Cybersecurity & Ethical Pitfalls of Everyday Law Office Computing

Paul J. Unger, Esq. (punger@affinityconsulting.com)
Affinity Consulting Group
Copyright © 2023

Protection of client information, confidences and secrets is one of the most sacred traits defining the relationship between lawyers and their clients. Without a proper understanding of technology, you may be compromising that relationship. Email, cloud computing, traditional computers, smartphones, tablets, networks, viruses, worms, spyware, metadata, electronic court filings, just to name a few, may already be compromising that relationship without you even knowing it.

Take email as an example. In 2023, the average legal professional will receive between 125-150 email messages daily and that doesn't include additional messages through applications like MS Teams or Slack. Without question, email is one of the most important technological communication advancements of the past 100 years. It has fundamentally changed the way we communicate with clients and the way that we do business. Major corporations and law firms are run via email communication instead of face-to-face communication. For lawyers, emails present a wide array of issues that most of the business world and ordinary consumers will never face.

In Canada and the U.S., lawyers have a duty to take reasonable steps to protect their client's confidential information, whether it is in the form of paper or electronic. Under ABA Model Rule 1.6, lawyers have a broad obligation to act competently and reasonably protect client information and confidences. Rule 1.6 (replacing DR 4-101) revised the scope of confidential information. Similarly, in Canada, Model Code of Professional Conduct, Rule 3.3 requires the same protection of client information and confidences. Practicing law without technology (and email) has almost become an impossibility.

However, law and technology have become so intertwined that you can find yourself in many ethical dilemmas pretty quick. This seminar and article seek to address these issues that may lead to an ethical violation or malpractice.

"Competence" Re-Defined / Taking Reasonable Steps to Protect Client Information

Trend in North America – Examples

The U.S. is not alone in requiring a lawyer to understand the benefits and risks of technology. On October 19, 2019, the Federation of Law Societies of Canada formally amended its Model Code to include the duty of technical competence. Comments to Rule 3.1-2 say:

> [4A] To maintain the required level of competence, a lawyer should develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer's duty to protect confidential information set out in section 3.3.
>
> [4B] The required level of technological competence will depend on whether the use or understanding of technology is necessary to the nature and area of the lawyer's practice and responsibilities and whether the relevant technology is reasonably available to the lawyer. In determining whether technology is reasonably available, consideration should be given to factors including:
>
> (a) The lawyer's or law firm's practice areas;
>
> (b) The geographic locations of the lawyer's or firm's practice; and
>
> (c) The requirements of clients.

Of course, individual Canadian provincial and territorial law societies still must adopt the rule, but that is anticipated over time. Like the U.S. the new language simply makes explicit what is already implied in the existing rules. Regardless, the act of making it explicit has clearly triggered a much higher awareness and we are seeing lawyers take significantly more steps to protect client electronically stored information.

Pennsylvania (approved October 22, 2013)

Rule 1.1 – Comment 8: Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer must keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with</u>

relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Pennsylvania was the first state to adopt the new language. 38 states have adopted the Duty of Technical Competence. Some of those include:

Alaska (effective October 15, 2017)
Arkansas (effective June 26, 2014)
Arizona (effective January 1, 2015)
California (effect March 22, 2021)
Colorado (approved April 6, 2016)
Florida (effective January 1, 2017)
Idaho (effective July 1, 2014)
Indiana (effective January 1, 2018)
Illinois (effective January 1, 2016)
Kansas (effective March 1, 2014)
Kentucky (effective January 1, 2018)
Louisiana (adopted April 11, 2018)
Michigan (effective January 1, 2020)
Minnesota (approved February 24, 2015)
Missouri (approved Sept. 26, 2017)
Montana (see paragraph 5 under Preamble). Bar petition. Court Order (Sept 2016).
New Hampshire (effective January 1, 2016)
New York (adopted March 28, 2015)
North Carolina (approved July 25, 2014)
Ohio (effective April 1, 2015)
Oklahoma (adopted September 19, 2016)
Pennsylvania (effective October 22, 2013)
South Carolina (approved November 27, 2019)
Virginia (effective March 1, 2016)
Washington (effective Sept.1, 2016)
West Virginia (effective January 1, 2015)
Wisconsin (effective January 1, 2017)

Montana

In Montana, technical competence is addressed in paragraph 5 of the Preamble:

> (5) In all professional functions a lawyer should be competent, prompt and diligent. Competence implies an obligation to keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. A lawyer should maintain communication with a client concerning the representation. A lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Rules of Professional Conduct or other law.

