Professional Responsibility Regarding Data Privacy and Security Whitepaper

Data privacy focuses on how what information is collected from an individual, how that data is used, and the rights that individual has regarding their data. Data security focuses on how the data is protected from disclosure to others. This whitepaper will discuss the various professional responsibility issues and concerns around keeping a client's data private and secure, and will detail how ElderDocx is designed to meet those duties.

Note: Each state has their own Model Rules of Professional Conduct. Check the specific rules in a particular jurisdiction as needed.

A. Duty of Competence

Rule 1.1 of the American Bar Association (ABA) Model Rules of Professional Conduct (MRPC), states "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." In comment 8 of this rule, the ABA clarifies that a lawyer has a duty to keep abreast of the "benefits and risks associated with relevant technology."

Ignorance is not a defense. A lawyer must educate herself and be competent regarding the different technologies that she uses in her practice, to ensure the use of such technology doesn't run afoul of laws and rules pertaining to data privacy and security.

B. Duty of Confidentiality

The ABA MRPC, in Rule 1.6, outlines a lawyer's responsibility regarding the confidentiality of a client's information. It says that a lawyer cannot divulge a client's data "unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted" in an enumerated list of circumstances. Rule 1.6 also says "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

The reasoning for such rule is common sense – a client needs to be able to trust the lawyer with sensitive information in order for the client to receive the best representation. A client will more readily be candid with the lawyer if the client knows that their secrets will be kept. Data privacy and security also has more practical effects, such as curtailing identity theft.

The rule not only applies to the lawyer divulging client information herself, but it also prohibits lawyer conduct that could lead to the discovery of the sensitive information by a third party. The MRPC comment to Rule 1.6 states that the rule of confidentiality is not violated when there is unauthorized access to a client's information if the lawyer "has made reasonable efforts to prevent the access or disclosure." For a further discussion on "reasonable efforts", keep reading.

C. Federal and State Privacy Laws

There is no comprehensive federal privacy law. Instead, there are federal privacy laws regarding specific types of information, such as the Health Insurance Portability and Accountability Act,

which governs the use and disclosure of health information. However, such federal law may not apply to your legal practice, as your practice may not qualify as a covered entity or business associate under the law. So, when analyzing a particular federal privacy law, also take note of who must comply with the law.

State privacy laws are emerging across the country. Many state laws center around a client's right with regard to information you have collected about them and requirements for keeping that data secure. For example, one such right is the "Right to Delete" and it dictates that a client has the right to request that you delete all personal information about them that you have collected.

D. Sharing or Storing Data with Third-Party Vendors

Most attorneys don't store paper files anymore; gone are the days of huge boxes filled with paper, jamming up closets and storage facilities. Instead, as more offices are going green and striving for efficiency when storing data, client files are kept in electronic format and stored with a third-party vendor. The "cloud" refers to storage services that are internet based. Meaning, it is not storage available locally on the attorney's computer or network but instead is located on a remote server. Most commonly, this remote server is hosted by a third party, such as Practice Panther, Dropbox, Clio, or Salesforce. In addition to storing data with a third-party vendor, client data can be shared with third-party vendors for various other purposes including billing, computer maintenance, or document drafting.

Ethics opinions

Many states have put forth ethics opinions that detail what reasonable efforts an attorney must undergo and issues to consider when storing clients' information in the cloud or otherwise divulging client data to a third-party vendor. For most, these elements include some form of the following:

1. Conduct due diligence to ensure the third party is a reputable business.
2. Ensure the third party has procedures in place to keep the information private and secure.
3. Ensure the third party will not use the data for any secondary purpose, such as advertising.

ElderDocx privacy and security

ElderCounsel is an industry-leader in document drafting solutions and has over a decade of experience offering services to attorneys around the country. ElderCounsel has procedures in place to keep information entered into ElderDocx private and secure. Our Privacy Policy outlines how data is collected and the use for that data. Our Security Policy details how we keep ElderDocx data secure. You can read both policies in our help center.

How is ElderDocx designed with data privacy and security in mind?

- When you use ElderDocx and enter a client's personal information into the system, this information is stored in the contact record. If you want to delete a client's personal information, simply delete their contact record. However, also be aware of any information entered into a text box into the ElderDocx interview. One common place for

text boxes is in the Medicaid Asset Protection Letter. You may want to review a client's matter to see if you have entered any personal information of a client in a text box or similar format.

- ElderDocx does not store generated documents. When you generate a document using ElderDocx, it generates on your computer and you have a choice where to save it, such as on your computer's hard drive, local network, or in the cloud. As such, you don't have to worry about ElderDocx storing, accessing, or using these documents.
- When you need assistance with a particular matter, you do not need to email an answer file to ElderCounsel. Instead, we obtain permission to access that file in your ElderDocx account. This way, you needn't worry about email interception or storage of confidential information. In addition, the permission you grant is time limited, and will expire after 14 days.
- ElderCounsel has an internal policy dictating that any employee that views an answer file must keep the information confidential. Employees cannot keep or store a copy of the answer file, cannot discuss the contents of the answer file with non-employees, and must receive periodic training on ElderCounsel's data privacy and security policies.

Conclusion

ElderCounsel takes data privacy and security seriously. We have designed ElderDocx with these issues in mind. If you have any questions, you can call 888-789-9908 ext. 560, email support@eldercounsel.com, or write to PO Box 1428, Bend, OR 97709.