Hot Topics in Ethics: Cybersecurity and Ways of Maintaining Client Confidentiality in a High-Tech World

Panel: W. Scott Blackmer, Info Law Group LLP, Salt Lake City, UT  
Claudia Rast, Butzel Long, Ann Arbor, MI  
David Ries, Clark Hill Thorp Reed, Pittsburgh, PA

Moderator: Pamela Esterman, Sive, Paget & Riesel, New York, NY

Top Ten Suggestions for Law Firm Lawyers

1. **Conduct Risk Assessment.** Evaluate the firm’s current cybersecurity risk profile taking into account the current date and device controls in place, the nature of data and information accessed by the firm, ethical obligations, and other relevant factors.

2. **Inventory & Evaluate Client Security Requirements.** Evaluate client-specific data security considerations (e.g., for covered entities under GLBA or HIPPAA for clients entrusting particularly sensitive corporate or personal data, etc.) that may require additional steps by the firm’s lawyers.

3. **Organize Your Governance.** Organize and empower an information security and data governance committee within the firm to manage information security and cybersecurity risks.

4. **Assign a Champion.** Appoint an individual within the firm (or hire an individual from outside the firm) to serve as a chief information security officer responsible for managing the firm’s day-to-day cybersecurity risks.

5. **Implement a Security Program.** Define and implement a standardized, auditable, risk-based information security program addressing data and cybersecurity.

6. **Require Compliance Among All Suppliers.** Establish stringent requirements for data security in software installations, cloud or other data service contracts, and vendor contracts.

7. **Develop an Incident Response Plan.** Develop, as part of the information security program, a data security incident response protocol or plan that addresses notification to clients, government authorities, or individuals affected by breaches. As part of this process, consider consulting with law enforcement, if and when appropriate, about cybersecurity risks.

8. **Develop & Enforce Controls.** Develop controls on internet access and on the use of personal devices by members and employees of the firm.

9. **Implement Training.** Educate lawyers and staff within the firm of their obligations as relating to cybersecurity and their role within the firm’s information security program.

10. **Conduct Periodic Audits.** Conduct routine audits of the firm’s information security risks and vulnerabilities.

---

**ETHICAL OBLIGATIONS CHECKLIST**

1. Develop a basic understanding of the risks associated with the technology that you use in your daily practice or consult with someone who does.

2. Staying current about changes in technology is an ongoing process; you must continually reassess and evaluate security measures as technologies change and develop.

3. Be aware that the scope of the information protected under ABA Model Rule 1.6 and the law in most jurisdictions is very broad. It includes all information relating to the representation, not just privileged information.

4. Be mindful of your obligations to protect a former client's confidential information under Model Rule 1.9 (c) as well.

5. When using technology to store or transmit information, you must make reasonable efforts to prevent inadvertent disclosure or unauthorized access to confidential client information.

6. “Reasonable efforts” to protect confidential information include accessing the sensitivity of the information and the likelihood of disclosure if additional safeguards are not employed.

7. Establish procedures to train and supervise others you practice with—both lawyers and nonlawyers—in their use of technology to ensure that client confidences are protected.

8. When disposing of portable electronic devices, take precautions to ensure that all confidential client information has been removed. If recycled, verify that the recycler follows appropriate protocols to remove the data.


10. When using cloud computing or outsourcing services, verify that the service provider has in place adequate security measures to prevent the inadvertent disclosure of or unauthorized access to confidential client information.

---

*ABA Handbook on Cybersecurity.*