Some jurisdictions have not yet adopted the new language within their rules of professional conduct. As of September of 2022, those include:

Oregon
Nevada
South Dakota
Mississippi
Alabama
Georgia
Maine
Maryland
New Jersey

Some states have not adopted the rule change but have addressed it in an ethics opinion. For example, **Oregon** in Formal Opinion 2011-187 imposes a duty of technical competence *when dealing with metadata* and cites Arizona Ethics Op No. 07-03. It is reasonable to conclude that all Oregonian lawyers should have general technical competence (not just technical competence with metadata) in light of this opinion on metadata and the national trend.

Acting Competently to Preserve Confidentiality

Idaho Rule 1.6, Comments 19 & 20 (underlining added)

[19] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[20] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Indiana Rule 1.6, Comments 16 & 17

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

Ohio Rule 1.6 (and Model Rule 1.6) and Comments 18 & 19

Rule 1.6(c) – Confidentiality of Information: A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Rule 1.6 – Comment 18 & 19: Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Similarly, many other states have taken the same approach in their comments, as the ABA and Ohio. Take Maine, New Hampshire and Oklahoma as an example:

Maine Rule 1.6
Acting Competently to Preserve Confidentiality – Comments 16 & 17

Acting Competently to Preserve Confidentiality

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. Consistent with Section 66 of the Restatement, a lawyer who takes action or decides not to take action allowed under this Rule is not, solely by reason of such action or inaction, subject to professional discipline, liable for damages to the lawyer's client or any third persons, or barred from recovery against a client or third persons. The legal effect of the lawyer's choice, however, is beyond the scope of the Model Rules of Professional Conduct.

[17] When transmitting a communication that includes confidences or secrets of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

Missouri Rule 4-1.6
Acting Competently to Preserve Confidentiality - Comments 15 & 16

[15] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 4-1.1, 4-5.1, and 4-5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 4-5.3, Comments [3]-[4].

[16] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

New Hampshire Rule 1.6
Acting Competently to Preserve Confidentiality - Comments 18 & 19

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these rules.

Oklahoma Rule 1.6
Acting Reasonably to Preserve Confidentiality – Comments 16 & 17

[16] Paragraph (c) requires a lawyer to act reasonably to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern date privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3] -[4].

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Louisiana Rule 1.6 – Comments 18 and 19

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Mississippi Rule 1.6 + Comments

Mississippi requires reasonableness and competency, but they don't provide as much guidance in their comments as other states:

> **Acting Competently to Preserve Confidentiality.** A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See rules 1.1, 5.1 and 5.3.
>
> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

Wisconsin 1.6 – Comments 18 and 19

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Breach Notification Laws

Data breaches, wherein unauthorized parties gain access to confidential data, pose significant risks all those involved. To mitigate these risks and uphold the rights of individuals, nearly every state has passed legislation mandating notification to those impacted.

A data breach occurs when there is unauthorized access, acquisition, disclosure, or loss of sensitive or personal information. This information could include names, addresses, financial data, medical records, passwords, and other confidential details. Data breach notification laws and regulations differ across jurisdictions. Countries, states, and regions have established their own rules and timelines for notifying affected individuals, regulatory bodies, and sometimes the media about a data breach. What follows are some sample states that most states model.

Indiana

On March 18, 2022, Indiana Governor Eric Holcomb signed into law an amendment to Indiana's data breach notification statute. The amendment requires notification of a data breach to affected individuals and the Indiana Attorney General without unreasonable delay, but no later than forty-five (45) days after discovery of the breach. The amendment to Ind. Code Ann. Section 24-4.9-1 took effect on July 1, 2022. Some states require notification to the Attorney General if the breach impacts a set number of residents, but in Indiana, it is important to note that notice must be provided to the Attorney General if notice is given to ANY Indiana resident. If more than 1,000 residents are notified, you must also notify all nationwide consumer reporting agencies, and provide information necessary to assist in fraud prevention, including the personal information of a resident affected by the breach.

