# CYBERSECURITY DUTIES FOR ATTORNEYS

## RULES OF PROFESSIONAL RESPONSIBILITY, ETHICS OPINIONS, CLE REQUIREMENTS AND STATE STATUTES

The following is a list of rules of professional conduct, ethics opinions, CLE requirements, and state statutes relevant to attorneys' cybersecurity obligations. All citations should be checked as they often change and some inadvertent errors may have been made. This chart was last updated in October 2023.

| | |
|---|---|
| **Alabama** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.6(c)** was not adopted. Also, **Rule 1.15** mandates preservation of client information for six years, instead of five years.<br>Link: https://judicial.alabama.gov/library/RulesBarConduct |
| Ethics Opinions | **Ethics Op. 2010-02 – Retention/Storage of Client Files** permits lawyers to use cloud computing if the lawyer uses reasonable care to ensure the provider will properly handle data security and will abide by a confidentiality agreement in handling the data. "Lawyers have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider."<br>Link: https://www.alabar.org/office-of-general-counsel/formal-opinions/2010-02/ |
| Statutes | **Data Breach Notification Act of 2018 (Ala. Stat. § 8-38-**1, ***et seq.***) requires government entities, persons and businesses maintaining computerized personal identifying information to implement reasonable security measures as defined in the statute. Establishes legal duty to investigate security breaches and notify Alabama residents and entities within 45 days of a security breach, in writing or via email. The law also mandates proper disposal of paper and digital records containing personal information.<br>Link: http://alisondb.legislature.state.al.us/alison/codeofalabama/1975/174919.htm |
| **Alaska** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.6(c)** specifies that a client may give informed consent to forgo security measures that would otherwise be required by the rule and directly mandates competency.<br>Link: https://courts.alaska.gov/rules/docs/prof.pdf |
| Ethics Opinions | **Ethics Op. 2014-3 - Cloud Computing** permits cloud computing as long as reasonable steps are taken to ensure safeguarding and confidentiality of data.<br>Link: https://alaskabar.org/wp-content/uploads/2014-3.pdf<br><br>**Ethics Op. 1998-2 – Communication by Email** permits lawyers to communicate with clients via unencrypted e-mail; client consent is unnecessary because the expectation of privacy in e-mails is no less reasonable than that in the telephone or fax.<br>Link: https://alaskabar.org/wp-content/uploads/98-2.pdf |

| | |
|---|---|
| Statutes | **Alaska Personal Information Protection Act (AS 45.48. 010 (2022))** requires state/local governmental agencies (except for judicial branch) and businesses that own or license computerized personal information data of state residents to provide notice of a security breach expeditiously to Alaska residents, and in writing or under certain circumstances, by electronic means. No disclosure required if, after an appropriate investigation, the subject entity determines there is no reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from breach. The analysis must be documented and preserved for five years.<br>Link: https://www.akleg.gov/basis/statutes.asp#45.48.010 |
| Arizona | |
| Rules of Professional Conduct | ABA Model Rules verbatim.<br>Link: https://www.azbar.org/for-lawyers/ethics/rules-of-professional-conduct/ |
| Ethics Opinions | **Ethics Op. 09-04 – Client Files, Electronic Storage** permits online file storage and retrieval system if "reasonable precautions" are taken to protect the security and confidentiality of the information. Lawyers must "recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field."<br>Link (enter opinion no.): https://www.azbar.org/for-lawyers/ethics/ethics-opinions/<br><br>**Ethics Op. 07-03 – Electronic Communications** permits electronic communication with reasonable precautions but prohibits analyzing embedded metadata.<br>Link: https://tools.azbar.org/RulesofProfessionalConduct/ViewEthicsOpinion.aspx?id=695<br><br>**Ethics Op. 97-04 – Computer Technology** suggests lawyers caution clients about transmitting sensitive information by e-mail or to consider the use of encryption.<br>Link (enter opinion no.): https://www.azbar.org/for-lawyers/ethics/ethics-opinions/ |
| Statutes | **Security System Breach Law (A.R.S. §§ 18-551 and 552)** mandates that some government agencies (see exemptions in §18-552(N)), person or business provide notice of a breach of personal identifying data to Arizona residents and business entities within 45 days. Notice not required if an independent third-party forensic auditor or law enforcement agency determines after a reasonable investigation that the breach has not or is not reasonably likely to result in substantial economic loss to affected residents such as when it is encrypted or redacted.<br>**This law specifically does not apply to prosecution agencies.<br>Links:<br>https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/18/00551.htm, |
| Arkansas | |
| Rules of Professional Conduct | ABA Model Rules verbatim, except for **Rule 1.15** which has further specifications that are not relevant to cybersecurity.<br>Link: https://opinions.arcourts.gov/ark/cr/en/item/1868/index.do |

| | |
|---|---|
| Ethics Opinions | Ethics opinions are only available to Arkansas bar members. |
| Statutes | **Personal Information Protection Act (AR Code § 4-110-103- 105 (2020))** requires state agencies and businesses that acquire or maintain computerized personal information about an Arkansas resident to implement reasonable security procedures and practices. Must also give notice of breach of electronic data containing personal information to Arkansas residents in the most expedient time possible and without unreasonable delay, in writing, electronic mail or substitute means under certain circumstances. Notification is not required if, after a reasonable investigation, the subject entity determines there is no reasonable likelihood of harm to consumers. Statute doesn't apply to encrypted or redacted personal information.<br>Link: https://law.justia.com/codes/arkansas/2010/title-4/subtitle-7/chapter-110/4-110-105 |
| **California** | |
| Rules of Professional Conduct | Although using somewhat different language and organization, no practical difference from relevant ABA Model Rules, except **Model Rule 1.6(c)** mirrors the California Business and Professions code, Section 6068. And **Rule 1.15** was revised January 2023 requiring certain procedures for receiving client funds, securities or property (potentially including data).<br>Link: https://www.calbar.ca.gov/Attorneys/Conduct-Discipline/Rules/Rules-of-Professional-Conduct/Current-Rules/Chapter-1-Lawyer-Client-Relationship |
| Ethics Opinions | **Formal Op. 2023-208 – Working Remotely** provides detailed guidance on how lawyers must ensure that technology used for remote working is consistent with ethical obligations. Suggests reasonable security measures.<br>Link: https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/Formal-Opinion-No-2023-208-WFH.pdf<br><br>**Formal Op. 2020-203 – Securing Electronic Systems** requires lawyers using electronic devices to take reasonable security steps to minimize the risk of unauthorized access. If a breach occurs, lawyers must investigate and notify clients who may be negatively impacted. Endorses ABA Formal Op. No. 483.<br>Link: http://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/Formal-Opinion-No-2020-203-Data-Breaches.pdf<br><br>**Formal Op. 2015-193 – E-Discovery** discusses the precautionary safeguards and response measures that need to be taken to satisfy the duties of competency, supervision and confidentiality in regards to e-discovery.<br>Link: https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL.pdf<br><br>**Formal Op. 2012-184 – Virtual Offices and Cloud Computing** permits virtual offices and concludes that no additional safeguards are needed for using the cloud when working remotely.<br>Link: https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/CAL%202012-184-ADA.pdf |

| | |
|---|---|
| | **Formal Op. 2010-179 – Using Technology to Store and Transmit Data** endorses ABA Formal Op. No. 483, which allows consulting an expert if a lawyer's own technology skills are lacking. The opinion provides factors to consider when choosing storage or transmission technology so that "appropriate steps" are taken to ensure that use of technology does not subject client information to an undue risk of unauthorized disclosure.<br>Link: https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/2010-179-Interim-No-08-0002-PAW.pdf<br><br>**Formal Op. 2001-157 – File Retention** establishes an obligation to make reasonable efforts to examine file contents and to obtain the former client's consent to any disposition that would prevent the former client from taking possession of the items. No specific time period for retention of a particular item can be specified. Files in criminal matters should not be destroyed without the former client's consent while the former client is alive.<br>Link: https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/2001-157.htm |
| Statutes | **Cal. Civ. Code §§ 1798.29** requires state agencies that own or licenses computerized data containing personal information to disclose a security breach and notify California residents in the most expedient time possible if unencrypted data or encryption key was stolen.<br>Link:<br>https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.29.&nodeTreePath=8.4.33.1.5&lawCode=CIV<br><br>**Cal. Civ. Code §§ 1798.80, *et seq.*** mandates businesses to have reasonable cybersecurity measures when they retain personal information, as well as proper disposal methods of data containing personal information. §1798.82(a) mandates notice of a security breach to California residents in the "most expedient time possible" and without unreasonable delay. Creates encryption safe harbor if the encryption key or security credential is not reasonably believed to have been acquired by an unauthorized person such that it could be used to render the personal information readable or usable. Notification is not dependent on risk of harm to consumer. **This law does not apply to government agencies.<br>Link:<br>https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.80.&nodeTreePath=8.4.36&lawCode=CIV<br><br>**Cal. Civ. Code §§ 1798.14, *et seq.*** sets out rules for state agencies that maintain personal information. §1798.21 requires appropriate, reasonable administrative, technical and physical safeguards to ensure security of confidential records. §1798.29 provides notice provisions for state agencies in the event of data security breaches. **Per the definition in Cal. Gov. Code §7920.510T, this law does not apply to local agencies.<br>Link to Cal. Civ. Code §§1798.14, *et seq*:<br>https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.14.&lawCode=CIV<br>Link to Cal. Gov. Code §7920.510:<br>https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=GOV&division=10.&title=1.&part=1.&chapter=2.&article= |

| | |
|---|---|
| | **California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) (Cal. Civ. Code §§ 1798.100–1798.194)** require certain businesses that collect consumers' personal information to implement and maintain reasonable data security procedures and practices. **This law does not apply to government agencies.<br>Link:<br>https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100 |
| Colorado | |
| Rules of Professional Conduct | ABA Model Rules verbatim, except **Rule 1.15** requires preservation of client property for 7 years. Colorado also added **Rule 1.16A** to specify the circumstances in which client files need to be retained or destroyed.<br>Link: https://www.cobar.org/rulesofprofessionalconduct |
| Ethics Opinions | **Formal Op. 141 (2020)- Data Breach and Cybersecurity Obligations** states that a lawyer must "make reasonable efforts to prevent, monitor for, halt and investigate any security breach of data the lawyer controls". Lawyers also must make timely notification of a security breach to all current clients and affected third parties. The opinion endorses ABA Formal Op. No. 483.<br>Link:<br>https://www.cobar.org/Portals/COBAR/Repository/ethicsOpinions/72020/Opinion%20141Final7-2020.pdf?ver=2020-07-20-100834-770<br><br>**Formal Op. 119 (2011) - Metadata** says lawyers must use "reasonable care" when transmitting electronic documents or files. The duty to provide competent representation requires a lawyer to be reasonably informed about the types of metadata that may be included in an electronic document or file, and the steps that can be taken to remove metadata if necessary.<br>Link:<br>https://www.cobar.org/Portals/COBAR/repository/ethicsOpinions/FormalEthicsOpinion_119_2011.pdf |
| Statutes | **Colorado Consumer Protection Act (C.R.S. §§ 24-73-101-103**- governmental entities**; C.R.S. §§ 6-1-713 713.5**- private entities) Entities that maintain, own or license computerized personal information must implement reasonable security procedures and a written data disposal policy. Must also provide notice of a data breach in the most expedient time possible, without unreasonable delay,. Notification is not required if, after a good faith and prompt investigation, the subject entity determines that misuse of information about a Colorado resident is not reasonably likely to occur, personal information is encrypted/redacted or other security measures were taken.<br>Link to C.R.S. §24-73-101: https://law.justia.com/codes/colorado/2022/title-24/article-73/section-24-73-101/<br>Link to C.R.S. §24-73-102: https://law.justia.com/codes/colorado/2022/title-24/article-73/section-24-73-102/<br>Link to C.R.S. §24-73-103: https://law.justia.com/codes/colorado/2022/title-24/article-73/section-24-73-103/<br>Link to C.R.S. §§ 6-1-713.5: https://law.justia.com/codes/colorado/2022/title-6/article-1/part-7/section-6-1-713-5/ |

