

HIPAA Privacy & Security (and Other Health Privacy Laws)
Syllabus

Summer Term 2016
Mitchell Hamline School of Law

General Course Information

Course: HIPAA Privacy
Credits: 2
Delivery Method: Distance Learning via Blackboard
Days/Times: June 1 - 29, 2016

Faculty Lead: Barbara Colombo
Affiliation: Mitchell Hamline School of Law, Director, Health Care Compliance Program, Assistant Professor of Law
Email: barbara.colombo@mitchellhamline.edu
Office Phone: 651-290-6316

Faculty Co-Lead: Sheri Beck
Affiliation: Prime Therapeutics, Privacy Officer and Senior Director, Corporate Compliance; Adjunct Professor, Mitchell Hamline School of Law
Email: sbeck45@msn.com

Course Description and Objectives

The focus of this course is the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the foundation for federal protections of health care information. Additionally, the course will examine preemption and the interplay between HIPAA and other federal and state health privacy laws, and the application and enforcement of those laws as they relate to privacy and security in the health care setting.

The objectives of this course include learning how to: (i) identify situations that implicate HIPAA; (ii) understand which provisions of the privacy and security law and rules apply to given situations and how to apply those provisions; and (iii) understand the significance of sound security measures in an era of increasing electronic crimes. Given the breadth of the subject matter and the short time allotted, students will not be expected to understand the full depth and complexity of applicable laws and rules; they will, however, be expected to understand key definitions and basic concepts under HIPAA and to analyze the interplay between HIPAA and other privacy laws, including basic preemption.

Course Materials

HIPAA Compliance Handbook 2016, by Patricia I. Carter, is the required textbook for this course. The book is written with the compliance/legal practitioner in mind. It includes a practical overview of the law with footnotes citing relevant statutes, regulations, and regulatory agency guidance.

In addition to the textbook, this Syllabus includes other required or relevant reading materials, such as: (i) primary sources (statutes and regulations); (ii) secondary sources (such as regulatory commentary); and (iii) a small number of select business forms and policies that showcase “HIPAA in action.” (Please note that Minnesota statutory law is cited a number of times throughout the syllabus for demonstrative purposes. Professors Colombo and Beck encourage students to review relevant law from their home states.)

Barbara Colombo – Faculty Lead

Barbara Colombo is the Director of the Health Care Compliance Certification Program and an Assistant Professor of Law at Mitchell Hamline School of Law (MHSL). Her responsibilities include the ongoing management and strategic growth and development of the Health Care Compliance Certificate Program. She launched MHSL'S distance learning (online) Health Care Compliance Certificate Program in 2012 and serves as the faculty lead for both the JD and online programs. More biographical information about Professor Colombo can be found on Blackboard.

In an effort to provide a meaningful and highly relevant program with practical insight, Professor Colombo has asked a number of industry professionals to present in addition to herself and Professor Beck (see below). You will learn from attorneys and privacy officers working in the privacy and security fields. Background and contact information related to each presenter will be posted on Blackboard.

Sheri Beck – Faculty Co-Lead

Sheri Beck is an adjunct professor of law with MHSL. Additionally, she currently serves as Privacy Officer and Senior Director, Corporate Compliance at Prime Therapeutics. In this role, Professor Beck is responsible for Privacy, including Incident Response, as well as oversight of the Corporate Compliance Function. This includes Code of Conduct, Conflict of Interest, Training, Governance and Business Continuity Management. More biographical information about Professor Beck can be found on Blackboard.

Course Evaluation and Grading

1. **Final Exam.** There will be a take-home, open-book final exam. **The exam will account for 65% of a student’s final grade.** The final exam will be administered via Blackboard. Students select a 72-hour window of time to complete the exam during the exam period which will run from Friday, July 1 through Friday, July 15, 2016. Additional information to follow.

- 2. Quizzes & Discussion Board Posts.** One discussion board post (original and responsive) will account for 25% of a student's final grade. Evaluation criteria for the discussion board posts are outlined below. Two quizzes will account for 10% of the student's final grade (each quiz accounting for 5%). Quiz #1 will focus on sessions 1, 2 and 4. Quiz #2 will focus on sessions 5 and 7.

Method of Instruction and Work Expectations

This course will be taught in 10 online sessions. Each session will include a recorded lecture with supportive PowerPoints. The course will open on Wednesday, June 1, 2016 at 8:00 am CDT.

