New York State Continuing Legal Education Board

Guidance Relating to the New Cybersecurity, Privacy and Data Protection Category of CLE Credit

The Cybersecurity, Privacy and Data Protection category of CLE credit has two parts: **Ethics** and **General** (New York State CLE Program Rules, section 1500.2[h]).

Below are program ideas intended to assist providers when planning Cybersecurity Ethics and Cybersecurity General courses. Providers are not limited to the subjects listed and are encouraged to develop relevant and timely programs.

Program Areas for Cybersecurity Ethics

Awareness/Application

1. The rules governing attorney conduct, including New York's Rules of Professional Conduct and the ABA Model Rules, as they apply to electronic data and communication
2. Ethics opinions relating to electronic data and communication, including ethics opinions of bar associations and other groups
3. Norms relating to lawyers' professional obligations to clients, law office, court and third parties regarding securing and protecting electronic data and communication
4. Hypotheticals addressing ethical issues relating to cybersecurity in legal practice (teaching about or discussion of the circumstances encountered when securing, protecting and maintaining electronic data and communication)

Protecting Client

1. Ethical obligations relating to confidentiality and how they apply to securing, protecting and maintaining clients' confidential, privileged and proprietary electronic data and communication
2. Ethical obligation to secure and protect escrow funds from cyber threats, cyber attacks and data breaches
3. Professional responsibility to safeguard and secure clients' electronic data and communication

Communicating and Obtaining Consent from Client

1. Responsibility to communicate with client about how and where client information will be stored, maintained, and related privacy implications
2. Responsibility to communicate with client about law office's electronic data and communication protection protocols and policies
3. Obtaining informed consent from client regarding electronic communication and data storage policies and practices

Protecting Law Office

1. Ethical obligations relating to confidentiality and how they apply to securing, protecting and maintaining law office's confidential, privileged and proprietary electronic data and communication (including remote work)
2. Professional responsibility to safeguard and secure law office's electronic data and communication
3. Ethical obligation to secure and protect escrow funds from cyber threats

Storing, Maintaining and Destroying

1. Ethical obligations and professional responsibilities as they relate to storing confidential, privileged and proprietary electronic data and communication
2. Ethical obligations and professional responsibilities relating to maintaining and destroying electronic data and communication

Supervision

1. Ethical obligations and professional responsibilities of supervising employees, vendors and third parties relating to electronic data and communication
2. Ethical obligations and professional responsibilities of supervising law office staff in securing, maintaining and destroying confidential, privileged and proprietary client and law office electronic data and communication

Inadvertent Disclosure/Law Office Failure

1. Ethical obligations surrounding inadvertent disclosure of confidential data and communication by electronic means (duty to client, court, opposing counsel, third parties)
2. Duty to refrain from revealing confidential information by electronic means (e.g., social media usage)

Data Breach/Cyber Attack/Cyber Threat

1. Ethical obligations to client surrounding a data breach, cyber attack, or cyber threat including disclosure to client
2. Ethical obligations to court, opposing counsel and third parties surrounding a data breach, cyber attack or cyber threat

Program Areas for Cybersecurity General

Understanding Technology

1. Understanding fundamental issues of securely sending, receiving and storing client and law office electronic data and communication (including securing internet access, understanding encryption of files, best practices in addressing cybersecurity risks, understanding and using security measures)
2. Understanding and using cybersecurity features of various technologies to protect client and law office electronic data and communication (including encryption, authentication, passwords, virtual private networks, firewalls)
3. Understanding how to reduce the possibility of cyber attacks affecting law office (including when using networks, platforms, mobile devices, software, hardware, backups, remote connections) and knowledge of computer hygiene (including hardware and software updates)
4. Understanding the appropriate questions to ask vendors, third parties and technology staff concerning platforms, hardware and software to protect and secure confidential client and law office information (including remote security management, virtual private networks, firewall settings, back-up systems, mobile device security, “dark web” monitoring)

Understanding Threats

1. Identification and awareness of cybersecurity threats affecting clients, legal professionals and legal organizations (including phishing schemes, malware, hacking, social engineering schemes)
2. Cybersecurity scams directed at legal professionals and legal organizations

Inadvertent Disclosure/Law Office Failure

1. Technological aspects of how to prevent inadvertent disclosure of confidential client and law office information when working with and storing electronic data and communication

Remote Work

1. Understanding and using security measures to protect client and law office electronic data and communication when working remotely (including passwords, authentication, encryption, network security)
2. Technological aspects of protecting client and law office electronic data and communication when using personal or business mobile devices (including

misplacing mobile devices, passwords, authentication, encryption, network security)

Vendors/Third Parties

1. Vetting and assessing vendors or third parties regarding their policies, protocols and practices on securing and protecting electronic data and communication

Cyber Incident Response Planning

1. Technological aspects of cyber incident response planning (including: avoiding data loss; detecting data intrusion; establishing, securing and updating backup systems; and monitoring for cyber threats, cyber attacks and data breaches)
2. Conducting risk assessments, data recovery, and post-breach investigations

Law Office Electronic Data and Communication Policies and Protocols

1. Creating, adopting and updating electronic data and communication protection policies and protocols for law office (including scope of cybersecurity insurance coverage)
2. Creating, adopting and updating cyber incident response plans for law office (including awareness of security best practices and industry standards, and evaluating how best to protect client and law office electronic data and communication)

Laws

1. Applicable laws relating to cybersecurity (data breach notification laws, other federal, state and local laws) and administrative rules and regulations
2. Applicable laws, rules and regulations relating to privacy and data protection
3. Discussion of the New York SHIELD Act (New York “Stop Hacks and Improve Electronic Data Security” Act) including application and compliance requirements