| | |
|---|---|
| | Link to C.R.S. §§ 6-1-713: https://law.justia.com/codes/colorado/2022/title-6/article-1/part-7/section-6-1-713/<br><br>**Colorado Privacy Act (Bill 2021-190)** mandates certain businesses (data controllers and processors as defined by statute) use reasonable security measures to store and use personal data. **This law does not apply to government agencies.<br>Link: https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf |
| **Connecticut** | |
| Rules of Professional Conduct | ABA Model Rules verbatim, except **Rule 1.15** requires retention of client property for seven years.<br>Link: https://www.jud.ct.gov/publications/PracticeBook/PB.pdf |
| Ethics Opinions | No relevant formal opinions.<br><br>**Informal Ethics Op. 2013-07- Cloud Computing** advises that a lawyer make reasonable efforts in selecting a cloud service provider to ensure that lawyer and client data is preserved ('backed up'), reasonably available to the lawyer, and reasonably safe from unauthorized intrusion.<br>Link: https://members.ctbar.org/resource/resmgr/Ethics_Opinions/Informal_Opinion_2013-07.pdf |
| Statutes | **Breach of Security- Computerized Data (Conn. Gen. Stat. § 36a-701b)** requires individuals and businesses that own, license or maintain computerized personal information to provide notice of a security breach to Connecticut residents and to the Attorney General within 60 days of discovery. Notification is not required if, after an appropriate investigation, the entity reasonably determines that the breach of security is unlikely to result in harm to the individual whose personal information had been breached such as when it was encrypted or otherwise secured. **This law does not apply to government agencies.<br>Link: https://cga.ct.gov/current/pub/chap_669.htm#sec_36a-701b<br><br>**Protection of Personal Information (Conn. Gen. Stat. § 42-470, *et seq.*)** mandates that individuals and businesses safeguard any data, computer files and documents containing the personal information of another person and sets out civil penalties with additional requirements if social security information is breached. **This law does not apply to government agencies.<br>Link: https://law.justia.com/codes/connecticut/2022/title-42/chapter-743dd/<br><br>**Conn. Data Privacy Act (Public Act 22-15)** mandates that certain businesses (data controllers and processors as defined by statute) implement reasonable security practices to protect personal information. **This law does not apply to government agencies.<br>Link: https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF |
| **Delaware** | |
| Rules of Professional Conduct | ABA Model Rules verbatim, except for **Rule 1.15** which adds further details about property in trust accounts.<br>Link: https://courts.delaware.gov/ODC/Digest/dlrpc.aspx |

| | |
|---|---|
| Ethics Opinions | **Opinion 2001-2 – Email Communication** endorses ABA opinions approving email transmission of confidential information because it is presumed to afford lawyers a reasonable expectation of privacy.<br>Link: http://media.dsba.org/ethics/pdfs/2001-2.pdf |
| Statutes | **Computer Security Breaches (Del. Code tit. 6, §§ 12B-100, *et. seq.*)** mandates that government agencies and businesses maintaining personal information must implement reasonable security procedures and practices to prevent unauthorize acquisition. Requires notice to and cooperation with any Delaware residents in the event of a security breach without unreasonable delay, but not more than 60 days following discovery of the security breach, unless the person suffering the breach determines, after an appropriate investigation, that the breach is unlikely to result in harm such as if the data was encrypted. Additional requirements if social security data/identifiers are subject of security breach.<br>Link: https://delcode.delaware.gov/title6/c012b/index.html |
| **District of Columbia** | |
| Rules of Professional Conduct | No practical differences from relevant ABA Model Rules, except **Rule 1.6** specifies that confidentiality is required for current, past and prospective clients, while this position was most likely only presumed under ABA.<br>Link: https://www.dcbar.org/for-lawyers/legal-ethics/rules-of-professional-conduct |
| Ethics Opinions | **Ethics Op. 281 (1998) - Electronic Mail** says that lawyers use of unencrypted e-mail is not a violation of the Rule 1.6 on confidentiality.<br>Link: https://www.dcbar.org/For-Lawyers/Legal-Ethics/Ethics-Opinions-210-Present/Ethics-Opinion-281 |
| Statutes | **Consumer Security Breach Notification Act (D.C. Code § 28–3851, *et seq.*)** mandates that a person or entity that owns, maintains or handles computerized personal information must implement reasonable security safeguards. Also, must notify consumers of a security breach (and Office of the Attorney General if more than 50 D.C. residents are affected) "in the most expedient time possible and without unreasonable delay." Additional requirements if the breach involved social security or tax identification numbers. **This law does not apply to government agencies.<br>Link: https://code.dccouncil.gov/us/dc/council/code/titles/28/chapters/38/subchapters/II |
| **Florida** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.6** comments endorse the goal of ABA Formal Opinion 477R (Securing Communications). **Rule 1.15** is heavily reduced to only require compliance with the Florida Bar Rules Regulating Trust Accounts.<br>Link: https://www-media.floridabar.org/uploads/2023/08/2023_02-AUG-RRTFB-Chap.4-8-21-2023-ADA-Complaint.pdf |

| | |
|---|---|
| | **Florida Standing Committee on Cybersecurity and Privacy Law** was created as a panel of experts dedicated to helping lawyers protect themselves, and their clients, from the constantly evolving threats. A Special Committee on AI Tools & Resources was also appointed to help Bar members keep abreast of the game-changing technology and thus comply with comment 8 for rule 1.1 on competency. They plan to release a more in-depth guidebook on cybersecurity for lawyers to protect themselves and their clients and hope to also make a presentation to circuit judges.<br>Link: https://www.floridabar.org/the-florida-bar-news/bars-committee-on-cybersecurity-privacy-law-aims-to-be-the-go-to-resource-for-lawyers/ |
| CLE Requirement | State bar mandates 3 credits of approved technology training in a range of topics.<br>Link: https://www.americanbar.org/events-cle/mcle/jurisdiction/florida/ |
| Ethics Opinions | **Ethics Op. 12-3- Cloud Computing** states lawyers should use "reasonable precautions" to ensure service providers maintain adequate confidentiality (relies on New York State Bar Ethics Opinion 842 (2010) and Iowa Ethics Opinion 11-10 (2011)).<br>Link: https://www.floridabar.org/etopinions/etopinion-12-3/<br><br>**Ethics Op. 12-2 - Access to Lawyer's Electronic File** permits a lawyer to provide their log-in credentials to an e-portal to trusted nonlawyer employees for the employees to file court documents that have been reviewed and approved by the lawyer (who remains responsible for the filing). The lawyer must properly supervise the nonlawyer, should monitor the nonlawyer's use of the e-portal, and should immediately change the lawyer's password if the nonlawyer employee leaves the lawyer's employ or shows untrustworthiness in use of the e-portal.<br>Link: https://www.floridabar.org/etopinions/etopinion-12-2/<br><br>**Ethics Op. 10-2- Confidentiality of Devices Containing Storage Media** advises that a lawyer who chooses to use devices that contain storage media (such as printers, copiers, scanners, and facsimile machines) should take reasonable steps to ensure that client confidentiality is maintained, and that the device is "sanitized" before disposal.<br>Link: https://www.floridabar.org/etopinions/etopinion-10-2/<br><br>**Ethics Op. 06-2- Metadata** states that a lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata.<br>Link: https://www.floridabar.org/etopinions/etopinion-06-2/<br><br>**Ethics Op. 06-1- Electronic File Storage** permits a law firm to store files electronically, unless a statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client's interests.<br>Link: https://www.floridabar.org/etopinions/etopinion-06-1/<br><br>**Ethics Op. 00-4 – Remote Services and Email Encryption** permits providing legal services online, but all rules of professional conduct apply to such services. Lawyers may communicate with a client using unencrypted e-mail under most circumstances. If a matter cannot be handled over |

| | |
|---|---|
| | the Internet because of its complexity, the matter must be declined. [Evaluate this guidance in light of subsequent ethics opinions.]<br>Link: https://www.floridabar.org/etopinions/etopinion-00-4/ |
| Statutes | **State Cybersecurity Act (2023 Fl. Stat. § 282.318)** spells out required cybersecurity measures for state agencies (per 2023 Fl. Stat. § 282.0041) and mandates that agencies produce and submit cyber incident response plans. Prosecutor offices likely are state agencies.<br>Link: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0200-0299/0282/Sections/0282.318.html<br><br>**Florida Information Protection Act (FIPA) (2023 Fl. Stat. §501.171)** requires government agencies and businesses that acquire or maintain computerized personal information to provide email or written notification of a security breach to individuals within the state. If breach impacts more than 500 residents, notice is required to Department of Legal Affairs. Notification not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement. the subject entity reasonably determines that the breach has not and will not likely result in identify theft or any other financial harm.<br>Link: https://m.flsenate.gov/Statutes/501.171 |
| **Georgia** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.6(c)** was not adopted. Also, **Rule 1.15** is subdivided into three categories, the first of which specifies preservation of general client property for six years after termination of representation, instead of five.<br>Link: https://www.gabar.org/barrules/georgia-rules-of-professional-conduct.cfm |
| Ethics Opinions | No relevant ethics opinions.<br><br>Link to Georgia Bar ethics opinions page:<br>https://www.gabar.org/Handbook/index.cfm#handbook/part10 |
| Statutes | **Identity Theft Law (Ga. Code § 10-1-910, *et seq.*)** requires state and local government agencies and businesses maintaining computerized personal information to provide notice of a security breach to Georgia residents within "most expedient time possible and without unreasonable delay." Notification is not dependent on risk of harm to the consumer.<br>Link: http://ga.elaws.us/law/10-1%7C34 |
| **Hawaii** | |
| Rules of Professional Conduct | ABA rules verbatim, except **Rule 1.15** specifies that client property shall be preserved for a period of 6 years after the termination of the representation.<br>Link: https://www.courts.state.hi.us/docs/court_rules/rules/hrpcond.htm |
| Ethics Opinions | No relevant ethics opinions.<br><br>Index of Hawaii ethics opinions: |

| | |
|---|---|
| | https://hawaiiethics.my.site.com/public/s/ethics-advice/Ethics_Advice__c/00B2K000009nHb3UAE |
| Statutes | **Security Breach Law (HRS § 487N-1, *et seq.*)** requires state and county government agencies and private businesses collecting computerized personal information to give notice of a security breach without unreasonable delay where illegal use of personal information has occurred, or is reasonably likely and creates a risk of harm. Statute covers physical personal information as well as electronic data.<br>Link: https://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/HRS_0487N-0001.htm |
| Idaho | |
| Rules of Professional Conduct | ABA rules verbatim.<br>Link: https://isb.idaho.gov/wp-content/uploads/irpc.pdf |
| Ethics Opinions | No relevant ethics opinions. Opinions not available online. |
| Statutes | **Identity Theft Law (Idaho Code § 28-51-104, *et seq.*)** requires state and local government agencies, individuals and commercial entities that own or license personal computerized information to provide notice to Idaho residents of a security breach in the "most expedient time possible without unreasonable delay." Notification not required if, after a reasonable and prompt investigation, the subject entity determines that misuse of resident's personal information has not and is not reasonably likely to occur or if the data was encrypted. Public agencies that have experienced a breach must also provide notice to Attorney General within 24 hours of discovery and to the Office of the Chief Information Officer within the Department of Administration.<br>Link: https://legislature.idaho.gov/statutesrules/idstat/Title28/T28CH51/ |
| Illinois | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.6** is slightly reorganized and reworded. **Rule 1.15** is entirely rewritten, but the only relevant difference is that there is no term of years specified for the retention of client property.<br>Link: https://www.illinoiscourts.gov/rules/supreme-court-rules?a=viii |
| Ethics Opinions | **Ethics Op. 19-04 (2019) - Outsourcing Support Services** permits lawyers to outsource legal and legal support services relating to a matter, provided the lawyer reasonably believes that the other lawyers' and nonlawyers' services will contribute to the competent and ethical representation of the client and reasonable measures are taken to protect client information and to avoid conflicts of interest. Disclosure to, and informed consent by, the client will ordinarily be required.<br>Link: https://www.isba.org/sites/default/files/ethicsopinions/Opinion%2019-04%20%28Outsourcing%29%28100119%29_0.pdf<br><br>**Ethics Op. 18-01 (2018) - Tracking Software Prohibited** prohibits a lawyer from using tracking software in emails or other electronic communications with other lawyers or clients in the |

| | |
|---|---|
| | course of representing a client without first obtaining the informed consent of each recipient to the use of such software. It is not reasonable to require that lawyers acquire special devices or programs to detect or defeat tracking software.<br>Link: https://www.isba.org/sites/default/files/ethicsopinions/Opinion%2018-01.pdf<br><br>**Ethics Op. 16-06 (2016) - Cloud Computing** permits lawyers to use cloud-based services in the delivery of legal services provided that the lawyer takes reasonable measures to ensure that the client information remains confidential and is protected from breaches. The lawyer's obligation to protect the client information does not end once the lawyer has selected a reputable provider. Similar to ABA Opinion 477R.<br>Link: https://www.isba.org/sites/default/files/ethicsopinions/16-06.pdf<br><br>**Ethics Op. 10-01 (2009) - Third-Party Technology Vendors** concludes that a law firm's utilization of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information.<br>Link: https://www.isba.org/sites/default/files/ethicsopinions/10-01.pdf<br><br>**Ethics Op. 96-10 (1997) – Email Encryption** (affirmed in 2010) permits lawyers to use unencrypted e-mail, including e-mail sent over the internet, to communicate with clients without violating Rule 1.6. Client consent is not required absent an extraordinarily sensitive matter. The expectation of privacy in an e-mail is no less reasonable than that in ordinary telephone calls.<br>Link: https://www.isba.org/sites/default/files/ethicsopinions/96-10.pdf |
| Statutes | **Illinois Personal Information Protection Act (815 ILCS §§ 530/1–530/50)** requires government agencies and businesses that possess Illinois residents' personal and other sensitive information to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. Also must notify affected residents of a security breach in the most expedient time possible without unreasonable delay. Notification not dependent on risk of harm to the consumer. Any state agency that suffers a breach involving more than 250 Illinois residents must notify the Attorney General.<br>Link:<br>http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815%C2%A0ILCS%C2%A0530/&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act.<br><br>**Illinois Biometric Information Privacy Act (740 ILCS §§ 14/1-99)** provides rules for private entities on the retention and destruction of biometric information. **This law does not apply to government agencies.<br>Link: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 |

