Alta Pro Fall 2020 Cybersecurity Webinar

Chapter 3: Putting Cyber Safety to Work in Your Practice

Live, one-hour CLE webinar (via Zoom)
September 7, 2020
11 AM Eastern Standard Time

11 AM – 11:20 AM
Cyber Liability Insurance and Risk Management

a) Cyber risk management is an ethical requirement.

b) The Duty of Technical Competence / ABA Model Rule of Professional Conduct 1.1 Comment [8]: *"Maintaining Competence: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology ...."*
c) Cyber liability insurance
- What it is, what is isn't
- Team cyber liability attorneys and security professionals
- Pre-breach risk management tools and services to help mitigate risk of a cyber incident occurs.

d) Cyber liability insurance and professional liability insurance: Compare and contrast

11:20 AM – 11:35 AM
Have a Data Privacy Policy

a) Data privacy is an ethical requirement.

b) ABA Model Rule 1.6 Client Confidentiality. "*A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."*

c) Things to consider including in your firm's Data Privacy Plan:
- Train and educate your staff to recognize, report and respond appropriately to a cyber threat or cyber event.
- Make sure all software programs are up-to-date and functioning properly.
- Install updates and patches when they become available.

- Use secure passwords (a password manager is recommended) and change them often.
- Use two-factor authentication.
- Have an office policy on cyber preparedness.
- Make sure your office policy has clear guidelines for working remotely and taking laptops and devices off-site.
- Limit access to sensitive systems, files and data.
- Obtain cyber liability insurance.
- Discuss ABA Model Rule 1.1 and its ramifications at your next office staff meeting.

11:35 AM – 11:50 AM
Have an Incident Response Plan

Things to consider:

- Procedures for initial reporting of an incident
- Confirmation of the incidents
- Escalation as appropriate
- Investigation
- Data breach response
- Electronic data restoration
- Having a designated incident response project manager
- Assembling a cross-disciplinary response team. The team might include everyone from IT professionals to a PR firm.
- Training the response team on breach reporting obligations, mitigation requirements and the steps needed for recovery.
- Post-incident review
- Revising the plan to incorporate all lessons learned

11:50 AM – 12:00 Noon
Q&A and Close

TODD
Insert Presenter Bios here