Quizzes

The quizzes are intended to give students an opportunity to evaluate their progress in analyzing and grasping the material. Two quizzes will accompany the sessions and can be found on Blackboard. Answers will be provided with an explanation of the correct answer. ***Quiz #1 will focus on sessions 1, 2 and 4. Quiz #2 will focus on sessions 5 and 7.***

Discussion Board

This course includes one discussion board assignment which is affiliated with Session One. For this assignment, students are required to participate in online discussions through two substantial postings. **The first post must be an original contribution to the discussion. The second post should be responsive to another student's original posting.**

Because students will be working at their own pace during this condensed course, the discussion board question will be open for the duration of the course. **All posts are due by June 29, 2016 at 11:55 pm.**

You are to approach the posted question or scenario from the perspective of work or professional experience, as well as your own personal experiences. Your evaluation will be based on the degree to which you seriously and deeply think about the question or scenario. Be thoughtful, practical and well-reasoned in your postings and make sure you answer the question and/or provide an analysis for each scenario presented. Additionally, *make sure you give the reasons for your position.* Write clearly and as succinctly as possible—more words do not necessarily make a post better. Read and edit your posting before submitting it. *Constructive but respectful debate is encouraged. Personal attacks are never appropriate.*

A “quality” original posting will be several full paragraphs in length and will specifically respond to the question posed or specifically analyze the scenario presented. Levels of complexity and sophistication of the original postings will be enhanced by reference to both readings and lecture content. A “quality” responsive posting will reflect thoughtful engagement with your cohort, building upon the original postings. This means doing more than merely agreeing or disagreeing with another student's posting. For example, a responsive posting similar to the following is not adequate: *[person's name], you are so right. You are so thoughtful. I was thinking the same thing myself!*”

Grading for Postings

Based on the following criteria, grading for postings is as follows:

Criteria	Maximum Possible
• Timely posting(s)	2
• Directly addressed the question/scenario presented	3
• Strong analytical skills and degree to which student refers to readings and lecture content	6
• Minimum of one original and one responsive posting	3
• “Seriously and respectfully” engaged other postings	6

Total possible points for discussion assignment **20**

19-20 points	A
17-18 points	A-
16 points	B+
15 points	B
14 points	B-
13 points	C+
12 points	C
11 points	C-
10 points	D+
9 points	D
8 points	D-
0-7 points	F

Student Course Outline and Order of Online Sessions

Note: Due to time constraints, we will cover some of the topics listed below in detail, and others at a more cursory level. If a topic is listed below, you should expect that it may appear on the final exam.

It is strongly suggested that you watch the course sessions in the order presented. Each session will likely build on information learned in one or more of the preceding sessions and, therefore, watching the sessions in order will be most beneficial.

Session One: Introduction to HIPAA & Key Terms

Instructor: Barbara Colombo, JD, BSN, Director, Health Care Compliance Program, Assistant Professor of Law, Mitchell Hamline School of Law

Note: This Session includes a discussion board assignment (worth 25% of a student's grade)

Learning Outcomes: Upon completion of this session, the student should be able to:

1. Describe the purpose and underlying philosophy of HIPAA;
2. Recognize the basic HIPAA rule and key terms; and
3. Identify and explain who is required to protect Protected Health Information (PHI) under HIPAA.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter:

Section 1.01 – Administrative Simplification – Background

Section 1.02 – To Whom Do the Administrative Simplification Regulations Apply?

Section 1.03 – Protected Health Information; De-Identified Information; Limited Data Sets

Section 3.01(A) – Minimum Necessary

Section 3.07 – Business Associate Agreements and Data Use Agreements

Section 5.02 – HIPAA Covered Health Plans

Section 5.03 – Non-Health Plan Information

Section 5.07 – Plan Document Requirements for Privacy and Security

Section 6.02(F) – Liability for Acts of Agents, Employees, and Business Associates

Other

- Please skim the following:
 - Sample Business Associate Agreement provisions
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>
 - De-Identification – OCR Guidance
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html>
 - Minnesota Department of Health Standard Consent Form to Release Health Information (2014)
<http://www.health.state.mn.us/divs/hpsc/dap/notices.html>
 - Minnesota Department of Health Access to Health Records Notice of Rights Form, including a list of reasons for release of records without consent under law <http://www.health.state.mn.us/divs/hpsc/dap/notices.html>

Session Two: Authorization and Exceptions

Instructor: Barbara Colombo, JD, BSN, Director, Health Care Compliance Program, Assistant Professor of Law, Mitchell Hamline School of Law

Learning Outcomes: Upon completion of this session, the student should be able to:

1. Identify the elements of a HIPAA authorization form;
2. Describe when authorization is not required; and
3. Describe special applications relating to uses and disclosures.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter:

Section 3.03 – Use and Disclosure of PHI

Section 3.04 – Special Applications of the Rules Relating to Uses and Disclosures

Session Three: Individual Rights

Instructor: Jesse Winsell, JD, Chief Compliance Officer, NorthPoint Health & Wellness Center

Learning Outcomes: Upon completion of this session, the student should be able to:

1. Describe how HIPAA protects individual privacy rights; and
2. Apply the HIPAA requirements related to a notice of privacy practices through review and analysis of a notice of privacy practices.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter
Section 3.02 – Individual Rights

Other

- Government Privacy Poster: Your Health Information Privacy Rights
http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf
- HHS Model Notices (NPP Booklet – HC Provider, and NPP Booklet –Health Plan)
<http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html>
- Minnesota Department of Health Access to Health Records Notice of Rights Form
<http://www.health.state.mn.us/divs/hpsc/dap/notices.html>

Session Four: Preemption Analysis

Instructor: Jesse Winsell, JD, Chief Compliance Officer, NorthPoint Health & Wellness Center

Learning Outcomes: Upon completion of this session, the student should be able to:

1. Explain the general rule of federal preemption analysis under HIPAA, and determine the types of exceptions that allow states to craft more stringent privacy laws in the health care setting; and
2. Describe specific examples of state laws that fall within the preemption exceptions due to the laws being more protective of health information than HIPAA.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter
Section 1.04 – Preemption

Other

- Minnesota Health Records Act, Minn. Stat. § 144.291-298
- Minnesota Consent of Minors for Health Services, Minn. Stat. § 144.341-.347
- Other Minnesota Law
 - Minnesota Government Data Practices Act: An Overview
<http://www.house.leg.state.mn.us/hrd/pubs/dataprac.pdf>
 - Minnesota Patient Bill of Rights, Minn. Stat. § 144.651
- Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, §§ 2.11-2.13

Session Five: HIPAA Security Rule and Compliance

Instructor: Sheri Beck, JD, Privacy Officer, Prime Therapeutics

Learning Outcomes: Upon completion of this session, the student should be able to:

1. Differentiate between the purposes of the security rule and the privacy rule;
2. Describe and provide examples of the security rule safeguards and summarize how to conduct a security assessment;
3. Understand how privacy relates to compliance activities for Covered Entities and Business Associates; and
4. Understand the basics of a compliance program, including the 7 elements of an effective compliance program.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter

Section 4.01 – General Principles of the Security Regulations

Section 4.02 – Security Program Safeguards

Section 4.03 – Documentation, Policies, and Procedures

Section 4.04 – Special Topics in Security

Section 6.09 – Privacy and Security Compliance Reviews and Audits

Session Six: HIPAA Security Rule and Mobile Device Challenges

Instructor: Gordon Apple, JD, Law Offices of Gordon J. Apple, P.C.

Learning Outcomes:

Upon completion of this session, the student should be able to:

1. Identify the general HIPAA security standards and implementation specifications applicable to Covered Entities and their Business Associates; and
2. Recognize how the HIPAA standards and implementation specifications meet the challenges posed by the pervasive use of mobile devices, such as laptops, tablets and smart phones.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter

Section 4.01 – General Principles of the Security Regulations

Section 4.02 – Security Program Safeguards

Section 4.04 – Special Topics in Security

Session Seven: Privacy Breaches

Instructor: Sheri Beck, JD, Privacy Officer, Prime Therapeutics

Learning Outcomes:

Upon completion of this session, the student should be able to:

1. Describe key terms, including unsecured protected health information and breach;
2. Explain the risk assessment process used for determining whether a breach has occurred; and
3. Differentiate breach notification under HIPAA and state law.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter
Section 3.06 – Breach Notification
Chapter 5 - Breach Regulations

Other

- Please skim the following:
 - Mass General Settlement Agreement
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralra.html>
 - OCR's Summary of Penalties (Civil and Criminal)
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>
 - Minn. Stat. § 325E.61 (Notice Required for Certain Disclosures)

Session Eight: HIPAA Enforcement

Instructor: Steve Warch, JD, Shareholder and Chair, Health Practice Group, Nilan Johnson Lewis PA

Learning Outcomes: Upon completion of this session, the student should be able to:

1. Describe how HIPAA is enforced through state activity, the Office of Civil Rights, and civil and criminal penalties;
2. Recognize 21st Century innovations and, therefore, challenges related to enforcement; and
3. Relate the incentive program used to increase the use of electronic health records, and identify unintended consequences of the program.

Readings:

HIPAA Compliance Handbook 2016, by Patricia I. Carter
Section 6.01 – Enforcement
Section 6.02- HIPAA Civil Penalties
Section 6.03 – Civil Complaints and Investigations
Section 6.04 – Civil Monetary Penalty Cases
Section 6.05(E) – Resolution Agreements (Massachusetts General Hospital (2011))
Section 6.05(K) (L) & (M) (2013 cases)
Section 6.06 – HIPAA Criminal Penalties
Section 6.07(A)(18) – Criminal Prosecution (Michel Case (2012))
Section 6.08 – Medicare Exclusion
Section 6.10 – No Private Right of Action
Section 6.11 – Using HIPAA Standards in State Law Actions

Session Nine: How to Respond to a Data Breach

Instructor: Paul Luehr, JD, Managing Director & Chief Privacy Officer, Stroz Friedberg

Learning Outcomes:

Upon completion of this session, the student will have gained insight into:

1. Setting-up a proper response plan and team to address a data breach in the healthcare sector;
2. Detecting and containing a breach when it occurs;
3. Managing communications effectively during a breach; and
4. Using lessons learned from a breach in order to improve data security and privacy.

Readings: None.

Session Ten: HIPAA – Security of Electronic Information and Cybercrime

Instructor: Mark Lanterman, CEO and Chief Technology Officer, Computer Forensic Services

Learning Outcomes: Upon completion of this session, the student should be able to:

1. Identify security threats due to the use of electronic devices;
2. Recognize the general types of information that can be recovered from deleted information and how to avoid a security threat when discarding used electronic devices; and
3. Review ethical considerations related to non-traditional evidence sources of information.

Readings: None