| Indiana | |
|---|---|
| Rules of Professional Conduct | ABA rules verbatim, with additions to **Rule 1.15** on trust accounts.<br>Link: https://www.in.gov/courts/rules/prof_conduct/ |
| Ethics Opinions | No relevant ethics opinions.<br><br>Link to index of Indiana Bar ethics opinions:<br>https://cdn.ymaws.com/www.inbar.org/resource/resmgr/Ethics_Opinions/Index.pdf |
| Statutes | **Ind. Code Ann. § 4-1-11, *et seq*.** requires state agencies that own or license computerized personal information to notify affected Indiana residents of a security breach without unreasonable delay.<br>Link: https://iga.in.gov/laws/2021/ic/titles/4#4-1-11<br><br>**Ind. Code Ann. § 4-1-10, *et seq*.** prohibits state agencies from disclosing social security numbers unless under exceptions specified by statute.<br>Link: https://iga.in.gov/laws/2021/ic/titles/4#4-1-10<br><br>**Ind. Code Ann. § 24-4.9-1, *et seq*.**. requires individuals and businesses that own or license computerized personal information to implement and maintain reasonable security safeguards. Also must notify affected Indiana residents and Attorney General of a security breach without unreasonable delay, but within 45 days of discovery of breach of any electronic or other tangible medium if transferred from computerized data. Notification is not required if the breach has not and could not result in identity deception, identity theft, or fraud affecting an Indiana resident. Statute does not apply to personal information stored on a portable electronic device if access to that device is protected by encryption that has not been compromised or disclosed or is otherwise known to the unauthorized actor. **This law does not apply to state agencies of any branch.<br>Link: https://iga.in.gov/laws/2023/ic/titles/24#24-4.9<br><br>**Data Privacy Law (Senate Enrolled Act No. 5 (2023))** creates data privacy rights for consumers and requires controllers of consumer data to maintain and implement reasonable security practices. **This law does not apply to government agencies.<br>Link: https://iga.in.gov/pdf-documents/123/2023/senate/bills/SB0005/SB0005.05.ENRH.pdf |
| **Iowa** | |
| Rules of Professional Conduct | ABA rules verbatim, except **Rule 1.15** specifies retention of client property for six years.<br>Link: https://www.legis.iowa.gov/docs/publications/ICRC/32.pdf |
| Ethics Opinions | **Ethics Op. 15-01 (2015) – Email Communication** advises that a lawyer sending or receiving substantive communications with a client via e-mail or other electronic means must ordinarily warn the client about the risk of interception, including the use of a computer or other device, or e-mail account, to which a third party may gain access.<br>Link:<br>https://s3.amazonaws.com/membercentralcdn/sitedocuments/isba/isba/0965/2076965.pdf?AWSAccessKeyId=AKIAIHKD6NT2OL |

| | |
|---|---|
| | 2HNPMQ&Expires=1696634835&Signature=BvGUmQXoVnguF5UkRn%2FqPVBvhsI%3D&response-content-disposition=inline%3B%20filename%3D%22Iowa%20Ethics%20Op%2E%2015%2D01%2Epdf%22%3B%20filename%2A%3DUTF%2D8%27%27Iowa%2520Ethics%2520Op%252E%252015%252D01%252Epdf&response-content-type=application%2Fpdf<br><br>**Ethics Op. 14-01 (2014) – Computer Security** affirms Ethics Op. 11-01 following the 2014 announcement from Microsoft that it will no longer support the Windows XP operating system with the release of new security patches, but brings attention that systems or procedures that may have been secure before, may no longer be so due diligence standards may change.<br>Link:<br>https://s3.amazonaws.com/membercentralcdn/sitedocuments/isba/isba/0086/2156086.pdf?AWSAccessKeyId=AKIAIHKD6NT2OL2HNPMQ&Expires=1696634890&Signature=8oW4iyvrfvaAqLlkHD2Kd9INBBk%3D&response-content-disposition=inline%3B%20filename%3D%22Ethics%20Opinion%2014%2D01%2D1%2Epdf%22%3B%20filename%2A%3DUTF%2D8%27%27Ethics%2520Opinion%252014%252D01%252D1%252Epdf&response-content-type=application%2Fpdf<br><br>**Ethics Op. 11-01 (2011) – Cloud Computing** advises lawyers must use "due diligence" to assess the degree of protection that will be needed when using various forms of information technology, and to act accordingly. The opinion lists questions lawyers should ask in making this assessment.<br>Link:<br>http://205.209.45.153/iabar/IowaEthicsOpinions.nsf/b6868944e3311dd0872581100042934f/a092fcd35bb508e0872581100042b927?OpenDocument<br><br>**Ethics Op. 97-01 (1997) – Internet and Sensitive Material** states lawyers should obtain written consent from clients for any sensitive material that is transmitted via e-mail. This opinion pre-dates ABA Formal Opinion 99-413, which likely holds more weight on this issue. Ethics Op. 96-33 (1997) defines sensitive material.<br>Link:<br>http://205.209.45.153/iabar/IowaEthicsOpinions.nsf/b6868944e3311dd0872581100042934f/315d6205d531771e872581100042b88a?OpenDocument<br><br>**Ethics Op. 96-33 (1996)- Internet and Sensitive Material** says that if sensitive material is to be transmitted via e-mail, counsel must have written acknowledgment by the client of the risk of violation of DR 4-101 ( ". . . information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client."). The acknowledgment should include consent for communication on the Internet or non-secure Intranet or other forms of proprietary networks, or the communication must be encrypted or protected by password/firewall or other generally accepted equivalent security system.<br>Link:<br>http://205.209.45.153/iabar/IowaEthicsOpinions.nsf/b6868944e3311dd0872581100042934f/d1d9dca80afa4c6e872581100042b888?OpenDocument |
| Statutes | **Personal Information Security Breach Protection (Iowa Code §§ 715C.1, 715C.2)** requires government agencies, individuals and businesses that own or license computerized personal information provide notice of a security breach of personal information to Iowa residents in the "most expeditious manner possible without unreasonable delay." Notice not required if, after an appropriate investigation or consultation with the relevant federal, state, or local law enforcement agencies, the entity determines that there is no reasonable likelihood of financial |

| | |
|---|---|
| | harm to residents whose information has been acquired such as when it is encrypted, redacted or otherwise altered.<br>Link: https://www.legis.iowa.gov/docs/code/715c.pdf<br><br>**Iowa Act Relating to Consumer Data Protection (Senate File 262 (2023))** requires controllers and processors of personal data to implement reasonable data security practices. **This law does not apply to government agencies.<br>Link: https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF%20262 |
| **Kansas** | |
| Rules of Professional Conduct | ABA rules verbatim. except **Rule 1.15** adds specifications for preserving trust accounts.<br>Link: https://www.kscourts.org/KSCourts/media/KsCourts/Rules/2023-Rule-Book.pdf |
| Ethics Opinions | No relevant ethics opinions.<br><br>Link to index of Kansas ethics opinions:<br>https://www.kscourts.org/Judges/Judicial-Ethics-Advisory-Panel |
| Statutes | **Kansas Cybersecurity Act (Kans. Stat. §§ 75-5236, *et seq.*)** makes the heads of most state agencies in the executive branch responsible for the security of all data and information technology resources. Agencies must implement agency-wide information security program, among other detailed cybersecurity duties.<br>Link:<br>http://www.kslegislature.org/li/b2023_24/statute/075_000_0000_chapter/075_072_0000_article/075_072_0036_section/075_072_0036_k/<br><br>**Kansas Cybersecurity Act of 2022 (HB 2019)** requires any public entities with a significant cybersecurity incident to notify the Kansas Information Security Office ('KISO') within 12 hours after its discovery.<br>Link: www.kslegislature.org/li/b2023_24/measures/documents/hb2019_enrolled.pdf<br><br>**Kansas Consumer Information and Security Breach Law (Kans. Stat. §§ 50-7a01 – 04)** requires government agencies, individuals and businesses that own or license computerized personal information to give notice of a breach of electronic data in most expedient time possible without unreasonable delay. Notification not required if subject entity determines after a reasonable and prompt investigation that misuse of personal information has not and is not reasonably likely to occur, such as when encrypted or redacted.<br>Link:<br>http://www.kslegislature.org/li_2020/b2019_20/statute/050_000_0000_chapter/050_007a_0000_article/050_007a_0001_section/050_007a_0001_k/ |
| **Kentucky** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.6** has fewer exceptions to the prohibition against divulging confidential information. Also, the comments to the rules are more concise. |

| | |
|---|---|
| | Link: https://casetext.com/rule/kentucky-court-rules/kentucky-rules-of-the-supreme-court/practice-of-law/rule-scr-3130-kentucky-rules-of-professional-conduct |
| Ethics Opinions | **KBA E-446 (2018)- Cybersecurity** states that attorneys should implement cybersecurity measures to protect clients' personal information, and that attorneys have a qualified obligation to advise clients about cyberattacks against the law practice and/or breaches of security. Attorneys are permitted to use third party service providers to comply with these obligations but are responsible to ensure that they are complying. Predates ABA Formal Opinion 483, but very similar.<br>Link: https://www.kybar.org/resource/resmgr/ethics_opinions_(part_2)_/kba_e-446.pdf<br><br>**KBA E-437 (2014) – Cloud Computing** permits cloud computing if the attorney acts competently, supervises the cloud provider and communicates with the client about the use of the cloud services when necessary. Similar to ABA opinion 477R.<br>Link: https://www.kybar.org/resource/resmgr/Ethics_Opinions_(Part_2)_/kba_e-437.pdf<br><br>**KBA E-436 (2013) – File Retention** concludes that while there is no set time that a lawyer must retain a closed client file, it is a matter of good practice to retain a paper or electronic file for at least five years after the file has been closed. Even then, a lawyer should carefully evaluate whether the file contains items that the lawyer should retain for a longer time or whether special circumstances exist such that the file should be retained for a longer time.<br>Link: https://www.kybar.org/resource/resmgr/Ethics_Opinions_(Part_2)_/kba_e-436.pdf<br><br>**KBA E-403 (1998) – Email Encryption** says that absent unusual circumstances, lawyers may use e-mail, including unencrypted Internet e-mail, to communicate with clients.<br>https://cdn.ymaws.com/www.kybar.org/resource/resmgr/Ethics_Opinions_(Part_2)_/kba_e-403.pdf |
| Statutes | **Kentucky Rev. Stat. §§ 61.931- 61.933** mandates that all government agencies that maintain or process computerized personal information must implement, maintain and update reasonable security procedures and practices. Definition of government agencies incudes prosecutor offices. Agencies must follow notification procedures in the event of a security breach.<br>Link to § 61.931: https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43575<br>Link to § 61.932: https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43576<br>Link to § 61.933: https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43577<br><br>**Data Breach Notification Law (Ky. Rev. Stat. § 365.732)** requires individuals and business entities that maintain computerized personal information must notify affected individuals of a security breach within most expedient time possible without unreasonable delay. Notification not required if entity reasonably believes the breach has not caused and will not cause identity theft or fraud against any resident, such as if the personal information is encrypted or redacted. **This law does not apply to government agencies.<br>Link: https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43326 |
| Louisiana | |

| | |
|---|---|
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.1** mandates compliance with the minimum requirements of continuing legal education as prescribed by Louisiana Supreme Court rule (CLE requirements), instead of adopting it in a comment the way the ABA did. No other ABA comments adopted within or along any of the rules.<br>Link: https://www.ladb.org/Material/Publication/ROPC/ROPC.pdf |
| Ethics Opinions | **PUBLIC Opinion 19-RPCC-021 (2019) - Lawyers' Use of Technology** permits a lawyer's use of evolving technology so long as the lawyer considers the associated benefits and risks, and uses reasonable care both to protect client information and to assure that client data is reasonably secure and accessible by the lawyer. More specifics than ABA Formal Opinion 483. The opinion adds that "failure to use basic minimum standards for security, such as secure passwords, firewalls and encryption, may put a lawyer at risk of a potential violation…"<br>Link: https://www.lsba.org/documents/Ethics/EthicsOpinionLawyersUseTech02062019.pdf<br><br>**PUBLIC Opinion 06-RPCC-008 (2006) – Client File Retention** states that attorneys should use orderly and prudent procedures for retaining and discarding clients' personal information, including consideration of the sensitivity of material.<br>Link: https://www.lsba.org/documents/Ethics/06LSBARPCC008.pdf |
| Statutes | **Database Security Breach Notification Law (La. Rev. Stat. §§ 51:3071 – 3077)** requires government agencies and businesses that owns or license computerized personal information to implement and maintain reasonable data security and disposal procedures and practices. Must also notify affected residents of a security breach within the most expedient time possible and without unreasonable delay, but no later than 60 days. Notification not required if, after a reasonable investigation, the entity determines that there is no reasonable likelihood of harm to residents, such as if the personal information is redacted or encrypted. If notice to residents is required, the entity must notify the Consumer Protection Section of the Attorney General's office, including names of all Louisiana citizens affected by the breach. Notice to the Attorney General's office will be "timely" if received within 10 days of notice to residents.<br>Link: http://legis.la.gov/Legis/Law.aspx?d=322027 |
| **Maine** | |
| Rules of Professional Conduct | ABA rules verbatim, except **Rule 1.6** adds guidance about sharing confidential client information in the event of the sale of a law practice, and about counseling clients when circumstances may lead to permissible divulging of confidential information. **Rule 1.15** is reworded to give specific instructions on the retention of client files and records.<br>Link: https://www.mebaroverseers.org/regulation/maine_conduct_rules.html |
| Ethics Opinions | **Ethics Op. 220 (2019) - Cyberattack and Data Breach** endorses ABA Formal Opinion 483. It states that despite a lawyer's reasonable efforts to protect electronic data created and stored in the service of clients, if a third party defeats those efforts, the lawyer's obligations are to take reasonable action in order to stop or contain the attack or breach; to investigate and ascertain whether confidential information relating to clients has been, or may have been, compromised; to determine whether the representation of current clients has been, or may have been, significantly impacted or impaired; and to promptly notify current and former clients.<br>Link: http://www.mebaroverseers.org/attorney_services/opinion.html?id=1267989 |