Iowa

Notification in Iowa shall be made in the most expeditious manner possible without unreasonable delay following discovery of a breach. Notice or receipt of notice must be provided to the Attorney General within 5 business days of giving notice to any consumer. If data is encrypted and the encryption key is not compromised, there is no duty to notify anyone of the breach.

Kentucky

Notice should occur in the most expedient time possible and without unreasonable delay, subject to the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Non-affiliated third-party notice should occur in the most expedient time possible and without unreasonable delay, within 72 hours of determining that a breach occurred. If an Entity discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at one time, the Entity shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus. If data is encrypted and the encryption key is not compromised, there is no duty to notify anyone of the breach.

Maine

Maine is like other states but must notify within a reasonable amount of time, but no later than 30 days those impacted and the Attorney General. If data is encrypted and the encryption key is not compromised, there is no duty to notify anyone of the breach.

Ohio

Ohio follows suit and requires notice within a reasonable amount of time, but no later than 45 days to those impacted and the Attorney General. If over 1000, then also the credit report agencies. If the data is encrypted and the encryption key is not compromised, there is no duty to notify anyone of the breach.

Oregon

Oregon is similar but requires notification to those impacted within 10 days and if over 250 people, the Attorney General within 45 days. If the data is encrypted and the encryption key is not compromised, there is no duty to notify anyone of the breach.

Wisconsin

Similar to Indiana and others, an entity shall provide notice within a reasonable amount of time, but not to exceed 45 days. If more than 1,000 residents are notified, must also notify all nationwide consumer reporting agencies. If the data is encrypted and the encryption key is not compromised, there is no duty to notify anyone of the breach.

Encryption Exception

All states cited - If data is encrypted and the encryption key is not compromised, there is no duty to notify anyone of the breach.

Penalties for Non-Compliance

Failure to comply with data breach notification requirements can lead to severe penalties, including fines, legal actions, and reputational damage for the organization responsible for safeguarding the data. In Indiana, for example, a violation may result in a civil penalty up to $150,000, plus reasonable costs.

In conclusion, the general rule of law regarding data breach notification requirements underscores the importance of transparency, accountability, and protection of individuals' privacy rights in the digital age. Organizations must stay informed about the specific laws applicable in their jurisdictions and take proactive measures to prevent breaches while establishing robust response strategies to ensure compliance with notification requirements in case of a breach.

Data Breach Safe Harbor Laws - Trending

Ohio was the first state in the U.S. to enact a data breach safe harbor law (Ohio Revised Code Section 1354.01 et seq.), (effective April 5, 2019). Ohio's safe harbor law provides business protection from some liability in exchange for having good cybersecurity practices in place. It is generally considered to be a win/win for both businesses and consumers. Here's a summary of Ohio's Data Breach Safe Harbor law:

Ohio Data Protection Safe Harbor Law:

- Ohio's law defines a data breach as the unauthorized access and acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information.
- Safe Harbor Conditions: To qualify for safe harbor protection, a business must have implemented and maintained a written information security program (WISP) that meets specific criteria outlined in the law. This program should be designed to protect personal information, and the business must regularly assess and update it.
- Requirements for the Cybersecurity Program: The cybersecurity program must be designed to:
    a. Protect the security and confidentiality of personal information.
    b. Protect against any anticipated threats or hazards to the security or integrity of personal information.
    c. Protect against unauthorized access to and acquisition of personal information.
    d. Ensure proper data disposal when it is no longer needed.
    e. Promote the security and privacy of personal information.
    f. The WISP must conform to one of several national frameworks such as NIST, FedRAMP or ISO.

- Benefits of Safe Harbor: If a business that has suffered a data breach can demonstrate that it was in compliance with Ohio's cybersecurity program requirements at the time of the breach, it may be eligible for safe harbor protection. This protection includes immunity from certain legal actions and statutory damages related to the breach.

Several other states have enacted similar data protection and safe harbor laws, although the specific requirements and conditions vary.

