

HIPAA (and Other Health Privacy Laws) Syllabus

January 2013

Taught by: Gina Kastel, J.D.
Hamline University School of Law

General Course Information

Course: HIPAA Privacy
Credits: 2
Classroom: Room 101 of the Law School Building
Days/Times: January 3-6, 2013
8:30am – 4:00pm
Instructor: Gina Kastel
Affiliation: Partner, Faegre Baker Daniels LLP
Email: gina.kastel@faegrebd.com

Course Description and Objectives

The focus of this course will be 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 the interplay between HIPAA and other federal and state health privacy laws and the application and enforcement of those laws in a variety of health care settings. Classroom work will incorporate discussions about the close and evolving relationships among health care policy, evolving social norms, and health privacy laws.

The objectives of this course include learning how to: identify situations that implicate HIPAA and other federal and state health privacy laws; understand which provisions of those laws apply to given situations; and apply those laws. 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 privacy laws; 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 analysis.

Course Materials

There is no textbook for this course. Most reading materials are available on the web, with links embedded in this Syllabus. Materials include primary sources (such as statutes and regulations) and secondary sources (such as regulatory commentary and articles from the popular media). I will also ask students to read a small number of select business forms and policies that showcase “HIPAA in action”; these will be made available in an assembled “supplement” that will be distributed at the first class.

Technology Policy

In order to facilitate an interactive class and group discussions, there will be occasions when the class will be asked to close or disable their computers/tablets/smartphones. At other times, students may use technology for note-taking, reference to assigned readings and, if requested by the instructor, for brief web-based research. **If a student uses classroom time to read or send email or text messages, visit websites or engage in any other technology-based activities (including phones and recording devices) for any other purpose, that student will be asked to drop the course and will not receive academic credit.**

Course Evaluation/Grading

1. **Exam.** There will be a take-home, open-book final exam. Students will have 72 hours between the time they “pick up” the exam online and the time they “return” it. Students can get their exam on January 7th, after class, and must return it by January 13th. **The exam will account for 100% of a student’s grade, except as noted below.**
Note 1: Exams will be graded on both substance and drafting. They should be well-written and well-reasoned, not simply a recitation of course content, as that is how practicing attorneys and practicing privacy officials are judged.
Note 2, per AR-105(B)(8): A student who does not take a scheduled examination will receive a grade of “F” for that examination, unless properly excused. In addition, any student who does not turn in a required paper on the scheduled date will receive a grade of “F” for that paper, unless properly excused. Failure to meet any course requirement can be the basis for a final grade of “F” in the class, unless properly excused.
2. **Participation. I reserve the right to “bump” up students’ final grades by ½ grade for meaningful class participation.** “Meaningful” means thoughtful, well-prepared and attentive participation in class discussion (quality being more important than quantity).

Course Attendance

At the beginning of each class, a roster will be circulated for students to sign. Given the short, intensive course duration, students should plan to attend during all classroom time. If possible, please advise the instructor in advance if you anticipate you may need to miss any portion of classroom time. Any unexcused absence will be treated as “excessive.” Exceptions to this policy will be made on a case-by-case basis.

Instructor Affiliation/Disclaimer

During my “day job” I am a partner in the Health and Life Sciences practice at Faegre Baker Daniels LLP. My clients include hospitals, physician practices, medical device manufacturers, and a variety of other health care companies. I advise clients on a range of health care regulatory matters, including managing health information privacy and security.

Much of what I will be teaching about draws on my legal and practical knowledge of health care organizations and the laws that impact them and the individuals they serve. However, all of the opinions I may express during this course are my own and do not represent the views of my firm or any of the firm’s clients.

Course Schedule and Reading Assignments

We will start class *promptly* at 8:30 am and finish by 4:00 pm each day. Class time is divided into two half-day sessions each day – morning and afternoon – separated by a one-hour lunch each day. (We will also take one short break during each morning session and one short break during each afternoon session.)

The course schedule, topics and associated reading assignments are laid out below by date, with “Morning” and “Afternoon” sessions on each day that we meet. There will be 8 “Sessions” altogether. Readings, however, are listed for the *day*, not the session, and students are expected to complete reading assignments *prior to* the day they are listed, unless otherwise noted. The reading list may look long on certain days, but most are very short excerpts from primary sources.

I reserve the right to modify the schedule slightly to accommodate guest lectures and interactive class discussions. *Note: Due to our limited classroom time, 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 it to appear on the exam; however, the extent to which you will be expected to address the topic on the exam will generally be commensurate with how much time we spent discussing it in class and/or the corresponding amount of assigned reading there was on that topic.*

Links to Essential Readings

Below I have provided links to essential primary sources (HIPAA Statute and Rules, for example). When the assigned reading for a given day relates to a specific section or subsection, I have provided, in the syllabus, the citation to the specific section or subsection in the readings for that day. *However, I will not link to each section or subsection, so students will be required to navigate their way through the statute or regulation to locate the cited materials.*

Following are links to essential primary sources. Students are encouraged to bookmark these. Links are current/working as of November 10, 2012.