| | |
|---|---|
| | **Ethics Op. 207 (2013) – Cloud Computing** permits cloud computing if appropriate safeguards are in place.<br>Link: http://www.mebaroverseers.org/attorney_services/opinion.html?id=478397<br><br>**Ethics Op. 195 (2008)- Email Encryption** permits the use of unencrypted email with appropriate safeguards.<br>Link: http://www.mebaroverseers.org/attorney_services/opinion.html?id=63338<br><br>**Ethics Op. 194 (2008)- Third-Party Technology Vendors** permits third-party electronic back-up and transcription services so long as appropriate safeguards are taken, including reasonable efforts to prevent the disclosure of confidential information, and an agreement with the vendor that contains "a legally enforceable obligation" to maintain the confidentiality of the client's information.<br>Link: https://www.mebaroverseers.org/attorney_services/opinion.html?id=86894 |
| Statutes | **Notice of Risk to Personal Data Act (Me. Rev. Stat. Tit. 10 §§ 1346 – 1350-B)** mandates state and municipal agencies, as well as individuals and businesses, that maintain computerized personal data to provide notice of a security breach to affected Maine residents as expediently as possible and without unreasonable delay, but not later than 30 days. For an entity that is not an "information broker" under the statute, notification is not required if, after a reasonable and prompt investigation, the entity determines there is no reasonable possibility that a resident's personal information has been or will be misused. If notice to residents is required, must also notify the appropriate state regulators within the Department of Professional and Financial Regulation, or, if not regulated by the Department, must notify the Attorney General.<br>Link: http://www.mainelegislature.org/legis/statutes/10/title10ch210-Bsec0.html |
| **Maryland** | |
| Rules of Professional Conduct | ABA rules verbatim, with limited exceptions not directly relevant to cybersecurity. **Rule 1.6**-Comment 18 was not adopted in its entirety, but the comment's guidance is substantially retained.<br>Link:<br>https://govt.westlaw.com/mdc/Browse/Home/Maryland/MarylandCodeCourtRules?guid=N29F342503A3311E69636A2C4C528971C&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default) |
| Ethics Opinions | No relevant ethics opinions.<br><br>Link to index of Maryland ethics opinions:<br>https://www.msba.org/site-search/?query=%20&page=5&configure%5BclickAnalytics%5D=true&refinementList%5BDataType%5D%5B0%5D=Ethics%20Opinion |
| Statutes | **Md. State Govt. Code § 10-135** requires government agencies that collect computerized personal information to implement and maintain reasonable cybersecurity and data disposal practices and procedures. Agencies that use third party services must ensure those services |

| | |
|---|---|
| | are using reasonable security practices. Agencies must also follow notice provisions in the event of a security breach.<br>Link: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gsg&section=10-1301&enactments=False&archived=False<br><br>**Commercial Law (Md. Code Ann., Com. Law §§ 14-3501, *et seq.*)** requires businesses that own or maintain computerized personal information implement reasonable security and data disposal procedures and practices. Must also give notice of a security breach to the Attorney General and affected Maryland residents as soon as reasonably practicable, but within no later than 45 days. Notification not required if the covered entity, as soon as a potential breach is discovered or made known, conducts a reasonable, prompt, and good faith investigation, and determines that misuse of personal information has not and is not likely to occur as a result of the breach. **This law does not apply to government agencies.<br>Link: https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gcl&section=14-3501&enactments=False&archived=False |
| Massachusetts | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. The comments to **Rule 1.6** specify that the confidentiality obligations apply to government lawyers who may disagree with the policy goals that their representation is designed to advance. **Rule 1.15** has several additional specifications for trust accounts and funds held for clients, as well as for determining how long to preserve client property.<br>Link: https://bbopublic.massbbo.org/web/f/rpc.pdf |
| Ethics Opinions | **Ethics Op. 12-03 (2012) - Electronic File Storage** outlines reasonable efforts to ensure that a cloud service provider's terms of use, privacy policies, practices and procedures are compatible with the lawyer's professional obligations.<br>Link: https://www.massbar.org/publications/ethics-opinions/ethics-opinion-article/ethics-opinions-2012-opinion-12-03<br><br>**Ethics Op. 05-04 (2005) – Third-Party Technology Vendors** permits lawyers' use of software and cloud computing, with reasonable efforts to ensure that the conduct of the cloud or software provider is compatible with the Rules of Professional Conduct. Considers cloud computing "impliedly authorized" by the client in order to provide representation.<br>Link: https://www.massbar.org/publications/ethics-opinions/ethics-opinion-article/ethics-opinions-2005-opinion-05-04<br><br>**Ethics Op. 00-1 (2000) - Email Encryption** permits a lawyer's use of unencrypted e-mail to engage in confidential communications, in usual circumstances.<br>Link: https://www.massbar.org/publications/ethics-opinions/ethics-opinion-article/ethics-opinions-2000-opinion-no-00-1 |
| Statutes | **Security Breach Law (Mass. Gen. Laws ch. 93 H §§ 1–6)** requires most government agencies to adopt rules and regulations to insure the security and confidentiality of personal information. This law also requires any type of agency or authority of the commonwealth to provide notice of breached personal information in electronic, paper or any other form, to affected |

| | |
|---|---|
| | Massachusetts residents, to the Attorney General and to the Director of Consumer Affairs and Business Regulation, "as soon as practicable and without unreasonable delay." Notification is not required if a breach does not create a substantial risk of identity theft or fraud against a resident such as if the confidential process or encryption key was not accessed or acquired.<br>Link: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h/Section1<br><br>**Personal Information Protection Standards** (**201 Mass. Code Regs. §§ 17.00-17.05**) creates a duty for government agencies, individuals and business that own or license computerized personal information to develop, implement and maintain a comprehensive information security program Duty applies to all agencies and authorities of the commonwealth.<br>Link: https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth/download#:~:text=The%20objectives%20of%20201%20CMR,to%20or%20use%20of%20such |
| Michigan | |
| Rules of Professional Conduct | Uses language from ABA Model Rules with some relevant refinements:<br>**Rule 1.1** is more precise in that it mandates that a lawyer shall not:<br>(a) handle a legal matter which the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it;<br>(b) handle a legal matter without preparation adequate in the circumstances; or<br>(c) neglect a legal matter entrusted to the lawyer.<br>**Rule 1.4** mandates that a lawyer may have to comply with reasonable requests for information from the client.<br>**Rule 1.6(d)** mandates that a lawyer shall exercise reasonable care to prevent employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client, except that a lawyer may reveal the information allowed by paragraph (c) through an employee.<br>Link: https://www.courts.michigan.gov/4a496f/siteassets/rules-instructions-administrative-orders/rules-of-professional-conduct/michigan-rules-of-professional-conduct.pdf |
| Ethics Opinions | **RI-388 (2023) - Safeguarding Digital Property** states that a lawyer's obligation to safeguard digital property under MRPC 1.S(d) are the same as other property entrusted to the lawyer. Where digital property is stored on a tangible medium, it is the tangible medium that must be safeguarded and not the underlying data. When the lawyer possesses the means to access the digital property, the obligation to safeguard the property extends only to the means of access.<br>Link: https://www.michbar.org/opinions/ethics/numbered_opinions/RI-388<br><br>**RI-381 (2020) - Cybersecurity Knowledge and Measures** states that lawyers have ethical obligations to understand technology (including cybersecurity), take reasonable steps to implement cybersecurity measures (adopted out of ABA Formal Opinion 483), supervise lawyers and other firm personnel to ensure compliance with duties relating to cybersecurity, and timely notify clients in the event of a material data breach (also adopted out of ABA Formal Opinion 483).<br>Link: https://www.michbar.org/opinions/ethics/numbered_opinions/RI-381 |

| | |
|---|---|
| Statutes | **Identity Theft Protection Act (Mich. Comp. Laws §§ 445.61, 445.63, 444.64, 445.72)** requires state agencies and businesses that own or license computerized personal data to provide notice of a data security breach to affected individuals without unreasonable delay. Notification not required if the entity determines that the breach has not or is not likely to cause substantial loss, injury, or identity theft to one or more Michigan residents, such as if encrypted or redacted information, provided that the encryption key is also not acquired. State agencies and businesses also must properly destroy personal information when removed from databases.<br>Link:<br>http://www.legislature.mi.gov/(S(t1qnbc53u0hayajurl0hwp55))/mileg.aspx?page=getObject&objectName=mcl-Act-452-of-2004 |
| Minnesota | |
| Rules of Professional Conduct | ABA rules verbatim, except **Rule 1.15** requires file preservation of client property for six years.<br>Link: https://www.revisor.mn.gov/court_rules/rule/prcond-toh/ |
| Ethics Opinions | **Ethics Op. 22 (2010) - Metadata** states that a lawyer must take reasonable steps in the generation, transmittal and receipt of documents containing metadata to prevent the inadvertent disclosure of confidential metadata.<br>Link: https://lprb.mncourts.gov/rules/LPRBOpinions/Opinion%2022.pdf<br><br>**Ethics Op. 19** (adopted 1999 and amended 2010) - **Communication via Technology** permits a lawyer to use technological means such as electronic mail (e-mail) and cordless and cellular telephones to communicate confidential client information without violating Rule 1.6 under certain conditions. E-mail without encryption may be used to transmit and receive confidential client information. Digital cordless and cellular telephones may be used by a lawyer to transmit and receive confidential client information when used within a digital service area. When the lawyer knows, or reasonably should know, that a client or other person is using an insecure means to communicate with the lawyer about confidential client information, the lawyer shall consult with the client about the confidentiality risks associated with inadvertent interception and obtain the client's consent.<br>Link: https://lprb.mncourts.gov/rules/LPRBOpinions/Opinion%2019.pdf |
| Statutes | **Government Data** (**Minn. Stat. § 13.01, *et seq.*)** sets out specific data security practices for all government entities, including prosecutors. Agencies must conduct a data inventory, follow limitations for collection of private or confidential data, establish appropriate security safeguards, and provide notice to affected individuals of a data security breach.<br>Link: https://www.revisor.mn.gov/statutes/cite/13.01<br><br>**Data Warehouses Law (Minn. Stat §§ 325E.61, 325E.64)** requires individuals and businesses that own or license computerized personal information to notify residents of a data security breach in the most expedient time possible without unreasonable delay. Notification is not dependent upon the risk of harm to the consumer. Statute does not apply to information that is encrypted or secured by another method of technology that makes the data unreadable or unusable, if the encryption key, password, or other means was not acquired.<br>Link: https://www.revisor.mn.gov/statutes/?id=325E.61 |

| | |
|---|---|
| **Mississippi** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. Comment to **Rule 1.1** suggests using a system of peer review in appropriate circumstances if one has been established to ensure reasonable measures are taken. **Rule 1.15** informs lawyers of their duty to follow the Mississippi Uniform Disposition of Unclaimed Property Act for the property of any clients with which they lost contact. It also mandates preservation of property for seven years after termination of representation.<br>Link: https://courts.ms.gov/research/rules/msrulesofcourt/rules_of_professional_conduct.pdf |
| Ethics Opinions | **Ethics Op. 263 (2020) – Cloud Computing** permits lawyers to use cloud-based electronic data storage systems to store client confidential information, but lawyers must undertake reasonable precautions in using those cloud-based systems.<br>Link: https://www.msbar.org/ethics-discipline/ethics-opinions/formal-opinions/263/<br><br>**Ethics Op. 259 (2012) - Metadata** requires an attorney to take reasonable precautions to make sure that confidential metadata is not inadvertently revealed by an electronic document. An attorney may not actively search for confidential metadata in an electronic document received from another attorney.<br>Link: https://www.msbar.org/ethics-discipline/ethics-opinions/formal-opinions/259/ |
| Statutes | **Enterprise Security Program (Miss. Code § 25-53-201)** creates a statewide cybersecurity program that all state agencies must follow. Makes the head of each state agency responsible for data security and IT resources for that agency, in compliance with rules and guidelines of the Mississippi Department of Information Technology Services.<br>Link: https://law.justia.com/codes/mississippi/2017/title-25/chapter-53/enterprise-security-program/section-25-53-201/<br><br>**Security Breach Notification Law (Miss. Code § 75-24-29)** requires a person who conducts business in the state and maintains data with personal information to give notice of a data security breach without unreasonable delay. Notification is not required if, after an appropriate investigation, the entity reasonably determines the breach will not likely result in harm to the affected residents, such as if its encrypted or rendered unreadable or unusable by any other method of technology. **This law does not apply to government agencies.<br>Link: https://law.justia.com/codes/mississippi/2020/title-75/chapter-24/subchapter-generalprovisions/section-75-24-29/ |
| **Missouri** | |
| Rules of Professional Conduct | ABA rules verbatim, except **Rule 1.15** is rewritten (only relevant difference is that preservation of client property is generally required for six years after termination of representation).<br>Link: https://www.courts.mo.gov/page.jsp?id=707 |
| Ethics Opinions | No relevant formal opinions.<br>Link to index of Missouri formal ethics opinions:<br>https://www.courts.mo.gov/page.jsp?id=11696 |