1. **Connecticut**: Connecticut's law encourages businesses to implement and maintain reasonable cybersecurity practices. Compliance may be used as an affirmative defense in a legal action.
2. **Utah**: Utah's law provides certain legal protections to entities that implement a written cybersecurity program and comply with it.
3. **Michigan**: Michigan's Cybersecurity Act offers safe harbor to businesses that meet specified cybersecurity standards.
4. **New York**: New York's SHIELD Act mandates that businesses implement reasonable data security measures and provides an affirmative defense for compliance. Failure to do so may result in penalties.
5. **Colorado**: Colorado's law requires the implementation of reasonable security practices and procedures to protect personal information.
6. **Massachusetts**: Massachusetts' data security regulations mandate the implementation of comprehensive information security programs.

Cloud Computing

Cloud computing is an umbrella term that covers several concepts. Within the scope of legal technology, it most often refers to Software-As-A-Service ("SaaS"). There are a ridiculous number of definitions of SaaS, but I think this one sums it up succinctly without using 15 more acronyms requiring definitions:

> "Generally speaking, it's software that's developed and hosted by the SaaS vendor and which the end user customer accesses over the Internet. Unlike traditional packaged applications that users install on their computers or servers, the SaaS vendor owns the software and runs it on computers in its data center. The customer does not own the software but effectively rents it, usually for a monthly fee. SaaS is sometimes also known as hosted software or by its more marketing-friendly cousin, 'on-demand.'"

To be clear, this means that you do not have the software installed on your computer - it is accessible only via a browser on the Internet. Further, your data and/or documents are located on the vendor's servers and not on your computer or server.

This obviously raises ethical concerns because you are entrusting client confidential information with someone other than you and your employees.

An excellent compilation of ethics decisions around the country can be found at the ABA Law Practice Management Section's Legal Technology Resource Center (LTRC).

http://www.americanbar.org/groups/departments_offices/legal_technology_resources.html

Probably the best decision that I have read to date in the U.S. comes from Pennsylvania:

http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/saas.html

Pennsylvania, and nearly every jurisdiction who has addressed the issue employ a standard of reasonableness and typically requires segregation of data, privacy/security of data, ability to keep a local download, and reliability of the vendor. The court stated:

The standard of reasonable care for "cloud computing" may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;

- Installing a firewall to limit access to the firm's network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the lawyer provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;
- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;
- Ensuring the provider:
    - explicitly agrees that it has no ownership or security interest in the data;
    - has an enforceable obligation to preserve security;
    - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
    - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
    - includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;
    - provides the firm with right to audit the provider's security procedures and to obtain copies of any security audits performed;

    - will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;

    - provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,

    - provides the ability for the law firm to get data "off" of the vendor's or third-party data hosting company's servers for the firm's own use or in-house backup offline

- Investigating the provider's:

    - security measures, policies and recovery methods;

    - system for backing up data;

    - security of data centers and whether the storage is in multiple centers;

    - safeguards against disasters, including different server locations;

    - history, including how long the provider has been in business;

    - funding and stability;

    - policies for data retrieval upon termination of the relationship and any related charges; and,

    - process to comply with data that is subject to a litigation hold.

- Determining whether:

    - data is in non-proprietary format;

    - the Service Level Agreement clearly states that the lawyer owns the data;

    - there is a 3rd party audit of security; and,

    - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.

- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

In Oregon, while the model rule language in Comments 18 & 19 has not been explicitly adopted, in Formal Opinion No. 2011-188 (revised 2015) they have adopted "the rule to act reasonably" as it applies to an lawyer's obligation under Rule 1.6 to protect client confidential information. Opinion 2011-188 specifically concludes that a lawyer may contract with a third-party vendor to store and retrieve files online via the Internet (i.e., cloud computing).

In Canada, only the Law Society of British Columbia has directly addressed cloud computing, and the Legal Education Society of Alberta has adopted the same standard. It seems to be a higher standard than the U.S., and many practicing in other areas of Canada that haven't addressed it have felt comfortable following the U.S. rules. The Law Society of BC developed an extensive checklist that is submitted as a separate paper hereto. The checklist encourages potential cloud service users to consider, among other things:

- use of a private cloud, which is designed to offer the same features and benefits of public cloud systems without some of the typical cloud computing concerns such as data control, security, and regulatory compliance;
- encryption of data using a 3rd party encryption product and the compatibility of the 3rd party product with the cloud provider's product and services;
- data security and responsibility for specific aspects of security, including firewall, encryption, password protection and physical security;
- regulatory requirements, including statutory privacy requirements, retention periods indicated in the LSBC Rules, the ability to produce documents with respect to a LSBC investigation in the form and time prescribed, and the retention of custody over client data;
- adequacy of remedies in the event of data breaches, data loss, indemnification obligations, and service availability failures;
- the cloud provider's breach notification obligations;
- termination of the services agreement with the cloud provider, specifically as it relates to issues including cost, service level failures (bandwidth, reliability, etc.), data availability after termination, and transition services;

- technical considerations, including compatibility with existing systems, uptime, redundancies, bandwidth requirements, security measures, and technical support service availability; and
- the track record of the cloud services provider (such as uptime, security, support service level, etc).

The above is neither an exhaustive list of applicable considerations nor a complete summary of the Checklist.

Advantages of Cloud Computing (Saas):

- Up Front Price Advantage: Let's say you want to start using a case management application for your practice. If you were to buy one such as Time Matters, you would have to pay for the software outright along with the annual maintenance contract which is mandatory ($905 for the first license and $525 for each license thereafter). You may have to buy a file server or otherwise upgrade your hardware in order to run the program. For an example cost, a new server plus installation and setup could easily run $5,000 - $8,000. Therefore, buying software may turn out to be quite expensive. In the alternative, you would begin subscribing to something like www.rocketmatter.com in which case you would pay $59.99 for the first user per month and $49.99 per user for the next 5 users per month. You wouldn't have to buy a server and you probably wouldn't have to upgrade any of your existing equipment assuming you already have high speed Internet access.

- Ease of Use

- World-Class Data Security

- New Hardware often <u>NOT</u> Required: If you already have a computer and high speed Internet access, then you probably don't need anything else from a hardware perspective.

- Works in Apple or Windows: Since these applications are browser based, they will usually work with both Apple and Windows computers.

- Updates Included: Most cloud application include all updates which are installed for you.

- Technical Support Included: With most cloud applications, you get "free" technical support included with your monthly subscription fee. Of course, purchased software also provides technical support but it is often an extra fee on top of the original software purchase price.

- Access From Anywhere: As long as you're using a computer with internet access, you can probably use your cloud applications. You wouldn't need a VPN, GotoMyPc, or any other type of additional remote access application to accomplish this.

- Share Applications Among Users Spread Out Geographically: For lawyers with multiple offices or who wish to work from multiple locations, cloud applications provide a lot of flexibility. Of course, there are other ways to gain access to programs besides subscribing to cloud applications, but this feature is obviously built in to cloud apps without buying anything else.

- Redundancy Provided: Since your data is stored on the host company's servers, they almost always provide redundant data storage along with that so that there is little (if any) risk that you would lose your data or access to your application due to a physical hardware failure.

E-Mail Encryption and Other Potential Pitfalls

❶ To Encrypt or Not to Encrypt?

According to most jurisdictions in the United States, a lawyer does not violate the duty to preserve confidences and secrets if an email is sent without encryption technology.

In Canada, the rules do not explicitly say that encryption is not required. Instead, the rules imply a duty to act reasonably to protect client confidences. Lawyers should consider the use of information technologies to communicate with the client in a timely and effective manner appropriate to the abilities and expectations of the client. Lawyers may use email (see Rule 3.1-1(d) and 3.1-2 of the Rules of Professional Conduct).

Lawyers must display the same care and concern for confidential matters regardless of the information technology being used. When communicating confidential information to or about a client, lawyers should employ reasonably appropriate means to minimize the risk of disclosure or interception of data by malicious intruders.

What are the risks that a particular information technology poses for inadvertent disclosure or interception? Lawyers should inform a client of the risks of unauthorized disclosure and interception before using information technologies. Lawyers need to ensure that their clients, too, understand that they need to protect the confidentiality of communications to them. Seeking client consent before using a particular technology for communications may be appropriate.

