CYBERSECURITY DUTIES FOR ATTORNEYS
RELEVANT ABA MODEL RULES OF PROFESSIONAL CONDUCT

ABA MODEL RULE	SECTIONS AND COMMENTS RELEVANT TO CYBERSECURITY
1.1 — Competence Link: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/	**Rule 1.1- Comment 8**: "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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."
1.4 — Communications Link : https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_4_communications/	**Rule 1.4(a)(3)** – "A lawyer shall…keep the client reasonably informed about the status of the matter." In conjunction with other Model Rules, this duty may include keeping clients informed about the status of client data. **Rule 1.4(b)** – "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." In conjunction with other Model Rules, this duty may include explanations of a lawyer's use of technology.
1.6 — Confidentiality of Information Link: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/	**Section 1.6(c)** – "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." **Rule 1.6- Comment 18** states that Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties, and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. **Rule 1.6- Comment 19** states that when transmitting a communication that includes information relating to the representation of a client, the lawyer must take

ABA MODEL RULE	SECTIONS AND COMMENTS RELEVANT TO CYBERSECURITY
	reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions
1.9 — Duties to Former Clients Link: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_9_duties_of_former_clients/	**Rule 1.9 – Comment 7** states that a lawyer has a continuing duty to preserve confidentiality of information about a client formerly represented. In conjunction with other Model Rules, this duty may include using appropriate data security safeguards for files of former clients.
1.15 — Safekeeping Property Link: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property/	**Rule 1.15 - Comment 1** states that a lawyer should hold property of others with the care required of a professional fiduciary. In conjunction with other Model Rules, this duty may include secure safekeeping of clients' or third persons' data and/or digital assets.
5.1 — Responsibilities of a Partner or Supervisory Lawyer Link: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_1_responsibilities_of_a_partner_or_supervisory_lawyer/	**Rule 5.1 – Comment 2**: "Paragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules of Professional Conduct. Such policies and procedures include those designed to… account for client funds and property and ensure that inexperienced lawyers are properly supervised." In conjunction with other Model Rules, this duty may include ensuring that data security protocols are followed by all lawyers in a firm.
5.3 — Responsibilities Regarding Nonlawyer Assistance Link:	**Rule 5.3 – Comment 3**: "A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include…hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an

ABA MODEL RULE	SECTIONS AND COMMENTS RELEVANT TO CYBERSECURITY
https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/	Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer."

ABA Ethics Opinions on Cybersecurity Topics

Formal Opinions	Opinion 498 (2021) — Virtual Practice Permits virtual practice but advises that when working remotely, there may be special precautions required to secure client information, and to prevent inadvertent or unauthorized disclosure or unauthorized access to information about a client or their case. The opinion also discusses virtual technology updates, mail correspondence, personal device policies, clean desk policies and the use of paralegal services. This opinion follows on Opinion 495 (2020), which considers the need for lawyers to work remotely. Link: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf
	Opinion 495 (2020) — Lawyers Working Remotely Lawyers may remotely practice the law of the jurisdictions in which they are licensed, while physically present in a jurisdiction in which they are not admitted, if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction, and do not provide or offer to provide legal services in the local jurisdiction. This practice may include the law of their licensing jurisdiction or other law as permitted by ABA Model Rule 5.5(c) or (d), including, for

	instance, temporary practice involving other states or federal laws. Having local contact information on websites, letterhead, business cards, advertising, or the like would improperly establish a local office or local presence under the ABA Model Rules. Link: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-495.pdf
	Opinion 482 (2018) — Ethical Obligations Related to Disasters Lawyers should maintain or be able to retrieve or to create on short notice, electronic or paper lists of current clients and their contact information. This information should be stored in a manner that is easily accessible. Information about how to contact the lawyer in the event of an emergency may be provided in a fee agreement or an engagement letter. Lawyers may not be able to gain access to paper files following a disaster. Consequently, lawyers must evaluate in advance how to store files electronically so that they will have access to those files via the Internet if they have access to a working computer or smart device after a disaster. If Internet access to files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer. lawyers should maintain an electronic copy of important documents in an off-site location that is updated regularly. Although not required, lawyers may maintain these files solely as electronic files, except in instances where law, court order, or agreement require maintenance of paper copies, and as long as the files are readily accessible and not subject to inadvertent modification or degradation. As discussed above, lawyers may also store files "in the cloud" if ethics obligations regarding confidentiality and control of and access to information are met. Link: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_482.pdf
	Opinion 483 (2018) — Lawyers' Obligation After an Electronic Data Breach or Cyberattack The duties of competence, confidentiality and responsible supervision require attorneys to "employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data." Lawyers using technology must safeguard and monitor the security of electronically stored client property and information. Lawyers also must act reasonably and promptly to stop a data breach and mitigate any resulting damage. It is recommended that lawyers proactively develop an incident response plan before falling victim to a data breach. If a breach occurs, lawyers must take all reasonable actions to restore computer operations in order to serve their clients. Lawyers also must conduct a post-breach investigation to determine what confidential material has been compromised and notify clients and any other parties ethically and legally entitled to notice. Link: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf
	Opinion 477R (May 2017) — Securing Communication of Protected Client Information [Update to ABA Formal Opinion 99-413- *Protecting the Confidentiality of Unencrypted E-Mail* (1999)] The use of unencrypted routine email generally remains an acceptable method of lawyer-client communication. However, cyberthreats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable

	to rely on the use of unencrypted email. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment 18 factors to determine what effort is reasonable. Link: https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/
	Opinion 11-459 (2011) — Duty to Protect the Confidentiality of Email with One's Client A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party. Link: https://www.americanbar.org/content/dam/aba/publications/YourABA/11-459.authcheckdam.pdf
	Opinion 99-413 (1999) — Protecting the Confidentiality of Unencrypted E-Mail Concludes that a lawyer does not violate his or her ethical obligations in transmitting client information by way of e-mail because of the overall complexity of intercepting email messages. Link: https://www.americanbar.org/products/ecd/chapter/219976/
	Opinion 95-398 (1995) — Access of Nonlawyers to a Lawyer's Data Base A lawyer must ensure that data service providers have in place, or will establish, reasonable procedures to protect the confidentiality of information to which they may have access, and moreover, that they fully understand their obligations in this regard. Link: https://www.americanbar.org/products/ecd/chapter/219961/
Informal Opinions	From Paper to Kilobytes (2008), referencing Informal Op. 1384 (1977) — Managing Closed or Dormant Files While generally files are permitted to be stored electronically, a client may have the expectation that certain items such as original wills, deeds or other client property be preserved in the original. Lawyers may have to retain old versions of software to maintain access to documents stored electronically using now-outdated programs. Lawyers must use reasonable care to whenever client confidential information is entrusted for storage to someone outside the firm or practice. Link: https://www.americanbar.org/content/dam/aba/publications/YourABA/201105_FromPaperToKilobytes0208.authcheckdam.pdf