| | |
|---|---|
| | **Informal Op. 2021-12 (Rule 4-1.6) - Virtual Offices** permits attorneys' use of virtual offices.<br>Link to informal opinion index (by rule number):<br>https://mobar.org/public/ethics/InformalOpinionsIndex.aspx<br><br>**Informal Op. 2020-26 (Rule 4-1.6) - Actions for Potential Data Breaches** states that if a stolen electronic device contains, or provides potential access to, information related to the representation of clients or former clients, an attorney must take all steps reasonably necessary to prevent unauthorized access to the information. These steps include, but may not be limited to, deactivating the cell phone; taking appropriate steps to secure attorney's law firm network and/or data in offsite storage; changing all passwords that may be stored on the electronic device; and consulting with a qualified information technology professional if appropriate. An attorney must communicate with affected clients to the extent reasonably necessary to allow each client to make informed decisions about the representation. An attorney must comply with any applicable law requiring notice to affected persons regarding disclosure of their personal information. Attorneys must take all necessary steps to protect the funds in the client trust account from unauthorized transfers and should monitor the trust account closely. To address the stolen bar card, an attorney may contact the Office of Attorney Enrollment of the Supreme Court of Missouri. Attorneys may also consider taking steps to protect the security of Attorney's e-filing account with applicable courts and consulting Attorney's malpractice insurance carrier for additional advice.<br>Link to informal opinion index (by rule number):<br>https://mobar.org/public/ethics/InformalOpinionsIndex.aspx<br><br>**Informal Op. 2018-09 (Rule 4-1.6) – Cloud Computing** permits cloud computing if an attorney maintains competence and makes reasonable efforts to safeguard confidential information from inadvertent or unauthorized disclosure or access, as warranted by the particular facts and circumstances of each client's matter.<br>Link to informal opinion index (by rule number):<br>https://mobar.org/public/ethics/InformalOpinionsIndex.aspx<br><br>**Informal Op. 2012-01 (Rule 4-1.6) - Email Communication** states that the Rules of Professional Conduct do not require attorneys to use a disclaimer on e-mails sent to clients. As with any form of communication with clients, attorneys must take reasonable precautions to prevent the unintended interception of confidential information, as explained in Comments [15] and [16] to the Confidentiality of Information Rule (4-1.6). Special circumstances or the need to transmit highly sensitive information may require special security measures in order to comply with Rule 4-1.6. For further information about the use of e-mail for client communication, Attorneys may consult Informal Opinions 990007, 980137, 980029, 970010, and 970161.<br>Link to informal opinion index (by rule number):<br>https://mobar.org/public/ethics/InformalOpinionsIndex.aspx<br><br>**Informal Op. 990007 (Rule 4-1.6)- Email Communication** advises that determining whether e-mail communication is appropriate may depend on the setting in which the client will send and receive e-mail, as well as the nature of the particular communication. Any communication with the client regarding this subject should be in plain language, as much as possible, and should discuss the various ways in which e-mail might be intercepted or accessed by someone else. E- |

| | |
|---|---|
| | mail is not the same as other types of communications because it is so new that many people are not aware of the basic risks of interception through technology or access. Informal Opinions 980137, 980029, 970230 970161 and 970010, also address this topic.<br>Link to informal opinion index (by rule number):<br>https://mobar.org/public/ethics/InformalOpinionsIndex.aspx<br><br>**Informal Op. 980137 (Rule 4-1.6)- Informed Consent Regarding Technology Used for Communication** states that attorneys owe a duty to clients to advise of the risks of attorney/client communications through a technology about which many clients only have a rudimentary knowledge. This advice does not have to be technical in nature. The advice must be adequate to inform the client of the nature of the risk before the client makes the decision that it is acceptable to use that method of communication.<br>Link to informal opinion index (by rule number):<br>https://mobar.org/public/ethics/InformalOpinionsIndex.aspx |
| Statutes | **Security Breach Notification Law (Mo. Rev. Stat. § 407.1500)** requires government agencies, individuals and businesses that own or license computerized personal information to provide notice of a data security breach to residents without unreasonable delay. Notification is not required if, after an appropriate investigation or consulting with relevant law enforcement agencies, the entity determines the risk of identity theft or other fraud to residents is not reasonably likely to occur.<br>Link: http://revisor.mo.gov/main/OneSection.aspx?section=407.1500&bid=23329&hl= |
| Montana | |
| Rules of Professional Conduct | ABA Model Rules verbatim, but comments were not adopted.<br>Link: https://www.montanabar.org/Membership-Regulatory/Ethics-Resources/Professional-Conduct |
| Ethics Opinions | No relevant ethics opinions.<br><br>Link to index of Montana Bar ethics opinions: https://www.montanabar.org/Membership-Regulatory/Member-Resources/Ethics-Opinions |
| Statutes | **State Agency Protection of Personal Information (Mont. Code §§ 2-6-1501-1503)** requires state agencies that maintain computerized personal information to notify affected individuals of a security breach.<br>Link: https://leg.mt.gov/bills/mca/title_0020/chapter_0060/part_0150/sections_index.html<br><br>**Computer Security Breach Law (Mont. Code Ann. §§ 30-14-1704, 1705)** requires a person or business to provide notice of data security breach involving personal information without unreasonable delay. Notification is not required if the entity reasonably believes the breach has not and will not cause loss or injury to a Montana resident, such as if the personal information is encrypted. Must simultaneously submit an electronic copy of the consumer notification to the Attorney General's Consumer Protection Office and a statement providing the date and method of distribution of the notification. **This law does not apply to government agencies.<br>Link: http://leg.mt.gov/bills/mca/title_0300/chapter_0140/part_0170/sections_index.html |

| | |
|---|---|
| | **Montana Consumer Data Privacy Act (SB 384 (2023))** requires controllers of data containing personal information to maintain reasonable data security practices. **This law does not apply to government agencies.<br>Link: https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf |
| Nebraska | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules.<br>Link: https://supremecourt.nebraska.gov/supreme-court-rules/chapter-3-attorneys-and-practice-law/article-5-nebraska-rules-professional |
| Ethics Opinions | **Ethics Op. 19-01- Internet Communication and Cloud Computing** permits transmission of information relating to the representation of a client over the internet and allows for that information to be stored on, and accessed through, third-party, off-site servers (generically referred to as "the Cloud"), if the lawyer has undertaken reasonable efforts to: (1)prevent inadvertent or unauthorized access to that information; (2) maintain the confidentiality of the information; and (3) establish reasonable safeguards to ensure the information is protected from loss, breaches, business interruptions, and other risks created by advancements in technology.<br>Link: https://supremecourt.nebraska.gov/sites/default/files/ethics-opinions/Lawyer/19-01.pdf |
| Statutes | **Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 (Neb. Rev. Stat. §§ 87-801 to 807)** requires government agencies, individuals and businesses that own or license computerized personal information to give notice of a security breach to affected residents and to the Attorney General as soon as possible and without unreasonable delay. Notification is not required if, after a reasonable and prompt investigation, the entity determines that unauthorized use of the information has not occurred and is not likely to occur, such as if the information is encrypted, redacted, or otherwise altered to render the information unreadable, so long as the encryption key was not accessed or acquired.<br>Link: https://nebraskalegislature.gov/laws/statutes.php?statute=87-801 |
| Nevada | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. Comments to ABA rules were not adopted, but are referenced in Nevada ethics opinions.<br>Link: https://www.leg.state.nv.us/CourtRules/RPC.html |
| Ethics Opinions | **Formal Ethics Op. 33 (2006) - Third-Party Technology Vendors** advises that attorneys may use third-party data storage and other technology vendors. Attorneys must take reasonable precautions, such as obtaining the third party's agreement to maintain confidentiality, to prevent both accidental and unauthorized disclosure of confidential information.<br>Link: https://www.nvbar.org/wp-content/uploads/opinion_33.pdf |
| Statutes | **Security and Privacy of Personal Information Law (NRS §§ 603A, *et seq*.)** requires government agencies and businesses that collect or handle computerized personal information to maintain reasonable security measures as specified by the statute. Must also provide notice to residents |

| | |
|---|---|
| | of a security breach in the most expedient time possible and without unreasonable delay. Notification is not dependent upon risk of harm to the consumer. Can seek guidance and training from the Technological Crime Advisory Board.<br>Link: http://www.leg.state.nv.us/NRS/NRS-603A.html |
| New Hampshire | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules.<br>▪ **Rule 1.1** lists minimum requirements for legal competency and client services duties. A note from the New Hampshire Bar Association Ethics Commission says that ABA Comment 8 may be read to assume more time and resources than will typically be available to many lawyers. Realistically, a lawyer should keep reasonably abreast of readily determinable benefits and risks associated with applications of technology used by the lawyer, and benefits and risks of technology lawyers similarly situated are using.<br>▪ A note from the New Hampshire Bar Association Ethics Commission that precedes Comments 18 and 19 for **Rule 1.6**, states that "a lawyer is responsible for reasonably securing adequate protection of client confidences in data held or stored by others, including, e.g., offsite storage and 'cloud' storage." This guidance is similar to that of ABA Formal Opinion 483.<br>▪ **Rule 1.15** is rewritten to emphasize complying with the New Hampshire Supreme Court Rules and requires preservation of client property for six years.<br>Link: https://www.courts.nh.gov/new-hampshire-rules-professional-conduct |
| Ethics Opinions | **Ethics Op. 2012-13/04 - Cloud Computing** lists 10 issues lawyers need to consider to ensure that the use of cloud computing is consistent with their ethical obligations.<br>Link: https://www.nhbar.org/ethics/opinion-2012-13-04<br><br>**Ethics Op. 2008-09/04 - Disclosure, Review and Use of Metadata** states that lawyers who send or receive electronic materials share an ethical obligation to preserve confidential information relating to the representation of clients. It is impermissible for New Hampshire lawyers to seek to review or use metadata received from opposing counsel.<br>Link: https://www.nhbar.org/ethics/opinion-2008-09-04 |
| Statutes | **Right to Privacy (N.H. Rev. Stat. §§ 359-C:19, C:20, C:21)** requires government agencies, individuals and businesses that own or license computerized personal information to give notice of a security breach to residents and to the Attorney General or specific regulatory agency, as quickly as possible. Notification is not required if an entity determines that misuse of the personal information has not and is not reasonably likely to occur, such as if the personal information was encrypted.<br>Link to N.H. Rev. Stat. § 359-C:19:<br>http://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-19.htm<br>Link to N.H. Rev. Stat. § 359-C:20:<br>https://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-20.htm<br>Link to N.H. Rev. Stat. §§ 359- C:21:<br>https://www.gencourt.state.nh.us/rsa/html/XXXI/359-C/359-C-21.htm |

| New Jersey | |
|---|---|
| Rules of Professional Conduct | New Jersey has adapted the ABA Model Rules, but utilizes significant portions of the Model Rules' language.<br>▪ Paragraph (f) of the comments that follow **Rule 1.6** requires a lawyer to "act competently to safeguard information, including electronically stored 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 or entities who are participating in the representation of a client or who are subject to a lawyer's supervision." This guidance is similar to ABA Formal Opinion 483.<br>▪ **Rule 1.15** requires compliance with court rules and mandates preservation of client property for seven years after the even that they record.<br>Link (listed under "Part 1 Appendices (RPC)- Rules of Professional Conduct"): https://www.njcourts.gov/attorneys/rules-of-court |
| Ethics Opinions | **Ethics Op. 701 (2006)** - **Electronic Storage and Access of Client Files** says that attorneys must exercise reasonable care against the possibility of unauthorized access to client information, which requires (1) an enforceable obligation with the cloud provider to preserve confidentiality and security, and (2) use of available technology to guard against reasonably foreseeable attempts to infiltrate the data.<br>Link: https://njlaw.rutgers.edu/collections/ethics/acpe/acp701_1.html |
| Statutes | **Disclosure of breach of security to customers** (**N.J. Stat. Ann §§ 56:8-160-167)** requires public entities, individuals and businesses that compile or maintain computerized personal information to provide notice of a security breach to residents and the division of State Police in the Department of Law and Public Safety, in the most expedient time possible and without unreasonable delay. Notification is not required if the entity determines that misuse of the personal information is not reasonably possible.<br>Link: https://casetext.com/statute/new-jersey-statutes/title-56-trade-names-trade-marks-and-unfair-trade-practices/chapter-568/section-568-161-definitions-relative-to-security-of-personal-information<br><br>**Bill S297 (2023)** requires public agencies to report cybersecurity incidents (as defined in the statute) to the New Jersey Office of Homeland Security and Preparedness.<br>Link: https://pub.njleg.state.nj.us/Bills/2022/S0500/297_I1.PDF |
| **New Mexico** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.15** states that attorney should keep complete records of client property for a period of five years after termination of the representation.<br>Link: https://nmonesource.com/nmos/nmra/en/item/5699/index.do#!fragment/zoupio-_Toc135123997/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgEYBmAVg4CYuATiEB2AJQAaZNlKEIARUSFcAT2gByDZIiEwuBEpXqtOvQZABlPKQBC6gEoBRADJOAagEEAcgGEnkqRgAEbQpOzi4kA |
| Ethics Opinions | No relevant ethics opinions. |

