Articles + Publications | February 3, 2021

Locke Lord Attorneys Contribute to ABA Book “Healthcare Cybersecurity

American Bar Association

WRITTEN BY

Molly McGinnis Stine | Laura L. Ferguson | Matthew Murphy

A team of Locke Lord attorneys has authored two chapters in “Healthcare Cybersecurity,” a book recently published by the American Bar Association.

Chicago Partner and Co-Chair of Locke Lord’s Privacy and Cybersecurity Practice Group **Molly McGinnis Stine** co-authored the chapter “RiskRx: Managing Privacy and Cybersecurity Risks,” which details the reasons health care professionals need to be acutely aware of privacy risks. The authors cover best practices for preventing issues, diagnosing and treating them when they do arise and risk management tools, such as insurance policies provided by commercial insurers.

“For whatever information you have and for whatever period of time, there are a number of practices you should consider for the care of that information or to address situations when your information assets may be vulnerable. Your consideration of your practices is not a one-time exercise. It is imperative that you revisit your information storage and retention practices regularly so that you can adjust them as needed to reflect your business and your risks at any given time,” the authors write.

To read the full chapter, click here.

Houston Partner **Laura L. Ferguson** co-authored the chapter “How to Prepare For and Respond to Cybersecurity Attacks,” which outlines necessary considerations for health care entities concerning their data collection and use, and how that can help prepare the entities for an attack so they are ready to respond. The chapter also lays out best practices for responding to cybersecurity incidents and requirements for notifying the affected parties, which differ from state to state and at the federal level.

“A number of steps can be taken to prepare for a breach notification, which will simplify the response in the event a notification must be made. The first is to maintain comprehensive system and network logs when possible and reasonable. This will improve the organization’s ability to reconstruct the incident and to better determine the affected population to be notified,” they write.

The authors close with an example of the progression of events during a cyberattack and an example of a response strategy.

To read the full chapter, click here.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber