HIPAA (and Other Health Privacy Laws)
Syllabus

Winter 2014

Adjunct Professor: Mary Prentnieks, J.D., M.P.H.
Hamline University School of Law

General Course Information

Course:	HIPAA Privacy
Credits:	2
Classroom:	Internet-delivered Course
Days/Times:	Internet-delivered Course
Instructor:	Mary Prentnieks
Affiliation:	Medica®, Senior Director, Associate General Counsel
Email:	mary.prentnieks@medica.com
Co-Instructor:	Amy Petschauer
Affiliation:	UnitedHealthcare, Compliance Consultant
Email:	apetschauer01@hamline.edu

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 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 a variety of health care settings.

The objectives of this course include learning how to: (i) identify situations that implicate HIPAA and other federal and state health privacy laws; (ii) understand which provisions of the privacy and security laws apply to given situations and how to apply those laws; 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 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: (i) primary sources (such as statutes and regulations); (ii) secondary sources (such as regulatory commentary and articles from the popular media); and (iii) a small number of select business forms and policies that showcase "HIPAA in action."

Instructor Affiliation/Disclaimer

During my "day job" I work at Medica, a Minnesota based health plan company, where I provide legal advice on a range of health care regulatory matters related to state and federal government programs, including matters related to health information privacy.

In an effort to provide a meaningful program with practical insight, I have asked a number of professionals to present in addition to myself. You will learn from attorneys and consultants who are experts in the privacy and security fields. Background and contact information related to each presenter will be posted on Blackboard. All of the opinions expressed during this course are the opinions of the presenters and do not represent the views of their employers or clients.

Co-Instructor Affiliation

Amy Petschauer is the Co-Instructor for the course. Amy currently works at UnitedHealthcare in the area of Medicare compliance for the customer service organization within the Medicare and Retirement business segment. Amy participated in the first online course of the Certificate in Health Care Compliance program at Hamline last year. Amy received her undergraduate degree and Master of Arts in Public Administration from Hamline.

Course Evaluation/Grading

1. **Final Exam.** Students can choose to take the final exam either in a proctored setting through the Hamline Law Registrar's Office or online via Respondus Monitor and LockDown Browser in Blackboard. **The exam will account for 50% of a student's final grade.** This will be an open-book, open-note exam (electronic notes and materials may not be used). Students will have up to two hours to take this exam. Students taking the exam online can take it during any two-hour time period, January 17th - 21st. Students taking the exam on campus can pick-up the exam on the following dates: January 17 (8:30 a.m. or 1:00 p.m.), January 18 (8:30 a.m.), January 19 (8:30 a.m.), or January 21 (8:30 a.m. or 1:00 p.m.)

2. **Discussion Board Posts, Assignments, and Quizzes.** Discussion Board posts, two assignments, and two quizzes will account for 50% of a student's final grade. Evaluation criteria for the Discussion Board posts are discussed below. Please note the following schedule for online Discussion Board posts, assignments, and quizzes.

   A. Session 2: Discussion Board Posts (original and responsive) (Discussion Board posts are due any time prior to a student taking the final exam.)
   B. Session 3: Assignment
   C. Session 4: Quiz

D. Session 5: Quiz
E. Session 6: Assignment

Method of Instruction and Work Expectations

This course will be taught in 11 online sessions. Each session will contain a videotaped lecture with supportive PowerPoints. The course will open on Thursday, January 2, 2014, and any session Discussion Board posts, assignments, and quizzes will be posted via Blackboard and are due on the date specified.

Please note: Assignments and quizzes will be posted in the corresponding Session folder under "Readings & PowerPoints." The discussion board question assigned in Session 2 will be posted on the Discussion Board.

Discussion Board posts, assignments, and quizzes must be submitted by specified deadlines. Late assignments will not be graded and will receive 0 points, unless an extension is received prior to the deadline.

Discussion Board

For the Discussion Board posts, assigned in Session 2, students are required to participate 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, all Discussion Board posts (original and responsive) may be submitted any time before a student takes the final exam.