| | |
|---|---|
| | Link to index of New Mexico ethics opinions: https://www.sbnm.org/Leadership/Committees/Ethics-Advisory-Committee/Ethics-Advisory-Opinions |
| Statutes | **Data Breach Notification Act (N. M. Stat. Ann. § 57-12C-1—57-12C-12)** requires a person who owns or licenses computerized personal information to maintain reasonable security practices and to give notice of a security breach to affected residents in most expedient time possible, but not later than 45 days. Notification not required if the covered entity, after an appropriate investigation, determines that the breach does not pose a significant risk of identity theft or fraud, such as if the personal information is encrypted, redacted or otherwise rendered unusable or unreadable. **This law does not apply to government agencies (§57-12C-12).<br>Link: https://nmonesource.com/nmos/nmsa/en/item/4423/index.do#!fragment/zoupio-_Toc146016633/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgEYAWANgAYOPHgGZhASgA0ybKUIQAiokK4AntADk6iREJhcCRcrWbtu-SADKeUgCE1AJQCiAGUcA1AIIA5AMKOJpGAARtCk7GJiQA |
| New York | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. Adopted Comment 8 to **Rule 1.1** that state competency includes familiarity with advances in technology, and also mandates (ii) keeping abreast of the benefits and risks associated with technology used to provide the client services or to store or transmit confidential information, and to (iii) engage in continuing study and education including that mandated by 22 N.Y.C.R.R. Part 1500 (CLE requirements).<br>Link: https://www.nycourts.gov/ad3/AGC/Forms/Rules/Rules%20of%20Professional%20Conduct%2022NYCRR%20Part%201200.pdf |
| CLE Requirement | The New York State Bar Association requires attorneys to obtain 1 CLE credit in cybersecurity, privacy and data protection per CLE cycle.<br>Link: https://www.americanbar.org/events-cle/mcle/jurisdiction/new-york/ |
| Ethics Opinions | **Ethics Op. 1019 (2014)- Remote Access to Electronic Files** permits law firms to give lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.<br>Link: https://nysba.org/ethics-opinion-1019/<br><br>**Ethics Op. 1020 (2014)- Cloud Computing** - Whether a lawyer to a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.<br>Link: https://nysba.org/ethics-opinion-1020/ |

| | |
|---|---|
| | **Ethics Op. 1025 (2014)** - **Virtual Law Offices** permits virtual law offices so long as lawyers act competently, including handling and access of client files. Lawyers also must maintain client confidentiality as related to all communications and electronic client file storage.<br>Link: https://nysba.org/ethics-opinion-1025/<br><br>**Ethics Op. 842 (2010)** – **Cloud Computing** permits outside online data storage, but outlines four requirements of reasonable care to ensure that the system is secure and that client confidentiality will be maintained.<br>Link: https://nysba.org/ethics-opinion-842/<br><br>**Ethics Op. 782 (2004)** - **Metadata** states that lawyers must exercise reasonable care to prevent the disclosure of confidences and secrets contained in metadata within documents they transmit electronically to opposing counsel or other third parties.<br>Link: https://nysba.org/ethics-opinion-782/<br><br>**Ethics Op. 749 (2001) - Examination of Electronic Documents** concludes that lawyers may not ethically use available technology to surreptitiously examine and trace e-mail and other electronic documents.<br>Link: https://nysba.org/opinion-749/<br><br>**Ethics Op. 709 (1998)** - **Use of Email** allows lawyers to use unencrypted Internet e-mail to transmit confidential information without breaching ABA Model Rule 1.6.<br>Link: https://nysba.org/opinion-709/<br><br>**Ethics Op. 680 (1996)- Electronic File Retention** permits a client's file to be stored electronically, except for documents that are required by the rules to be kept in original form. Lawyers should ensure that documents stored electronically cannot be inadvertently destroyed or altered, and that the records can be readily produced when necessary.<br>Link: https://nysba.org/opinion-680/ |
| Statutes | **NY CLS State Tech. Law § 208** requires state agencies (except the judiciary) that own or license computerized personal information to engage in a series of notification procedures in the event of a data security breach.<br>Link: https://www.nysenate.gov/legislation/laws/STT/208<br><br>**Notification of Unauthorized Acquisition of Private Information (N.Y. Gen. Bus. Law § 899-aa)** requires any person or business that owns or licenses computerized personal information to give notice of a security breach to New York residents, the Attorney General, the N.Y. Dept. of State, and State Police in the most expedient time possible, without unreasonable delay. Notification is not required if the breach was an inadvertent disclosure by persons authorized to access the information, and the entity reasonably determines the breach will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credential. **This law does not apply to government agencies.<br>Link: https://www.nysenate.gov/legislation/laws/GBS/899-AA |

| | |
|---|---|
| | **N.Y. Gen. Bus. Law § 899-bb** requires a person or businesses that owns or licenses computerized personal information to develop, implement and maintain reasonable data security safeguards as set forth in the statute. **This law does not apply to government agencies.<br>Link: https://www.nysenate.gov/legislation/laws/GBS/899-BB |
| North Carolina | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules.<br>Link: https://www.ncbar.gov/for-lawyers/ethics/rules-of-professional-conduct/index-to-the-rules-of-professional-conduct/ |
| CLE Requirement | North Carolina CLE requirements include 1 hour of technology training in every CLE cycle.<br>Link: https://www.americanbar.org/events-cle/mcle/jurisdiction/north-carolina/ |
| Ethics Opinions | **2011 Formal Ethics Op. 6 (2012) - Security Requirements for Use of Software** states attorneys must take steps to minimize the risk of inadvertent or unauthorized disclosure of confidential client information when using software that is accessed online. Mandatory security requirements are not provided because they would create a false sense of security in an environment where the risks are continually changing. Instead, due diligence and frequent and regular education are required. Several recommended security measures are listed.<br>Link: https://www.ncbar.gov/for-lawyers/ethics/adopted-opinions/2011-formal-ethics-opinion-6/<br><br>**2008 Formal Ethics Op. 1 (2009) - Use of Metadata** states that a lawyer must use reasonable care to prevent the disclosure of confidential client information hidden in metadata when transmitting an electronic communication. A lawyer who receives an electronic communication from another party or another party's lawyer must refrain from searching for and using confidential information found in the metadata embedded in the document.<br>Link: https://www.ncbar.gov/for-lawyers/ethics/adopted-opinions/2009-formal-ethics-opinion-1/<br><br>**2008 Formal Ethics Op. 5 (2008) - Internet File Storage and Access** advises that client files may be stored on a website accessible by clients via the internet provided the confidentiality of all client information on the website is protected. If the law firm chooses to use a system that allows clients to access and download their own files at the end of the representation, the confidentiality and security of each client's file must be protected. See Rules 1.6 and 1.15.<br>Link: https://www.ncbar.gov/for-lawyers/ethics/adopted-opinions/2008-formal-ethics-opinion-5/ |
| Statutes | **Statute on Protection from Security Breaches (G.S. §§ 75-61, 75-65)** requires businesses that own or license computerized personal information to give notice of a security breach to North Carolina residents and to the Attorney General Office's Consumer Protection Division without unreasonable delay. Notification is not required if illegal use has not and is not reasonably likely to occur, and the breach does not create a material risk of harm to an individual. **This law does not apply to government agencies (although NC Attorney General's website states that it does). |

| | |
|---|---|
| | Link: https://www.ncleg.gov/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_75/Article_2A.html |
| North Dakota | |
| Rules of Professional Conduct | ABA Model Rules verbatim.<br>Link: https://www.ndcourts.gov/legal-resources/rules/ndrprofconduct |
| Ethics Opinions | **Ethics Op. 99-03 (1999) - Online Data Backup** permits law firms to subscribe to an online data backup service, provided the law firm ensures that the security of the data transmission and the security of the data storage are adequate for the sensitivity of the records that are to be transmitted and stored.<br>Link: https://cdn.ymaws.com/www.sband.org/resource/resmgr/docs/for_lawyers/99-03.pdf<br><br>**Ethics Op. 97-09 (1997) - Email Encryption** allows lawyers to communicate with clients using unencrypted e-mail unless unusual circumstances warrant heightened security measures.<br>Link: https://cdn.ymaws.com/www.sband.org/resource/resmgr/docs/for_lawyers/97-09.pdf |
| Statutes | **N.D. Cent. Code §§ 54-50.1.01, *et seq.*** mandates most government agencies disclose cyber incidents (as defined by the statute) to the state Information Technology Department.<br>Link: https://www.ndlegis.gov/cencode/t54c59-1.pdf#nameddest=54-59p1-01<br><br>**Notice of Security Breach for Personal Information (N.D. Cent. Code §§ 51-30-01, *et seq.*)** requires a person who owns or licenses computerized personal information to provide notice of a security breach to North Dakota residents, as well as to the Attorney General if more than 250 residents are notified, in most expedient time possible and without unreasonable delay. Notification is not dependent on risk of harm to the consumer. **This law does not apply to government agencies.<br>Link: http://www.legis.nd.gov/cencode/t51c30.pdf?20141017130430 |
| Ohio | |
| Rules of Professional Conduct | ABA Model Rules verbatim.<br>Link: https://www.supremecourt.ohio.gov/pdf_viewer/pdf_viewer.aspx?pdf=909861.pdf&subdirectory=2021-1143%5CDocketItems&source=DL_Clerk |
| Ethics Opinions | **Op. 2017-05- Virtual Law Office** allows provision of legal services via a virtual office if the attorney maintains the requisite competence regarding the technology employed and uses reasonable efforts to prevent the inadvertent disclosure of client information.<br>Link: https://www.ohioadvop.org/wp-content/uploads/2017/03/Adv.-Op.-2017-5.pdf<br><br>**Informal Advisory Op. 2013-03 – Third-Party Online Storage Vendor** demands competence (1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering what special circumstances call for extra protection. Opinion also lists common security issues. |

| | |
|---|---|
| | Link: https://www.splice.net/wp-content/uploads/2017/09/OSBAInfAdvOp2013-03.pdf<br><br>**Op. 99-2- Email Encryption** states that a lawyer does not violate the duty to preserve confidences and secrets under DR 4-101 of the Ohio Code of Professional Responsibility by communicating with clients through electronic mail without encryption. An attorney must use his or her professional judgment in choosing the appropriate method of each attorney-client communication.<br>Link: https://www.ohioadvop.org/wp-content/uploads/2017/04/Op-99-002.pdf |
| Statutes | **Agency Disclosure of Security Breach of Computerized Personal Information Data (Ohio Rev. Code Ann. § 1347.12)** requires government agencies that own or license computerized personal information to notify affected individuals in the event of a security breach.<br>Link: https://codes.ohio.gov/ohio-revised-code/section-1347.12<br><br>**Private Disclosure of Security Breach of Computerized Personal Information Data (Ohio Rev. Code Ann. §§ 1349.19, 1349.191, 1349.192, 1354.01, *et seq.*)** requires individuals and businesses that own or license computerized personal information to give notice to Ohio residents in the most expedient time possible but no later than 45 days. Notification is not required if the entity reasonably believes that the breach has not and will not cause a material risk of identity theft or other fraud to any resident, such as if the personal information is encrypted, redacted or otherwise made unreadable or unusable. **This law does not apply to government agencies.<br>Link: http://codes.ohio.gov/orc/1349.19<br><br>**Ohio Rev. Code Ann. § 1345.01, *et seq.*** requires businesses that access, maintain or process personal information to create, maintain and comply with a written cybersecurity program as specified in the statute. **This law does not apply to government agencies.<br>Link: https://codes.ohio.gov/ohio-revised-code/section-1354.02 |
| Oklahoma | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules.<br>Link (rules are listed under Appendix 3-A):<br>https://www.oscn.net/applications/oscn/Index.asp?ftdb=STOKST05&level=1 |
| Ethics Opinions | No relevant ethics opinions.<br>Link to index of Oklahoma ethics opinions: https://www.okbar.org/wp-content/uploads/2018/10/Ethics-Topical-Index-6-12-14-3.pdf |
| Statutes | **Security Breach Notification Act (24 Okla. Stat. §§ 161—166)** requires government entities, individuals, and businesses that own or license computerized personal information to give notice of a security breach to affected Oklahoma residents in the most expedient time possible without unreasonable delay. Notification is not required if the entity reasonably believes that the breach has not caused and will not cause a resident to suffer identity theft or other fraud, such as if the personal information is encrypted, redacted or otherwise made unreadable or unusable.<br>Link: https://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=452235 |