1. **Health Insurance Portability and Accountability Act of 1996** (hereafter referred to as “HIPAA” or “HIPAA Statute”). PL 104-191.
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/index.html#1177>
2. **HIPAA Privacy Rule.** 45 CFR Parts 160, 162 and 164.
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/admsimpregtext.pdf>
OR in Federal Register Format, 65 Fed. Reg. 82,462 (December 28, 2000)
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf>
3. **HIPAA Security Rule.** 45 CFR Parts 160, 162 and 164.
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/admsimpregtext.pdf>
4. **Health Information Technology for Economic and Clinical Health (HITECH) Act** of the American Recovery and Reinvestment Act (ARRA) of 2009. PL 111-5, Division A, Title XIII, Subtitle D (Privacy).
5. **Minnesota Health Records Act.** Minn. Stat. 144.291-.34.
<https://www.revisor.mn.gov/statutes/?id=144>
6. **Confidentiality of Alcohol and Drug Abuse Patient Records.** Public Health Service Act, codified at 42 USC 290dd-3 and 290ee-3.
http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=02b3d31742318b503b8d4ba0111d0e35&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl

January 3, 2013

Day 1: Thursday Morning (Session 1)

What Is Health Privacy, and Why Do (Some) People Care (More than Others)?

- Instructor's Introduction/Background
- Syllabus, Grading and Other Expectations
- Introduction to the State of Health Privacy Today and Public Policy Underpinnings
- Student Introductions, including "Privacy Experiences"
- General Statutory and Regulatory Schemes

Some Basic HIPAA Concepts: What Is (and Isn't) Protected, and Who Needs to Protect It?

- "PHI and EPHI": What Is "Protected" Under HIPAA?
- De-Identification (versus Aggregation versus Encryption)
- "Covered Entities"

Day 1: Thursday Afternoon (Session 2)

More HIPAA Basics: Covered Entities and the People They Serve

- Treatment, Payment, Health Care Operations (TPO)
- Minimum Necessary Rule
- Individual Rights

Day 1 (January 3) Readings:

- HIPAA Statute Section 261 (Purpose)
- HIPAA Statute Section 264 (Recommendations with respect to Privacy of Certain Health Information)
- HIPAA Privacy Rule – HHS Commentary in 65 Federal Register, Page 82463 ("Purpose") through Page 82474 ("Consents") (December 28, 2000)
- HIPAA Privacy Rule (Applicability)
 - s. 160.102, s. 164.104, s. 164.500
- HIPAA Privacy Rule (Definitions)
 - s. 160.103 (Covered Entity, Electronic Protected Health Information (EPHI), Group Health Plan, Health Care, Health Care Clearinghouse, Health Care Provider, Health Plan, Health Information, Individually Identifiable Health Information (IHI), Transaction)

- s. 164.501 (Covered Functions, Data Aggregation, Designated Record Set, Health Care Operations, Individual, Payment, Protected Health Information (PHI), Treatment, Use)
- HIPAA Privacy Rule (Uses and Disclosures of PHI; Treatment, Payment and Health Care Operations (TPO); Minimum Necessary; De-Identification)
 - s. 164.503
 - s. 164.506
- HIPAA Privacy Rule (Individual Rights)
 - s. 164.502(i); s. 164.520 (Notice of Privacy Practices (NPP))
 - s. 164.524 (Access to PHI)
 - s. 164.528 (Accounting of Disclosures of PHI)
 - s. 164.526 (Amendment)
 - s. 164.522(b) (Special Communications)
 - s. 164.522(a) (Special Restrictions)
 - s. 160. 306, s. 164.520(b)(1)(vi); 164.530(d)(1) (Complaint)
 - Government Privacy Poster: Your Health Information Privacy Rights http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf
- Amendments under HITECH/ARRA Statute
 - S. 13400(e) (Access in e-format)
 - S. 13400(c) (Accounting through EHR)
 - S. 13400(a) (Special restrictions on disclosures to health plans)

January 4, 2013

Day 2: Friday Morning (Session 3)

Permissions and Exceptions

- Permissions
 - Notice of Privacy Practices
 - Consents
 - Authorization
 - Agree/Object (Opt-in, Opt-out)
 - Facility Directories, Clergy
 - Individuals Involved in Care
- Exceptions
 - Mandated Disclosures
 - Public Health
 - Disaster Relief
 - Health Oversight
 - Judicial and Administrative Proceedings
 - Law Enforcement
 - Special Government Functions
 - Workers' Compensation

- “Incidental Disclosures”

Day 2: Friday Afternoon (Session 4)

HIPAA Was the Easy Part: Now It Gets Complicated

- HIPAA Pre-emption
- State Laws (focus on Minnesota)
- Heightened Protections
 - Psychotherapy Notes
 - Genetic Information
 - Drug/Alcohol Treatment
 - Developmental Disabilities
 - Minors

Day 2 (January) Readings:

- HIPAA Privacy Rule
 - s. 164.508 (Uses and Disclosures for which an Authorization Is Required)
 - s. 164.510 (Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object)
 - s. 164.512 (Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object Is Not Required)
 - s. 164.530(c) (Incidental Disclosures)
 - Subpart B – Preemption of State Law (ss. 160.201-.205)
 - s. 164.508 (a)(2) (Psychotherapy Notes)
 -
 - s. 164.502(g) (3) (Unemancipated Minors)
- Minnesota Health Records Act, Sections 144.291-298
- Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2
- Notice of Privacy Practices
http://www.allinahealth.org/ahs/customerservice.nsf/page/patient_privacy
 (Minnesota version)

January 5, 2013

Day 3: Saturday Morning (Session 5)

More Complications: Doing Business – Securely and Compliantly

- Business Associates and BAAs
- HIPAA Security Provisions
- Elements of a *Privacy* Compliance Program

Day 3: Saturday Afternoon (Session 6)

Covered Entities Revisited; Special Uses

The Real World and Special Uses

- ACEs, OHCAs, Hybrids and the CE/BA dilemma
- Marketing
- Fundraising
- Research

January 5 Readings:

- HIPAA Privacy Rule
 - s. 160.103 (Definition of Business Associate)
 - s. 164.502(e) (Disclosures to Business Associates)
 - s. 164.504(e) (Business Associate Contracts)
 - s. 164.504(a) (Definition of Hybrid Entity)
 - s. 164.504(b), (c) (Hybrid Entities and Health Care Components)
 - s. 164.504(d) (Affiliated Covered Entities)
 - s. 164.504(g) (Multiple Covered Functions)
 - s. 164.501 (Definition of Organized Health Care Arrangement)
 - s. 164.506(c)(5) (Organized Health Care Arrangements)
 - s. 164.530(a), (b), (c), (d), (e), (f), (g), (i), (j) (Administrative Requirements)
 - s. 164.501 (Definition of Marketing)
 - s. 164.508(a)(3) (Marketing)
 - s. 164.514(f) (Fundraising)
 - s. 164.501 (Definition of Research)
 - s. 164.512(i) (Research)
- Amendments under HITECH/ARRA Statute
 - s. 13404 (Application of Privacy Provisions and Penalties to Business Associates of Covered Entities)
 - s. 13406(a) (Conditions on Marketing Contacts)
 - s. 13406(b) (Conditions on Fundraising Contacts)
- Examples of Compliance Program Documents – skim:
 - HIPAA Compliance Program Document Developed for a Medical Specialty Clinic by a Law Firm (out of date, but still a fairly typical example)
<http://www.ohiopainclinic.com/pdf/HIPAAPolicy.pdf>
 - Pharmaceutical Company Compliance Program Document (not HIPAA-specific)
<http://www.merck.com/about/how-we-operate/compliance/MerckCo-Comprehensive-Comp-Prog.pdf>
- HIPAA Security Rule – Relax: students will not have to read the Rule itself! Instead, just skim:

- OCR's Security 101 Publication
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf>

January 6, 2012

Day 4: Sunday Morning (Session 7)

When Things Go Awry

- Privacy Breaches
- Breach Notification
- Enforcement and Penalties

Day 4: Sunday Afternoon (Session 8)

21st Century Innovations and Challenges

- Electronic Health Records
- Meaningful Use and Interoperability
- Personal Health Records
- Social Media
- Mobile Devices
- Medical Identity Fraud
- The Cloud

Wrap-Up

January 6 Readings: YOU SHOULD JUST SCAN THE POPULAR MEDIA ARTICLES AND GOVERNMENT POSTS FOR TODAY AND BOOKMARK THEM FOR FUTURE REFERENCE

- Mass General Settlement Agreement
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgenerala.html>
- HIPAA Privacy Rule
 - s. 164.400-414 (Notification of Security Breach)
 - s. 164.530(f) (Mitigation)
 - Subpart C (s. 160-304, .308, .312) (Principles for Achieving Compliance, Compliance Reviews, Secretarial Action)
 - OCR's Summary of Penalties (Civil and Criminal)
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>
- Amendments under HITECH/ARRA
 - s. 13402 (Notification in the Case of Breach)
- Minnesota Statutes
 - Section 325E.61 (Notice Required for Certain Disclosures)
- Popular Media Articles and Government Posts to SCAN:
 - "Health Care Social Media Sites Neglect Privacy Protections," *Information Week Healthcare*, Feb. 14, 2011
<http://www.informationweek.com/news/healthcare/patient/229218547>
 - "Cyber Security, Health Care, and Mobile Devices," *Dartmouth Now*, Sept. 20, 2011
<http://now.dartmouth.edu/2011/09/cybersecurity-health-care-and-mobile-devices/>
 - "Security in the Cloud," by John Degaspari, *Healthcare Informatics*, August 2011
<http://www.healthcare-informatics.com/me2/dirmod.asp?sid=9B6FFC446FF7486981EA3C0C3CE4943&nm=Articles%2FNews&type=Publishing&mod=Publications%3A%3AArticle&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=3A350ADA3EA548D18D58A865C64C782C>
 - Medical Identity Theft
<http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.shtm>

dms.us.51081908.01