



Department of Health Administration and Policy

College of Public Health

Spring 2026

Syllabus Revised 10 January 2026	
Course information	HAP 462: Privacy and Security in Health Informatics Date/time: Online Location: Online
Course placement	<input checked="" type="checkbox"/> Core <input type="checkbox"/> Concentration <input type="checkbox"/> Elective <input type="checkbox"/> Pre-requisite(s) <i>() Course(s) recommended before taking this course:</i>
Instructor	Prof. Phillip C. Zane, JD 4400 Peterson Hall Contact Info: pzane@gmu.edu Office Hours: Wednesdays, 1:30 to 3:30 and by appointment
Course description	Health information security and privacy issues in the current healthcare system. Evaluates methods to achieve privacy & security. Discuss the important role of sound security policies and procedures; Looks into technical solutions and non-technical solutions for achieving privacy & security.
Course objectives	<p>Upon completion of the course the student will be able to:</p> <ol style="list-style-type: none"> 1. Explain the importance of security policies for technology use (<i>Knows how</i>). 2. Demonstrate knowledge of major security threats in healthcare (<i>Knows how</i>). 3. Describe the importance of privacy in healthcare (<i>Knows how</i>). 4. Draft policies for responding to security incidents and malfunctions (<i>Knows how</i>). 5. Demonstrate awareness of legal requirements for patient privacy and security (<i>Knows</i>). 6. Analyze impact of security operations on healthcare organizations (<i>Knows</i>). 7. Evaluate the costs and benefits of increased privacy and security (<i>Knows</i>). 8. Identify the security problems generated from telecommuting, out-sourcing, and the internet of things (<i>Knows how</i>). 9. Identify the role that social engineering plays in the security of information systems (<i>Knows</i>). 10. Propose revisions to privacy and security policies and regulations to reflect technical developments and recent research in behavioral science (<i>Knows</i>).

Required materials	<p>REQUIRED</p> <p>1. Brzezinski, R. (2018). <i>HIPAA Guidelines: Rules, Laws, Risks, Enforcements, Privacy, Security and Notification Requirements & Compliance in Practice</i>. ISBN-13: 978-1423238713; ISBN-10: 1423238710. This is a six-page, laminated reference guide available for about \$10. You may use it on the exams.</p> <p>2. Krager, D. and Krager, C. (2018). <i>HIPAA for Healthcare Professionals</i>. 2nd edition. Cengage.</p> <p>3. Ciampa, M. (2024). <i>Security Awareness: Applying Practical Cybersecurity in Your World</i>. 6th edition. Cengage.</p>																								
Course requirements	Participate in the various components of the Group Project; participate in the online discussions; participate in the experiments and simulations; participate in the other interactive activities of this course; complete the final exam and the midterm.																								
Teaching methods	<input checked="" type="checkbox"/> Lecture <input checked="" type="checkbox"/> Group work <input type="checkbox"/> Independent research <input type="checkbox"/> Field work <input checked="" type="checkbox"/> Papers <input type="checkbox"/> Guest speakers <input checked="" type="checkbox"/> Student presentations <input checked="" type="checkbox"/> Case Studies <input checked="" type="checkbox"/> Lab (virtual) <input checked="" type="checkbox"/> Class discussion <input type="checkbox"/> Other _____																								
Evaluation	Group Project (Analyzing a Privacy Breach): 20% Lucid Spark Introduction: 5% Experiments & Simulations: 15% Amending Rules: 15% Discussion Posts: 10% Midterm: 15% Final: 20%																								
Grading Scale	<p>Letter Grades will be awarded according to the following schedule:</p> <table border="0" style="margin-left: 40px;"> <tr><td>Grade</td><td>Percent</td></tr> <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> <tr><td>D</td><td>60-69</td></tr> <tr><td>F</td><td>0-59</td></tr> </table> <p>Plagiarism means an automatic F. Please familiarize yourself with the GMU policy on plagiarism and proper citation of materials. <i>This also applies to your contributions to the Discussion Boards.</i></p>	Grade	Percent	A+	98-100	A	93-97	A-	90-92	B+	87-89	B	83-86	B-	80-82	C+	77-79	C	73-76	C-	70-72	D	60-69	F	0-59
Grade	Percent																								
A+	98-100																								
A	93-97																								
A-	90-92																								
B+	87-89																								
B	83-86																								
B-	80-82																								
C+	77-79																								
C	73-76																								
C-	70-72																								
D	60-69																								
F	0-59																								

Common Policies Affecting All Courses at George Mason University	https://stearnscenter.gmu.edu/home/gmu-common-course-policies/
E-mail Policy	Check your email at least twice each day. This course relies on email to communicate important reminders, scheduling changes, and other information essential to your success.
Writing Center	Take advantage of the Writing Center as you work on written assignments in this course. You can book free 45- minute appointments with tutors who will work with you on any phase of a writing project. They can provide feedback on a draft, answer your questions, and show you strategies for brainstorming, organizing, drafting, revising, and editing. To schedule an appointment, visit the center's main location in Robinson Hall B 213 or go to writingcenter.gmu.edu , register with the center, and make an appointment using the online scheduler.