| | |
|---|---|
| | **Okla. Stat. § 74-3113.1** requires government agencies that own or license computerized personal information to disclose security breaches and notify affected individuals.<br>Link: http://www.oklegislature.gov/osStatuesTitle.aspx |
| Oregon | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. Comments not adopted.<br>Link: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj-mIi86aeAAxWxjIkEHVgvA7gQFnoECBYQAQ&url=https%3A%2F%2Fwww.osbar.org%2F_docs%2Frulesregs%2Forpc.pdf&usg=AOvVaw19AZcs9wrF45JCqeY38qTf&opi=89978449 |
| Ethics Opinions | **Ethics Op. 2016-191- Electronic Files** permits lawyers to maintain electronic-only files and convert paper files to electronic form, however they should take reasonable steps to ensure the security and availability of electronic files documents. Limited exceptions for documents that are intrinsically significant or are valuable original paper documents.<br>Link: https://www.osbar.org/_docs/ethics/2016-191.pdf<br><br>**Ethics Op. 2011-188 – Third-Party Electronic Storage** lists suggestions for reasonable steps in maintaining confidentiality of client data when using third-party storage providers, and discusses the need for re-evaluation as technology advances.<br>Link: http://www.osbar.org/_docs/ethics/2011-188.pdf<br><br>**Ethics Op. 2011-187 – Disclosure of Metadata** requires reasonable competence to safeguard information relating to representation of a client contained in communications with others, including metadata. The opinion also gives more information on requirements when receiving inadvertently disclosed personal information and the metadata within it.<br>Link: https://www.osbar.org/_docs/ethics/2011-187.pdf |
| Statutes | **Consumer Information Protection Act (Or. Rev. Stat. §§ 646A.600–626)** requires government agencies, business and individuals that own or maintain computerized personal information to implement and maintain reasonable data security safeguards. Also must give notice to Oregon residents (and the Attorney General if more than 250 residents are affected) in the most expeditious time possible without unreasonable delay, but no later than 45 days after discovery of a security breach. Notification not required if, after an appropriate investigation or consultation with relevant federal, state, or local law enforcement agencies, the entity reasonably determines that residents have not and are unlikely to suffer harm as a result of the breach, such as if the personal information is encrypted, redacted or otherwise made unreadable or unusable.<br>Link: https://www.oregonlegislature.gov/bills_laws/ors/ors646a.html |
| Pennsylvania | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules.<br>Link: https://www.padisciplinaryboard.org/Storage/media/pdfs/20230411/202120-rpc2023-04-11.pdf |

| | |
|---|---|
| Ethics Opinions | **Formal Op. 2022-500 - Storage of Client Information on Smartphones** says that if a lawyer stores information governed by Rule 1.6 on a smartphone, then the lawyer must take steps to prevent access to or disclosure of the information. Consequently, a lawyer may not consent to share the information with a smartphone app unless the lawyer concludes that no human being will view that information, and that the information will not be sold or transferred to additional third parties, without the client's consent.<br>Link: https://www.pabar.org/Members/catalogs/Ethics%20Opinions/Formal/F2022-500.pdf<br><br>**Formal Op. 2022-400** - **Email Communication** sets out the security considerations that must be addressed if an attorney wants to communicate information relating to the representation of a client through email.<br>Link: https://www.pabar.org/Members/catalogs/Ethics%20Opinions/Formal/F2022-400.pdf<br><br>**Formal Op. 2020-300** – **Working Remotely** permits lawyers to work remotely if they consider the security and confidentiality of their procedures and systems. This obligation includes protecting computer systems and physical files and ensuring that the confidentiality of client telephone and other conversations and communications remain protected.<br>Link: https://www.pabar.org/Members/catalogs/Ethics%20Opinions/Formal/F2020-300.pdf<br><br>**Formal Op. 2020-100** – **Email Communications with Opposing Counsel** sets out precautions to take when divulging attorney client confidential information and privileged information if communicating via email with opposing counsel and to avoid including their clients on the same email.<br>Link: https://www.pabar.org/Members/catalogs/Ethics%20Opinions/Formal/F2020-100.pdf<br><br>**Formal Op. 2011-200** - **Precautions with Cloud Services** advises reasonable safeguards for using cloud service providers (suggests over 30 precautions) but also mentions that some information may be too important to risk inclusion in cloud services.<br>Link: http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf |
| Statutes | **Breach of Personal Information Notification Act (73 P.S. §§ 2301–2329)** requires state agencies, individuals and businesses that maintain, store or mange computerized personal information to use encryption and take other reasonable steps to secure this data. Must also give notice of a security breach to affected Pennsylvania residents without unreasonable delay, unless the entity reasonably believes that the breach has not and will not cause loss or injury to any resident, such as if the personal information is encrypted, redacted or otherwise made unreadable or unusable.<br>Link:<br>https://govt.westlaw.com/pac/Browse/Home/Pennsylvania/UnofficialPurdonsPennsylvaniaStatutes?guid=N9B3F41908C4F11DA86FC8D90DD1949D4&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default) |
| Rhode Island | |
| Rules of Professional Conduct | ABA Model Rules verbatim, except did not adopt subsection (c) or Comment 18 of **Rule 1.6**. **Rule 1.15** requires preserving client property for seven years. |

| | |
|---|---|
| | Link: https://www.courts.ri.gov/AttorneyResources/ethicsadvisorypanel/PDF/EthicsArticle5.pdf#search=breach |
| Ethics Opinions | No relevant ethics opinions.<br>Link to index of Rhode Island ethics opinions: https://www.courts.ri.gov/AttorneyResources/ethicsadvisorypanel/PDF/EthicsIndex.pdf |
| Statutes | **Identity Theft Protection Act of 2015 (R.I. Gen Laws §§ 11-49.3-2 to 11-49.3-6)** requires government agencies that store, collect or use personal information to implement and maintain a risk-based information security program as specified in the statute. Must also give notice of a breach of personal information, in paper or electronic form, to affected Rhode Island residents, in the most expedient time possible, but no later than 45 days. Notification not required if breach or disclosure of personal information does not pose a significant risk of identity theft to any resident, or if its encrypted.<br>Link: http://webserver.rilin.state.ri.us/Statutes/TITLE11/11-49.3/INDEX.HTM |
| South Carolina | |
| Rules of Professional Conduct | No relevant practical differences from ABA Model Rules.<br>Link (listed under Rule 407): http://www.sccourts.org/courtReg/index.cfm |
| Ethics Opinions | **Ethics Op. No. 1997-08 - Email Communication** states that because there is a reasonable expectation of privacy when sending confidential information by e-mail, communicating client confidences via email does not violate Rule 1.6 (Confidentiality).<br>Link: https://www.scbar.org/lawyers/legal-resources-info/ethics-advisory-opinions/eao/ethics-advisory-opinion-97-08/ |
| Statutes | **Breach of Security of State Agency Data (S.C. Code § 1-11-490)** requires government agencies that own or license computerized personal identifying information to disclose a security breach and notify affected individuals in the most expedient time possible and without unreasonable delay.<br>Link: https://www.scstatehouse.gov/code/t01c011.php<br><br>**Breach of Security of Business Data (S.C. Code. § 39-1-90)** requires businesses that own or license computerized personal identifying information to give notice of a security breach to affected South Carolina residents in the most expedient time possible and without unreasonable delay. Notification is not required if the entity reasonably believes that illegal use has not and is not reasonably likely to occur, and the use of the information does not create a material risk of harm to the resident, such as if the personal information is encrypted, redacted or otherwise made unreadable or unusable. **This law does not apply to government agencies.<br>Link: http://www.scstatehouse.gov/code/t39c001.php |

| South Dakota | |
|---|---|
| Rules of Professional Conduct | No relevant practical differences from ABA Model Rules. No comments were adopted.<br>Link: https://sdlegislature.gov/Statutes/16-18-A |
| Ethics Opinions | No relevant ethics opinions.<br>Link to index of South Dakota ethics opinions: https://www.statebarofsouthdakota.com/ethics-opinions/ |
| Statutes | **Identity Crimes (S.D. Codified Laws §§ 22-40-19 to 26)** requires businesses and individuals that own or license computerized personal information to give notice of a security breach to affected South Dakota residents (and to the Attorney General if more than 250 residents are notified) not later than 60 days. Notification not required if the entity, after an appropriate investigation and notice to the Attorney General, reasonably determines that the breach will not likely result in harm to the affected persons. Statute does not apply to information that is encrypted or otherwise rendered unusable, unreadable, or indecipherable, as long as the encryption key is not acquired, or in accordance with the Federal Information Processing Standard 140-2. **This law does not apply to government agencies.<br>Link:<br>http://sdlegislature.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=StatuteChapter&Statute=22-40 |
| **Tennessee** | |
| Rules of Professional Conduct | Some re-organization, but no relevant practical differences from ABA Model Rules.<br>Link: https://www.tncourts.gov/rules/supreme-court/8 |
| Ethics Opinions | **Formal Ethics Op. 2023-F-170 (2023) - Credit Card Payments and Payment Platforms** permits lawyers accepting credit card payments to use payment processing services such as PayPal or Venmo, so long as the lawyer ensures compliance with applicable Tennessee RPC regarding confidentiality, how credit card transaction fees will be treated and the security of client trust funds.<br>Link: https://docs.tbpr.org/feo-2023-f-170.pdf<br><br>**Formal Ethics Op. 2015-F-159 (2015) - Cloud Computing** says a lawyer may ethically store confidential client information in "the cloud" if the lawyer takes reasonable care to assure that: (1) all such information or materials remain confidential; and (2) reasonable safeguards are employed to ensure that the information is protected from breaches, loss, and other risks. Due to rapidly changing technology, the Board does not attempt to establish a standard of care, but instead offers guidance from other jurisdictions. Informal opinions do not get published but instead get sent to person making the inquiry.<br>Link: https://www.tbpr.org/ethic_opinions/2015-f-159 |
| Statutes | **Release of Personal Consumer Information (Tenn. Code § 47-18-2107)** requires government agencies, individuals, and businesses that own or license computerized personal information to provide notice of a security breach to affected Tennessee residents no later than 45 days from |

| | |
|---|---|
| | the discovery or notification of a breach, regardless of whether there is a risk of harm for the consumer.<br>Link: https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=612c9960-987f-4cd0-bd37-8860eca77097&nodeid=ABVAAUAAVAAH&nodepath=%2fROOT%2fABV%2fABVAAU%2fABVAAUAAV%2fABVAAUAAVAAH&level=4&haschildren=&populated=false&title=47-18-2107.+Release+of+personal+consumer+information.&config=025054JABlOTJjNmIyNi0wYjI0LTRjZGEtYWE5ZC0zNGFhOWNhMjFlNDgKAFBvZENhdGFsb2cDFQ14bX2GfyBTaI9WcPX5&pddocfullpath=%2fshared%2fdocument%2fstatutes-legislation%2furn%3acontentItem%3a4X8K-XB40-R03J-K1K5-00008-00&ecomp=f38_kkk&prid=ae167118-3d03-4a8c-af3c-83c6191bfd5e<br><br>**Tenn. Code § 8-4-119 –** State agencies must notify the comptroller of the treasury of any confirmed or suspected unauthorized acquisition of computerized data or breach of security system.<br>Link: https://advance.lexis.com/documentpage/?pdmfid=1000516&crid=709701b0-09e6-4969-a164-a37ab221d99b&nodeid=AAIAAEAABAAT&nodepath=%2FROOT%2FAAI%2FAAIAAE%2FAAIAAEAAB%2FAAIAAEAABAAT&level=4&haschildren=&populated=false&title=8-4-119.+Report+to+comptroller+of+treasury+of+government+fraud.&config=025054JABlOTJjNmIyNi0wYjI0LTRjZGEtYWE5ZC0zNGFhOWNhMjFlNDgKAFBvZENhdGFsb2cDFQ14bX2GfyBTaI9WcPX5&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A560C-WWB0-R03K-P21R-00008-00&ecomp=f38_kkk&prid=1ebbe805-18ab-4aae-92e0-ec985d915ffa<br><br>**Tennessee Information Privacy Act (SB 0073 (2023))** requires data controllers and processors to maintain reasonable data security practices. **This law does not apply to government entities.<br>Link: https://www.capitol.tn.gov/Bills/113/Amend/HA0348.pdf |
| **Texas** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. The rules are slightly re-numbered. Comment 8 to **Rule 1.1** on maintaining competency was adopted in part. **Rule 1.6(c)** was not adopted.<br>Link:<br>https://www.texasbar.com/AM/Template.cfm?Section=Home&Template=/CM/ContentDisplay.cfm&ContentID=27271 |
| Ethics Opinions | **Ethics Op. 680 (2018) - Cloud Computing** concludes a lawyer may use a cloud-based electronic data storage system or cloud-based software document preparation system to store client confidential information or prepare legal documents. However, lawyers must remain alert to the possibility of data breaches, unauthorized access, or disclosure of client confidential information and undertake reasonable precautions in using those cloud-based systems.<br>Link: https://www.legalethicstexas.com/resources/opinions/opinion-680/<br><br>**Ethics Op. 665 (2016) – Metadata** requires lawyers to take reasonable measures, as appropriate for the factual circumstances, to avoid the transmission of confidential information embedded in electronic documents, including the employment of reasonably available technical means to remove such metadata before sending such documents to persons other than the lawyer's client. A Texas lawyer is required to avoid misleading or fraudulent use of information the lawyer may obtain from the metadata. In the absence of specific governing provisions, a lawyer who is considering the proper course of action regarding confidential information in metadata contained in a document transmitted by opposing counsel should determine whether the |