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 a few full paragraphs in length and will specifically respond to the question posed or specifically analyze the scenario presented. Levels of complexity and sophistication of our 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 these 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 each 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
Session Length: One Hour Fifty Minutes (unless otherwise indicated)

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 it to appear on the final exam; however, the extent to which you will be expected to address the topic on the final exam will generally be commensurate with how much time was spent covering the material during a session and/or the corresponding amount of assigned reading there was on that topic.

Links to Essential Readings

- **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

- **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).

- **HIPAA Administrative Simplification Regulation Text (Privacy and Security Rule)**. 45 CFR Parts 160, 162 and 164. For a copy of the regulation text, as amended after HITECH, click on the following link, and then scroll down and click on "View the Combined Regulation Text."
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

  For a copy of the Federal Register notice of the "Final Rule to Modify HIPAA Privacy, Security, and Enforcement Rules," also referred to as the "HIPAA Omnibus Rule," that was promulgated to implement statutory amendments under HITECH and the Genetic Information Nondiscrimination Act of 2008, click on the following link:
  http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

  For a history of the privacy rule, refer to the preambles in the Federal Registers, 65 Fed. Reg. 82,462 (December 28, 2000), and 67 Fed. Reg. 53,182 (August 14, 2002), which can be accessed by clicking on the following links:
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf

  http://www.gpo.gov/fdsys/pkg/FR-2002-08-14/pdf/02-20554.pdf

- **Minnesota Health Records Act**. Minn. Stat. § 144.291-.34.
  https://www.revisor.mn.gov/statutes/?id=144

- **Confidentiality of Alcohol and Drug Abuse Patient Records.** 42 CFR Part 2.
  http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=02b3d31742318b503b8d4ba0111d0e35&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl

Course Session Schedule

Note: 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 & Covered Entities

Instructor: Mary Prentnieks, Senior Director, Associate General Counsel, Medica

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

1. Describe the underlying rationale for HIPAA and how it has evolved,
2. Recognize the basic HIPAA rule and exceptions, and
3. Identify and explain who is required to protect Protected Health Information (PHI) under HIPAA.

Session Description:
Course Overview
Introduction to Health Privacy

The Evolution of HIPAA
Basic Rules and Exceptions
What is HIPAA?

- Privacy & Security Rules

Key Players (Regulators)
Who is required to protect PHI?

- Covered Entities, including
  - Health Plans
  - Health Care Providers
  - Health Care Clearinghouses

When is it appropriate to share information without authorization?

- Treatment, Payment and Health Care Operations
- Transactions

Session 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 (Uses and Disclosures of PHI; Treatment, Payment and Health Care Operations (TPO)
  - s. 164.501
  - s. 164.502
  - s. 164.506

<u>Session Two: HIPAA Key Terms</u> (Includes Discussion Board Post)
Instructor: Mary Prentnieks, Senior Director, Associate General Counsel, Medica

Learning Outcomes: Upon completion of this session, the student should be able to identify and explain key HIPAA terms.

Session Description:
Protection of PHI by Business Associates
The Type of Information Protected
How Information Is Protected

HIPAA Key Terms

- Business Associate
- Business Associate Agreement
- Data Aggregation
- Health Information
- Individually Identifiable Health Information
- Protected Health Information (PHI)
- Electronic PHI
- De-identified Information

- Limited Data Set & Data Use Agreement
- Encryption
- Authorization and Core Elements
- Exceptions to Required Authorizations
- Consent
- Personal Representative
- Incidental Disclosures
- Minimum Necessary
- Designated Record Set

Session Readings:

- HIPAA Privacy Rule
  - s. 164.504(e) (Standard Business Associate Contracts)
  - 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)
  - 164.514 (a)(b)(c) (De-Identification; See also OCR Guidance at link noted below)
  - 164.514(d) (Standard for Minimum Necessary; See also s. 164.502(b))
  - s. 164.530(c) (Incidental Disclosures; See also HHS Commentary in 67 Federal Register, Pages 53193-53195 (Aug. 14, 2002))
- HIPAA Privacy Rule (Definitions)
  - s. 160.103 (Business Associate, Health Information, Individually Identifiable Health Information, Protected Health Information, Electronic Protected Health Information)
  - s. 164.501 (Data Aggregation, Designated Record Set)
- HITECH
  - s. 13400(2)(3)(5)(6)(7)(8)(10)(12)(16) (Definitions)
  - s. 13404 (Application of Privacy Provisions and Penalties to Business Associates)
  - s. 13405(b) (Minimum Necessary)
  - s. 13405(d) (Sale of Protected Health Information)
  - s. 13406(a) (Marketing)
  - s. 13408 (Business Associate Contracts Required for Certain Entities)
- Relax, students need to only 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 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 Three: HIPAA Privacy Rights (Includes Assignment)
Instructor: Bethan Davies, Associate General Counsel, Medica

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

1. Describe how HIPAA protects individual privacy rights,
2. Define what is meant by minimum necessary under HIPAA and describe a limited data set, and
3. Apply the HIPAA requirements related to a notice of privacy practices through review, analysis, and drafting or revising a notice of privacy practices.

Session Description:
Minimum Necessary

- General Rule and Exceptions
- Limited Data Set

Individual Rights

- Notice of Privacy Practices
  - Description and Content
  - Sample Notice Review
  - Distribution
  - Revisions
- Access
  - General Rule
  - Designated Record Set
  - Form/Format, Timing, and Fees
  - Denials
- Accounting of Disclosures
  - General Rule and Exceptions
  - EHR
  - Proposed Regulations
- Amendment
  - General Rule
  - Acceptance and Denials
- Confidential Communications
  - General Rule
  - Provider vs. Health Plan
- Restrictions
  - General Rule
  - Self-payment Exception
- Complaint

Session Readings:

- HIPAA Privacy Rule (Minimum Necessary)
  - s. 164.502(b); s. 164.514(d)

    - s. 164.514(e)(2) (Limited Data Set)
- HIPAA Privacy Rule (Individual Rights)
    - s. 164.520 (Notice of Privacy Practices)
    - s. 164.524 (Access to PHI)
    - s. 164.501 (Designated Record Set)
    - s. 164.528 (Accounting of Disclosures)
    - s. 164.526 (Amendment)
    - s. 164.522(b) (Confidential Communications)
    - s. 164.522(a) (Restrictions)
    - s. 160. 306; s. 164.530(d); s. 164.520 (Complaint to HHS; Complaint to Covered Entity; Notice of Privacy Practices)
    - Government Privacy Poster: Your Health Information Privacy Rights http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf
    - HHS Model Notices http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html
- HITECH
    - s. 13404(a); 13405(b) (Minimum Necessary)
    - s. 13405(c) (Accounting of Disclosures through EHR)
    - s. 13400 (Electronic Health Record)
    - s. 13405(a) (Restrictions on Disclosures to Health Plans)

Session Four: HITECH – What is it and how does it impact HIPAA? (Includes Quiz)

Instructor: Terri Tersteeg, Independent Health Care Policy Analyst, Government and Private Contracts

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

1. Describe the overall changes to HIPAA as a result of HITECH and GINA, and
2. Determine the implications of those changes.

Session Description:

Purpose of HITECH

Overview of HITECH and Its Impact on HIPAA

- Application of Security Provisions to Business Associates
- Breach Notification Provisions
- Education on Health Information Privacy
- Application of Privacy Provisions to Business Associates
- Restrictions on Certain Disclosures; Sales of Health Information; Accounting of Certain PHI Disclosures; Access to Electronic Format of PHI
- Marketing and Opportunity to Opt Out of Fundraising
- Requirement of Business Associate Agreement
- Improved Enforcement (Tiers, Penalties, Authority of State AGs)
- Audits
- Genetic Information Nondiscrimination Act (GINA) and HIPAA Privacy
- Clinical Laboratory Improvement Amendments (CLIA) and HIPAA Privacy

Session Readings:

- HITECH, Title XIII Subtitle D-Privacy http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf
  - s. 13401 (Security Provisions)
  - s. 13402 (Breach Notification)
  - s. 13403 (Education)
  - s. 13404 (Privacy Provisions)
  - s. 13405 (Restrictions on Disclosures, Sales of PHI, Accounting of Disclosures, and Access to PHI in Electronic Format)
  - s. 13406 (Marketing and Opportunity to Opt out of Fundraising)
  - s. 13407 (Breach Notification for Vendors and Non-HIPAA Entities)
  - s. 13408 (Business Associate Agreements)
  - s. 13410 (Enforcement-Tiers and Penalties, State Attorneys General Authority)
  - s. 13411 (Audits)
- HIPAA Omnibus Rule-Preamble – Contains information on comments and how HITECH provisions are integrated into HIPAA https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the
- Genetic Information Nondiscrimination Act of 2008 (GINA) PL 110-233 http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf. (Relax – students can just skim so they have understanding of relation to HIPAA.)
- Clinical Laboratory Improvement Amendments of 1988 (CLIA) and Privacy – Federal Register, 76 FR 56712 (September 14, 2011) http://www.gpo.gov/fdsys/pkg/FR-2011-09-14/pdf/2011-23525.pdf. (Relax – students can just skim so they have an understanding of why it was a concern for HIT Committee.)

<u>Session Five: Federal Preemption and Intersection with State Law – Part I</u>
(Includes Quiz)
Instructor: Jesse Winsell, Privacy Officer, Metropolitan Health Plan

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.

Session Description:
Preemption Analysis
General Rule (Releases)
HIPAA versus State Law

- Minors (Emancipated and Unemancipated)

- Patient Rights
- Consent and Exceptions to Consent
- Gaps
- Recordkeeping
- Mental Health
- Research
- Penalties
- Release to Law Enforcement
- Release to Business Associate
- Preemption Examples

Session Readings:

- Minnesota Health Records Act, Minn. Stat. § 144.291-298
- Minnesota Consent of Minors for Health Services, Minn. Stat. § 144.341-.347
- Notice of Privacy Practices http://www.allinahealth.org/ahs/customerservice.nsf/page/patient_privacy (Minnesota version)
- HIPAA Privacy Rule
  - Subpart B – Preemption of State Law (ss. 160.201-.205)
  - s. 164.501 (Definition of Research)
  - s. 164.512(i) (Research)

Session Six: Federal Preemption and Intersection with State Law – Part II (Includes Assignment)

Instructor: Jesse Winsell, Privacy Officer, Metropolitan Health Plan

Learning Outcomes: This session is a continuation of Session Five. Upon completion of this session, the student should be able to

1. Further describe specific examples of state laws that fall within the preemption exceptions because the state laws are more protective of health information than HIPAA, and
2. Recognize other relevant privacy standards related to accreditation requirements.

Session Description:

Other Minnesota Law

- Data Practices Act (Chapter 13)
- Patient Bill of Rights
- Practitioner Licensure Statutes

Other Privacy Standards

- Joint Commission
- Medicare Hospital Conditions of Participation
- Privacy Act of 1974
- CMS Data Use Agreement

Heightened Protections

- Psychotherapy notes (HIPAA)
- HIV/AIDS
- Genetic Information

- Drug/Alcohol Treatment Records
- Developmental Disabilities

Session Readings:

- Privacy Act of 1974
  http://www.justice.gov/opcl/privstat.htm
- HIPAA Privacy Rule
  - s. 164.508 (a)(2) (Psychotherapy Notes)
- 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

Session Seven: HIPAA Security Rule

Instructor: Kari Myrold, JD, CHPC, Privacy Director, Optum Corporate – United Health Group

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 and security relate to marketing, fundraising, research and the electronic health record,
4. Understand how privacy relates to compliance activities for Covered Entities and Business Associates, and
5. Understand the basics of a compliance program.

Session Description:

HIPAA Security Rule

- Standards
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Risk Assessment

Marketing
Fundraising
Research and Limited Data Set
EHR
Covered Entities Revisited

- ACEs, OHCAs, Hybrids and the CE/BA relationship

Business Associate Agreement Revisited
Privacy Compliance Activities

- 7 Elements of an Effective Compliance and Ethics Program

Session Readings:

Amendments under HITECH

- s. 13404 (Application of Privacy Provisions and Penalties to Business Associates of Covered Entities)

- s. 13406(a) (Conditions on Marketing)
- s. 13406(b) (Conditions on Fundraising)

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. 164.103, s. 164.105 (Hybrid Entities and Health Care Components)
- s. 164.104(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), (h), (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)
- s. 13406(b) (Conditions on Fundraising Contacts)

Students should skim the following resources as they may be helpful references for future problem solving.

