Work: Self-Plagiarism
Plagiarism also includes submitting the same work for assignments in more than one class (copying from oneself) without permission from the instructor and without appropriate citation, the same or subsequent semesters. If you are retaking a course, you must seek approval from your current course instructor about the reuse of materials previously submitted for class assignments and discussions. Your instructor reserves the right to deny this request. If you have previously submitted an assignment via Turnitin/SafeAssign and you submit the same work for another course or a retake, it will be highlighted on the similarity report as possible plagiarism.

Documented Absence Process
To be permitted to make up missed coursework MCPHS students must seek a documented absence from the Dean of Students office. In all cases, it is the student's responsibility to notify the Dean of Students. In the case of an absence (anticipated or urgent), every effort must be made to notify course faculty AND the Dean of Students office. Email notification is preferred.

Regardless of the reason for absence, a student must notify the Dean of Students office and their course faculty or preceptor of the absence. **Students must also complete the online form and upload supporting documentation within five (5) business days from the first date of absence to the Dean of Students office**. A documented absence does not always excuse a student from missing academic work. Students are expected to abide by the course syllabus and academic program's policy related to class absences. Reasons of work conflict, travel, and poor time management are not eligible for documented absence, and acceptance of late work is solely at the instructor's discretion. Permitted absences do not exclude the enforcement of the late submission policy with potential point deductions.

Email Statement
All MCPHS students are required to open, utilize, and maintain the MCPHS email account they are assigned within limits set by Information Services. Official college communications and notices, including communications for this course are ONLY delivered to MCPHS email accounts. All students are responsible for regularly checking their MCPHS email and for information contained therein.

Guidelines for Faculty Email Communications and Questions
You are strongly encouraged to use the Q&A section of the course to post course/assignment-specific questions as peers may either have the answer or benefit from the responses. When you need to contact the faculty by email, they will respond to email messages in a timely manner, generally within 24 hours. Note that weekends and other University holidays affect the timing of email responses from faculty. Students are expected to treat faculty, peers and group members with the same respect that they expect and deserve.

Office of Student Access and Accommodations (OSAA)
A student's right to equal education is protected under the Americans with Disabilities Act and Section 504 of the Rehabilitation Act. All students must abide by the Academic Policies and Procedures set forth

in the MCPHS Academic Catalog. Questions regarding accommodations can be directed to the Office of Student Access and Accommodations.

Under the ADA/Section 504, students with documented disabilities/conditions, that impact their access to education, and wish to request reasonable accommodations can contact the Office of Student Access and Accommodations (OSAA). To initiate services, students can complete the Student Request for Services Form: https://mcphs-accommodate.symplicity.com/public_accommodation/

OSAA can be contacted via email at OSAA@mcphs.edu or via phone at 617-879-5995.

Center for Academic Success & Enrichment (CASE) - WOR/MAN/Graduate/Online Programs
The Center for Academic Success and Enrichment (CASE) supports students through providing a number of academic support services introducing them to the strategies that will enhance performance in their academic programs and ultimately contribute to their professional lives.

The CASE staff are available to meet with students on an appointment basis Monday – Friday 9:00 a.m. to 4:00 p.m. EST. To schedule an appointment with a CASE staff member, visit the following link: mywconline.com/casewm and select your schedule and program to bring you to the correct availability.

Questions related to CASE services can be directed to case.wm@mcphs.edu.

University Learning Network (ULN)
The ULN is intended to support students to meet the challenges of our health science based programs with our resources consisting of: Enrichment/Professional Tutoring, English Language Resource Center, Writing Center, and TutorMe.

Students can utilize the ULN's appointment-based services (Enrichment/Professional Tutoring, English Language Resource Center, & Writing Center) by visiting www.mywco.com/uln. TutorMe can be accessed through the Tools section of the course's Blackboard page.

Questions related to University Learning Network services can be directed to ULN@mcphs.edu.

Course Outline

HIN.740 – Health Data Security and Ethics

Unit 1	Unit 1 Dates:	**Unit 1 Title:** Course Introduction **Unit 1 Learning Objectives:** - Introduce HIN.740, and - Establish course objectives and outcomes.	**Unit 1 Reading/Viewing:** 1. Course introduction lecture
Unit 2	Unit 2 Dates:	**Unit 2 Title:** The Internet of Medical Things (IoMT) **Unit 2 Learning Objectives:** - Discuss the risks and benefits of having medical devices connected to the internet, - Explain the differences in the various types of attacks against internet connected medical devices, - Identify the risks associated specifically with telehealth and other remote patient monitoring technologies, - Discuss the historical challenges presented by the use of internet connected medical devices and how they were overcome, and lastly - Differentiate the levels of interconnectivity between internet connected medical devices.	**Unit 2 Reading/Viewing:** 1. Webster, Ch 1, 2
Unit 3	Unit 3 Dates:	**Unit 3 Title:** Creation, Application, and Storage of Healthcare Data **Unit 3 Learning Objectives:** - Define the term "medical data," - Understand the different internal and external sources of medical data, - Describe the Five "V's" of data, and lastly - Compare and contrast HIPAA medical data and non-HIPAA medical data.	**Unit 3 Reading/Viewing:** 1. Webster, Ch 3 2. Shilo, S., Rossman, H., & Segal, E. (2020). Axes of a revolution: challenges and promises of big data in healthcare. *Nature medicine*, *26*(1), 29-38.

School of Healthcare Business

Unit 4	Unit 4 Dates:	**Unit 4 Title:** Legal and Regulatory Affairs pertaining to Health Data **Unit 4 Learning Objectives:** • Understand the various key pieces of legislation that regulate and protect healthcare data, • Discuss the enforcement mechanisms in place related to data breaches used by the Office of Civil Rights and at an organizational level, • Explain the challenges in enforcing said mechanisms with a changing threat landscape, and lastly • Propose suggestions to strengthen an organization's existing enforcement and protection mechanisms.	**Unit 4 Reading/Viewing:** 1. Webster, Chs 4, 6, 7
Unit 5	Unit 5 Dates:	**Unit 5 Title:** Threat Actors and Cybersecurity **Unit 5 Learning Objectives:** • Understand and explain the "anatomy" of a data security breach, • Differentiate between **phishing & pharming**, and **vishing & smishing**, and illustrate how these attack vectors are used, • Discuss the differences between black-hat and white-hat hacking, • Compare and contrast the roles of different types of threat actor roles, and lastly • Explain the key disciplines of cybersecurity.	**Unit 5 Reading/Viewing:** 1. Webster, Chs 5, 8, 9 2. Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. DIGITAL HEALTH. https://doi.org/10.1177/20552076221081716

Unit 6	Unit 6 Dates:	Unit 6 Title: The Internet and Network Infrastructure **Unit 6 Learning Objectives:** • Understand how local area and wide area networks are constructed and how they work, • Interpret different types of network architectures and designs, • Discuss the different types of internet services and how they are utilized by both consumers and enterprise organizations, • Translate how different network architectures and security measures can be used to protect internet connected medical devices, and lastly • Explain the relationship between internet connected medical devices and the internet services they use and consume.	Unit 6 Reading/Viewing: 1. Webster, Chs 10, 11 2. Khera, M. (2017). Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications. Journal of Diabetes Science and Technology, 11(2), 207–212. https://doi.org/10.1177/1932296816677576
Unit 7	Unit 7 Dates:	Unit 7 Title: Threat, Vulnerabilities, and IT Hygiene **Unit 7 Learning Objectives:** • Identify the most commonly overlooked areas of IT and cybersecurity hygiene, • Understand what comprises a strong enterprise change management strategy, • Describe the structure of the Common Vulnerability Scoring System (CVSS) and its importance related to vulnerability management, • Discuss the phases of a planned penetration test and the different test execution strategies, and lastly • Explain the importance of the MITRE ATT&CK framework and how it is used in an enterprise.	Unit 7 Reading/Viewing: 1. Webster, Chs 12, 14