| | |
|---|---|
| | possible course of action poses material risks to the lawyer's client and if so explain them to the client so they can make confirmed decisions on the communication used in representation.<br>Link: https://www.legalethicstexas.com/resources/opinions/opinion-665/ |
| Statutes | **Tex. Gov. Code § 2054.603** requires state agencies and local governments that own or license computerized personal or other confidential information to comply with the notification requirement of Section 521.053 (see below), as well as notify the Texas Department of Information Resources.<br>Link: https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm<br><br>**Identity Theft Enforcement and Protection Act (Tex. Bus. & Com. Code §§ 521.002, 521.053, 521.151, 521.152)** requires a business holding computerized personal information to implement and maintain reasonable security procedures, including destruction of records. Must also give notice of a security breach to affected Texas residents (and to the Attorney General if more than 250 residents are notified) as quickly as possible, but no later than 60 days after breach is determined, regardless of whether there is a risk of harm for the consumer. **This law does not apply to government agencies.<br>Link: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.002<br><br>**Disposal of Business Records (Tex. Bus. & Com. Code §§ 72.002, 72.004)** directs businesses to properly dispose of digital records containing personal information. **This law does not apply to government agencies.<br>Link: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.72.htm |
| **Utah** | |
| Rules of Professional Conduct | ABA Model Rules verbatim, but did not adopt any comments.<br>Link: https://parkcitybar.org/sites/default/files/Utah%20State%20Bar%20-%202017%20Rules%20of%20Professional%20Conduct.pdf |
| Ethics Opinions | **Ethics Op. 00-01- Email Encryption** permits using unencrypted internet e-mail to transmit client confidential information in ordinary circumstances, so long as there is a reasonable expectation of confidentiality like there normally is when using landline telephone, fax and ordinary mail.<br>Link: https://www.utahbar.org/wp-content/uploads/2022/12/2000-01.pdf |
| Statutes | **Protection of Personal Information Act (Utah Code §§ 13-44-101 – 301)** requires a person who maintains computerized personal information to implement and maintain reasonable security and disposal procedures as specified in the statute. Must also provide notice of a security breach to affected Utah residents in most expedient time possible without unreasonable delay. Notification not required if, after a reasonable and prompt investigation, the covered entity determines that the personal information has not or will not be misused for identity theft or fraud. Statute does not apply to information that is encrypted or otherwise protected by another method that renders the data unreadable or unusable. **This law does not apply to government agencies.<br>Link: https://le.utah.gov/xcode/Title13/Chapter44/13-44.html |

| | |
|---|---|
| | **Utah Code §§ 78B-4-701, *et seq.*** offer an affirmative defense to businesses sued for security breach if followed a written cybersecurity program as specified in the statute.<br>Link:<br>https://le.utah.gov/xcode/Title78B/Chapter4/78B-4-P7.html?v=C78B-4-P7_2021050520210505<br><br>**Utah Consumer Privacy Act (Utah S.B. 227)** creates data security requirements for controllers and processors of data containing personal information. **This law does not apply to government entities.<br>Link: https://le.utah.gov/~2022/bills/static/SB0227.html |
| **Vermont** | |
| Rules of Professional Conduct | ABA Model Rules verbatim, except **Rule 1.6** omits some details on the reasonableness of safeguarding efforts for confidential information. Also, **Rule 1.15** mandates preserving client property for six years, instead of five.<br>Link:<br>https://www.vermontjudiciary.org/sites/default/files/documents/VermontRulesofProfessionalConduct.pdf |
| Ethics Opinions | **Advisory Ethics Op. 2010-6 (2011) - Selecting a Cloud Provider** advises that attorneys can use cloud computing and similar services if they take reasonable precautions to protect the confidentiality and ensure access to client materials. Lists the measures required for "due diligence" in selecting and using cloud providers.<br>Link: https://www.vtbar.org/wp-content/uploads/2021/03/10-06.pdf<br><br>**Ethics Op. 2009-1 (2009) - Metadata** advises lawyers to scrub metadata when sending client information and does not prohibit receiving lawyers from reviewing files to uncover metadata. With the adoption of Rule 4.4(b), Vermont lawyers must notify opposing counsel if they receive documents that they know or reasonably should know were inadvertently disclosed.<br>Link: https://www.vtbar.org/wp-content/uploads/2021/03/09-01.pdf<br><br>**Ethics Op. 1997-5 (1997)** - **Email Encryption** allows lawyers to use unencrypted internet e-mail to transmit confidential information without breaching the duty of confidentiality under state analog to ABA Model Rule 1.6<br>Link: https://www.vtbar.org/wp-content/uploads/2021/03/97-05-2.pdf |
| Statutes | **Notice of Security Breaches (9 V.S.A. §§ 2430, 2435)** requires government agencies, businesses and individuals that collect or broker computerized personal identifying information to provide notice of a security breach within in most expedient time possible and without unreasonable delay, but not more than 45 days from discovery of breach. Notification is not required if the entity establishes that misuse of the personally identifiable information or login credentials is not reasonably possible.<br>Link: http://legislature.vermont.gov/statutes/chapter/09/062 |
| **Virginia** | |

| | |
|---|---|
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.1** is verbatim for ABA, however the comments add details regarding competency with evolving technology.<br>Link: https://vsb.org/Site/Site/about/rules-regulations/rpc-part6-sec2.aspx |
| Ethics Opinions | **Ethics Op. 1872 (2013) – Virtual Office and Cloud Computing** permits the use of virtual law offices relying on services such as cloud computing, so long as the attorney exercises care in the selection of vendors and instructs vendors to preserve the confidentiality of information.<br>Link: https://www.vacle.org/opinions/1872.htm |
| Statutes | **Breach of Personal Information Notification (Va. Code Ann. § 18.2-186.6)** requires government agencies, individuals and businesses that own or license computerized personal information to provide notice of a security breach to affected Virginia residents and to the Attorney General without unreasonable delay. Notification is not required if the subject entity reasonably believes that the data is encrypted and the breach has not caused and will not cause identity theft or other fraud to any resident.<br>Link: http://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/<br><br>**Breach of Medical Information (Va. Code Ann. § 32-127.1:05)** directs government agencies holding personal medical information to disclose a security breach unless the entity reasonably believes that the data is encrypted and the breach has not caused and will not cause identity theft or other fraud to any resident.<br>Link: https://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05/<br><br>**Virginia Consumer Data Protection Act (Va. Code Ann. §§ 59.1-575 – 59.1-585)** mandates reasonable data security practices for certain businesses that control or process personal information. **This law does not apply to government entities.<br>Link: https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-575/ |
| Washington | |
| Rules of Professional Conduct | Adopts much of the ABA Model Rules and associated Comments, but with changes and revisions not relevant to cybersecurity issues.<br>Link: https://www.courts.wa.gov/court_rules/?fa=court_rules.list&group=ga&set=RPC |
| Ethics Opinions | **Ethics Op. 201601 (2022)- Virtual Offices and Cloud Computing** covers ethical considerations for virtual offices and using cloud services, including technological competency and measures to preserve confidentiality of client representation.<br>Link: https://ao.wsba.org/print.aspx?ID=1700<br><br>**Ethical Op. 2217 (2012) - Use of Employer Provided Technology** concludes that a lawyer has an obligation to advise the client that confidentiality may be jeopardized when the client is using an employer-provided computer or email account.<br>Link: https://ao.wsba.org/print.aspx?ID=1668 |

| | |
|---|---|
| | **Ethical Op. 2216 (2012)** – **Metadata** discusses the ethical responsibility of protecting metadata contained in documents transmitted and received, and advises the ethical risks of using software to recover such metadata that is not readily accessible.<br>Link:: https://ao.wsba.org/print.aspx?ID=1664<br><br>**Ethics Op. 2215 (2012)** – **Third-Party Technology Vendors** suggests best practices for lawyers storing confidential client data with third-party vendors.<br>Link: https://ao.wsba.org/print.aspx?ID=1662 |
| Statutes | **Personal Information- Notice of Security Breaches (Wash. Rev. Code §§ 42.56.001, 42.56.590)** requires government agencies that own or license computerized personal information to disclose a security breach and notify affected parties unless the data is encrypted or the breach is not reasonably likely to subject consumers to a risk of harm.<br>Link: http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590<br><br>**Personal Information - Notice of Security Breaches (Wash. Rev. Code §§ 19.255.005–040)** requires persons or businesses that own or license computerized data that includes personal information to give notice of a security breach to affected Washington residents in the most expedient time possible without unreasonable delay, no more than 30 days after discovery. Notice is not required if the breach is not reasonably likely to subject consumers to a risk of harm.<br>Link: https://apps.leg.wa.gov/rcw/default.aspx?cite=19.255 |
| **West Virginia** | |
| Rules of Professional Conduct | ABA Model Rules verbatim.<br>Link: http://www.courtswv.gov/legal-community/court-rules/professional-conduct/contents.html |
| Ethics Opinions | **L.E.O. 2012-01- Electronic File Storage** permits electronic file storage so long as attorneys ensure the confidentiality and integrity of the data, and its accessibility to the client.<br>Link: http://www.wvodc.org/pdf/leo2012.pdf |
| Statutes | **West Virginia Consumer Credit and Protection Act (WV Code § 46A-2A-101 to 105)** requires government agencies, individuals, and businesses that own or license computerized personal data to give notice of a security breach to affected West Virginia residents without unreasonable delay, unless the entity reasonably believes that the breach has not and will not cause identity theft or other fraud to a West Virginia resident.<br>Link: http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=46a&art=2A#2A |
| **Wisconsin** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. All ABA comments are adopted. **Rule 1.15** specifies that client files must be retained for six years instead of five.<br>Link: https://www.wicourts.gov/courts/offices/docs/olrscr20annotated.pdf |

| | |
|---|---|
| Ethics Opinions | **Op. EF-21-02- Working Remotely** permits lawyers to work remotely, concluding that with it becoming the norm, lawyers must develop new skills and knowledge to continue to comply with their core responsibilities. The opinion also discusses general guidance on cybersecurity measures, training and supervising both attorneys and non-attorneys at the firm and how to prepare clients.<br>Link: https://www.wisbar.org/formembers/ethics/Ethics%20Opinions/EF-21-02%20Working%20Remotely.pdf<br><br>**Op. EF-15-01- Cloud Computing** permits lawyers to use cloud computing as long as they use reasonable efforts to adequately address the risks associated with it. To determine what efforts are reasonable, lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication, and encryption for information stored both in the cloud and on the ground. Lawyers should also understand the dangers of using public Wi-Fi and file sharing sites. Lawyers who outsource cloud computing services should understand the importance of selecting a provider that uses appropriate security protocols. Lawyers should also understand the importance of regularly backing up data and storing data in more than one place. A lawyer may consult with someone who has the necessary knowledge to help determine what efforts are reasonable.<br>Link: https://www.wisbar.org/formembers/ethics/Ethics%20Opinions/EF-15-01%20Cloud%20Computing%20Amended.pdf |
| Statutes | **Data Breach Notification Law (Wis. Stat. § 134.98, *et seq.*)** requires certain government entities (see definition) and businesses that maintain or license computerized personal information to provide notice of security breach to a Wisconsin consumer within a reasonable time not exceeding 45 days, by mail or any method previously agreed to. Notice not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the consumer.<br>Link: http://docs.legis.wisconsin.gov/statutes/statutes/134/98 |
| **Wyoming** | |
| Rules of Professional Conduct | Some changes, but no practical differences from relevant ABA Model Rules. **Rule 1.15A** was added to specify retention of client files.<br>Link: https://www.courts.state.wy.us/wp-content/uploads/2017/05/RULES-OF-PROFESSIONAL-CONDUCT-FOR-ATTORNEYS-AT-LAW-8_05.pdf |
| Ethics Opinions | No reporting of ethics opinions. |
| Statutes | **Consumer Protection Act (WY Stat § 40-12-502 (2022))** mandates individuals and commercial entities that own or license computerized personal identifying information to provide notice to affected persons for security breaches "as soon as possible" to Wyoming residents and "as soon as practicable" to business entities whose information was breached. Notification not required if, after a reasonable and prompt investigation, the entity determines the breach will not cause, or is not reasonably likely to cause misuse of the personal information, especially if the personal information was redacted. **This law does not apply to government agencies.<br>Link: https://wyoleg.gov/statutes/compress/title40.pdf |