Examples of Compliance Program Documents

- 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

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

De-Identification

- OCR Guidance
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html

Research

- OCR Guidance http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/research.html
- HIPAA Privacy Rule [and Research], U.S. Department of Health and Human Services National Institutes of Health (google or can be found at: http://privacyruleandresearch.nih.gov/faq.asp)

Session Eight: HIPAA – Security of Electronic Information from a Practical Perspective

Instructor: Mark Lanterman, CEO and Chief Technology Officer of 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.

Session Description:

The Impact of Digital Evidence

- Impact of Pervasive Use of Computers on Attorneys and Their clients
- Protection from Cybercrime Threats
- Benefits and Burdens of Electronic Evidence
- Recovery of Deleted Information
- Non-traditional Evidence Sources(iPhone, iPad, Social Media) and Related Ethical Considerations

Session Readings: (The following articles are not required reading and may be read at the student's discretion.)

- 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=9B6FFC446FF7486981EA3C0C3CCE4943&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

Session Nine: Risk Assessment and Privacy Breaches
Instructor: Gina Kastel, Partner, Faegre Baker Daniels LLP

Learning Outcomes:
Upon completion of this session, students 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.

Session Description:
Privacy Breaches
- Definition, Examples and Exceptions
- Breach Notification
- Unsecured PHI
- Encryption
- Destruction

Risk Assessment
Discovery of Breach
- Notice to Individuals, Media and HHS
- Timing

Business Associate Post-HITECH Business Associate Notice
Burden of Proof
Administrative Requirements
Preemption and State Law
Examples

Session Readings:
- Mass General Settlement Agreement http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralra.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
  - Minn. Stat. § 325E.61 (Notice Required for Certain Disclosures)

Session Ten: HIPAA Enforcement

Instructor: Steve Warch, 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.

Session Description:

HIPAA Enforcement

- State Activity
- HIPAA Penalties
  - Civil Penalties
  - Criminal Penalties
- Common Process (OCR)
- OCR Investigations
- OCR Audits
  - Initial Auditees
  - Key Findings

Recap of Covered Entity Variations

21st Century Innovations and Challenges

EHR

- The Vision
- HITECH New Programs
- EHR Incentive Program
- EHR as Tool to Transform Health
- Unintended Consequences
- Personal Health Record

Session Readings:

- HIPAA Privacy Rule
  - s. 160.306 (Complaints to HHS)
  - s. 160.308 (Compliance Reviews)
  - s. 160.310(c)(3) (HHS Disclosure to Another Agency if Permitted by Law)
  - s. 160.312 (HHS Response to Complaints)
  - s. 160.314 (Investigational Subpoenas and Inquiries)
  - s. 160.316 (CE and BA Refraining from Retaliation)
  - s. 160.401 (Reasonable Cause)
  - s. 160.402; s. 160.406; s. 160.408 (Basis for Civil Money Penalty (CMP) (s. 160.402(c) (Removed an exception to liability for CE's agents and made BAs liable for CMP.; Amount of CMP; Factors Considered for Amount of CMP)
  - s. 160.406 (Number of Violations)
  - s. 160.410 (Affirmative Defenses)

- s. 160.412; s. 160.414; s. 160.416; s. 160.418; s. 160.420;160.422; 160.424; 160.426 (Waiver; Limitations; Authority to Settle; Penalty Not Exclusive; Notice of Proposed Determination; Failure to Request a Hearing; Collection of Penalty; Notice of Public and Other Agencies)
- s. 160.504 – 160.548 (ALJ Hearings and Related Provisions)

Session Eleven: Course Wrap-Up
Instructor: Mary Prentnieks, Senior Director, Associate General Counsel, Medica