Unit 8	Unit 8 Dates:	**Unit 8 Title:** Data Protection and Access Management **Unit 8 Learning Objectives:** - Compare the different "minimal identity practices" and identify their key importance, - Describe the process of Authentication, Authorization, and Accounting (AAA), - Explore each step of the data governance lifecycle, - Understand enterprise encryption practices and how each applies to an organization's data strategy, and lastly - Explain the relationship between Identity and Access Management (IAM) and Data Loss Prevention (DLP).	**Unit 8 Reading/Viewing:** 1. Webster, Chs 13, 15
Unit 9	Unit 9 Dates:	**Unit 9 Title:** Breaches happen, now what? **Unit 9 Learning Objectives:** - Understand how data breaches are investigated, - Identify the major sources of investigative information, - Explain the key components of the incident response framework, and lastly - Describe the field of data forensics and it's importance to a breach investigation.	**Unit 9 Reading/Viewing:** 1. Webster, Ch 16

Unit 10	Unit 10 Dates:	Unit 10 Title: Organizational Risk Management **Unit 10 Learning Objectives:** • Understand the different levels of an organizational structure and their relationship to data security, • Describe the different risk frameworks that organizations use in risk management, • Compare and contrast Qualitative vs. Quantitative Risk management, • Explore the different sources of risk that exist internal and external to an organization, and lastly • Design the framework of an enterprise risk management plan.	Unit 10 Reading/Viewing: 1. Webster, Ch 17
Unit 11	Unit 11 Dates:	Unit 11 Title: The Future of Data Security **Unit 11 Learning Objectives:** • Understand how the development of technology and innovation drives new security threats, • Describe the responsibilities of data "manufacturers" and how new regulations drive their innovation practices, • Explain how an organization's governance structure helps and hinders their own technology innovations, and lastly • Identify the importance of "Security Assurances" and how they strengthen an organizations security posture.	Unit 11 Reading/Viewing: 1. Webster, Chs 18, 19, 20

Unit 12	Unit 12 Dates:	Unit 12 Title: The Theory and Principles of Healthcare Ethics **Unit 12 Learning Objectives:** • Describe the different normative ethical theories, • Explain how each of the ethical theories applies to the practice and delivery of healthcare, • Compare the most commonly used ethical principles and their relationship to healthcare, and lastly • Understand the importance of ethics in a decision-making model.	**Unit 12 Reading/Viewing:** 1. Morrison, Chs 1, 2
Unit 13	Unit 13 Dates:	Unit 13 Title: Ethics and Information Technology Management **Unit 13 Learning Objectives:** • Describe the function and roles of an Ethics Committee and its importance to an organization, • Distinguish the different members of an Ethics Committee and the specific role they serve, • Discuss various ethical dilemmas pertaining to data management and healthcare information systems, • Understand the ethical definition and importance of informed consent, and lastly • Define the ethical concerns related to the technical innovation process.	**Unit 13 Reading/Viewing:** 1. Morrison, Chs 6, 7, 8

| Unit 14 | Unit 14 Dates: | Unit 14 Title:
The Ethics of Big Data and Healthcare Research

Unit 14 Learning Objectives:
• Describe the five primary areas of concern in the area of big data ethics,
• Understand the role of an Institutional Review Board (IRB) in healthcare research,
• Explore the creation and application of the "Ethics Framework for Big Data in Health and Research,"
• Discuss the relationship between informed consent and electronic clinical data, and lastly
• Analyze ethical scenarios pertaining to the use of secondary research data. | Unit 14 Reading/Viewing:
1. Curtis, Ch 19 |
| Unit 15 | Unit 15 Dates: | **Final Exam Week** | |

Course Assignments/Rubrics
All course assignments and rubrics will be made available through the course's Blackboard course site.

Students must abide by the Academic Policies and Procedures set forth in the MCPHS University Catalog and Student Handbook. *Important information regarding Description of Credit Hour Policy, Excused Absence Approval, Disability Support Services for students, Academic Honesty and Plagiarism and other academic policies is set forth in the Academic Policies and Procedures section of the MCPHS Catalog.*

MCPHS University Course Catalog
> **https://www.mcphs.edu/academics/university-course-catalog**

MCPHS University Student Handbook
> **https://my.mcphs.edu/departments/student-affairs**

Students must read, understand, and comply with all of these policies and procedures.