SCHEDULE OF CLASSES AND ASSIGNMENTS

January 20	Module 1—Introduction: Healthcare IT Environment, Privacy and Security Framework
	<ul style="list-style-type: none"> - Participate in Experiment 1: The Ultimatum Game - Read Krager & Krager, Chapter 1, pages 1 to 25. - <i>Participate in the LucidSpark introduction exercise</i>
January 26	Module 2—Introduction to the Privacy Rule
	<ul style="list-style-type: none"> - Read Krager & Krager, Chapter 2, pages 27 to 51 - LucidSpark Bleeping Computer activity
February 2	Module 3—Transactions & Code Sets
	<ul style="list-style-type: none"> - Read Krager & Krager, Chapter 3, pages 53 to 74 <ul style="list-style-type: none"> o Privacy Rule (main post due by Sunday at 10:00 pm; two responses due by Tuesday at 10:00 pm) - Group Project: Select Preferred Role by the end of this week
February 9	Module 4—The HIPAA Security Rule
	<ul style="list-style-type: none"> - Read Krager & Krager, Chapter 4, pages 75 to 97 - Discuss privacy assignment <ul style="list-style-type: none"> o <i>Security Rule 1</i>

February 16	Module 5—Unique Health Identifiers and HIPAA Myths
	<ul style="list-style-type: none"> - Read Krager & Krager, Chapter 5, pages 99 to 116 <ul style="list-style-type: none"> o <i>Security Rule 2</i> - <i>Group Project: Respond to your group-mates on Lucidspark</i>
February 23	Module 6—Introduction to Cybersecurity
	<ul style="list-style-type: none"> - Read Ciampa, Module 1, pages 1 to 19 - Privacy Policy Project feedback - <i>Discussion Board due by next week (to be announced)</i> - Group Project: Case Researcher shares findings with group
March 2	Module 7—Personal Cybersecurity
	<ul style="list-style-type: none"> - Read Ciampa, Module 2, pages 27 to 47 - Group Project: Policy analyst shares findings with group - Review for Midterm & Proposed Amendment to Privacy or Security Rule
March 9-15	Spring Break
March 16	Module 8—Computer Security
	<ul style="list-style-type: none"> - Read Ciampa, Module 3, pages 55 to 78 - Group Project: Data Analyst shares findings with group - Midterm due March 2 at 11:59 pm. - <i>Discussion Board: Malware</i>
Mar 23	Module 9—Internet Security
	<ul style="list-style-type: none"> - Read Ciampa, Module 4, pages 87 to 107 - <u>Group Project: Presenter shares draft with group.</u> - Ransomware Simulation: The Trust Game (<i>Harmonize Discussion Board</i>)
March 30	Module 10—Mobile Security
	<ul style="list-style-type: none"> - Read Ciampa, Module 5, pages 115 to 136 - Group Project: Presenter submits presentation. - <i>Harmonize Discussion Board due by next week (Mobile Security)</i>
April 6	Module 11—Privacy, Theft & Encryption
	<ul style="list-style-type: none"> - Read Ciampa, Module 5, pages 145 to 167 - Group project: self-evaluation - <i>Encryption Exercise</i>
April 13	Module 12— Incident Response and Disaster Management
	<ul style="list-style-type: none"> - Simulation: Encryption Game & Bitcoin Mining Game - Group Project: Respond to hypothetical question and respond to questions about the group project - <i>Discussion Board due by next week (Disaster Management)</i>
April 20	Module 13— A Virtual Field Trip to the Dark Web
	<ul style="list-style-type: none"> - <i>The Dark Web, Cryptocurrencies, and National Security</i>

	- Harmonize Discussion Exercise (due April 26) on the Dark Web
April 27	Module 14—HIPAA Compliance, Future Trends in Healthcare and Health IT
	<ul style="list-style-type: none"> - Lecture on Further Rulings Influencing HIPAA, Future Trends - Read Chapter 6 - Discussion Board due by next week (Post Data Analysis PPT and comment on other students' work)
May 4	FINAL EXAM: ONLINE

Syllabus is subject to change as events require, such as promulgation or proposals of new rules, or significant breaches of privacy and/or security. Additional details about assignments, readings, and links will be posted on Canvas Please make sure you check it often. Don't neglect the reading! This class does not have formal lectures.