Law School

Continuing Legal Education

Compliance and Risk Management Program Health Law Intensive

"Privacy and Information Security in Health Services"
April 20-21, 2018
Cartwright Hall, Drake University
2608 Forest Ave. | Des Moines, IA

Approved for 8.5 CLE hours (Activity ID Number: 276450)

The Compliance Certification Board (CCB)® has approved this event for up to 10.2 CCB CEUs. Continuing Education Units are awarded based on individual attendance records. Granting of prior approval in no way constitutes endorsement by CCB of this event content or of the event sponsor.

Registration:

Fee for both days is $425 per person. To register online, visit *www.drake.edu/law/cle*.

Academic Information

Optional classroom work is available to qualify for one-half credit toward Drake's Compliance and Risk Management Master of Jurisprudence (MJ) or Master of Laws (LLM) degrees. Attendees who are not currently enrolled in the MJ or LLM program who complete the academic requirement for one intensive can receive this credit if they later apply for and are accepted into Drake's Compliance and Risk Management MJ or LLM program.

In the course, students will participate in a series of skill-building exercises regarding steps that institutions should take to maintain the privacy and security of protected health information. The session culminates with a real-world role play requiring students to demonstrate Health Care Compliance Association competencies during a simulated institutional data breach.

The optional course is April 22, 12:30-4:30 p.m., at Cartwright Hall. For more information including a complete description of the course, visit *www.drake.edu/law/cle*.

Drake UNIVERSITY

Schedule:

Friday, April 20

5-6 p.m. - Registration

6-6:15 p.m. - Welcome and Introduction
Dean Jerry Anderson and Professor Cathy Lesser Mansfield, Drake University Law School

6:15-7:45 p.m. - "Overview of Privacy and Security Laws and Rules"
Craig Sieverding, Davis Brown Law Firm
This session will present an overview on privacy and security rules that impact the access, use, maintenance, and disclosure of information in the health care industry. Laws and regulations covered will include HIPAA/HITECH, Substance Abuse Confidentiality Regulations, applicable Federal Trade Commission (FTC) regulations, Fair Credit Reporting Act (FCRA), and other federal and state laws and regulations that govern the privacy and security of information in this industry. The discussion will cover the types of information protected; the individuals who must comply; and best practices, enforcement, and upcoming trends.

8-9 p.m. - "Patient Access to Records"
JoEllen Whitney, Davis Brown Law Firm
There is a definite tension in the world of medical records regarding ownership and access issues. Providers worry about patient misinterpretation of records, families want to be informed about their loved ones, and patients want access to everything with little effort. HIPAA/HITECH sought to mediate this problem, but the devil is in the details. This session will focus on the core legal expectations of production and patient access, state and federal limitations, the complexities of using apps and other processes for gathering and sharing data; and common but difficult questions that arise.

Saturday, April 21

9-10:15 a.m. - "Risk Analysis"
John Harmon, FR Secure, and JoEllen Whitney, Davis Brown Law Firm
All compliance begins with the core of the security requirements: risk analysis and mitigation. This session focuses on the process for such analysis both before and after a security breach, as well as common and effective processes for legal compliance. The discussion will focus on issues that arise as software and threats change instantly, such as the need for proper policy and governance around information security; the intent behind the law in regard to information security compliance; measuring risk instead of identifying security gaps; and incident likelihood and impact.

10:30-11:45 a.m. - Panel Discussion: "Identifying, Investigating, and Responding to Suspected Breaches"
Moderator: Heather Campbell, Mercy Medical Center
Organizations are increasingly in the news for data breaches. Despite an organization's implementation and maintenance of appropriate privacy and security practices to prevent and/or mitigate the risk of a data breach, they sometimes do occur. This moderated panel discussion will cover what to do when you suspect your organization has suffered a data breach, including how to investigate the suspected breach, determine whether there has been a breach under applicable law, and how and when to respond to the breach.

11:45 a.m.-1 p.m. - Lunch
Keynote Speaker: Ryan Rohlfsen, Ropes & Gray

1:15-2:30 p.m. - "Enforcement and Settlements"
Alissa Smith, Dorsey & Whitney
This session will address HIPAA's enforcement rule, including a discussion of the enforcement agencies, the potential civil money penalties and how they are calculated, the criminal penalties, and enforcement statistics and processes. The presentation will review internal responses to potential privacy violations and best practices for responding to government inquiries. It will also review government enforcement actions under HIPAA, including an analysis of the factors in each case, the penalties imposed, and lessons that can be learned.

2:45-5 p.m. - "Hot Topics"
George Eichhorn, ChildServe
Health information privacy and security concerns continually make the news, whether it is litigation or regulatory action. This session provides a discussion of current "hot" topics, including patient information and an examination of competing interests between payers, providers, and patients; class action lawsuits for data breaches; legislative initiatives to limit penalties and damages for data breaches; and social media usage and concerns.