In Ohio, Ethics Opinion 99-2, issued April 9, 1999, by contrast states that a lawyer does not violate the duty to preserve confidences and secrets if an email is sent without encryption technology citing DR 4-101 of the Ohio Code of Professional Responsibility. A lawyer must use his or her professional judgment in choosing the appropriate method of each attorney-client communication. Most jurisdictions in the U.S. are consistent with Ohio.[1] Also see Formal Opinion No. 99-413 of the American Bar Association

---

[1] Excerpt from Ohio Op. 99-2:

The trend among advisory bodies in other states (and the District of Columbia) is that electronic mail without **encryption** is ethically proper under most circumstances.

In the District of Columbia, "[i]n most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security." District of Columbia Bar, Op. 281 (1998).

In Illinois, "[l]awyers may use electronic mail services, including the Internet, without **encryption** to communicate with clients unless unusual circumstances require enhanced security measures." Illinois State Bar Ass'n, Op. 96-10 (1997).

In New York, the state bar association advised that "lawyers may in ordinary circumstances utilize unencrypted Internet **e-mail** to transmit confidential information without breaching their duties of confidentiality under Canon 4 to their clients, as the technology is in use today. Despite this general conclusion, lawyers must always act reasonably in choosing to use **e-mail** for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular **e-mail** transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet **e-mail**." New York State Bar Ass'n, Op. 709 (1998). The city bar association advised that "[a] law firm need not **encrypt** all **e-mail** communications containing confidential client information, but should advise its clients and prospective clients communicating with the firm by **e-mail** that security of communications over the Internet is not as secure as other forms of communication." Ass'n of the Bar of the City of New York, Formal Op. 1998-2 (1998).

In North Dakota, "Rule 1.6 of the North Dakota Rules of Professional Conduct is not violated by a lawyer who communicates routine matters with clients, and/or other lawyers jointly representing clients, via unencrypted electronic mail (**e-mail**) transmitted over commercial services (such as America Online or MCI Mail) or the Internet unless unusual circumstances require enhanced security measures." State Bar Ass'n of North Dakota, Op. 97-09 (1997).

In Vermont, "[a] lawyer does not violate DR 4-101 by communicating with a client by **e-mail**, including the Internet, without **encryption**." Vermont Bar Ass'n, Op. 97-5.

One state is reticent in its advice regarding unencrypted electronic communication with clients. In Arizona, the state bar responded "Maybe" to the question "Should lawyers communicate with existing clients, via **e-mail**, about confidential matters?" They advised "it is not unethical to communicate with a client via **e-mail** even if the **e-mail** is not **encrypted**" but suggested "it is preferable to protect the attorney/client communications to the extent it is practical." The committee suggested using a password known only to the lawyer or client, using **encryption** software, or at a minimum using a cautionary statement such as "confidential" and "Attorney/Client Privileged" either in the "re" line or beginning the communication. An additional suggestion was to caution clients about transmitting highly sensitive information via **e-mail** if the **e-mail** is not **encrypted** or otherwise secure from unwanted interception. Attorneys were "reminded that **e- mail** records may be discoverable." State Bar of Arizona, Op. 97-04 (1997).

Several states have reconsidered their initial views on the issue. In South Carolina, the bar association first advised that "unless certainty can be obtained regarding the confidentiality of communications via electronic media, that representation of a client, or communication with a client, via electronic media, may violate Rule 1.6, absent an express waiver by the client." South Carolina Bar, Op. 94-27 (1995). Later, the bar advised that "[t]here [now] exists a reasonable expectation of privacy when sending confidential information through electronic mail (whether direct link, commercial service, or Internet). Use of electronic mail will not affect the confidentiality of client communications under South Carolina Rule of Professional Conduct 1.6." South Carolina Bar, Op. 97-08 (1997).

In Iowa, the bar association rescinded Formal Op. 95-30 and replaced it with Formal Op. 96-1 advising that "with sensitive material to be transmitted on **E-mail** counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgment includes consent for the communication thereof on the Internet or non-secure Intranet or other forms of proprietary networks, or it must be **encrypted** or protected by password/firewall or other generally accepted equivalent security system." Iowa State Bar Ass'n, Op. 96-1 (1996). See also Iowa State Bar Ass'n Op. 96-33 (1997). Later, the bar

Standing Committee on Ethics and Professional Responsibility, *Protecting the Confidentiality of Unencrypted Email*, dated March 10, 1999.

The opinion contains an important caveat that should not be ignored:

> The conclusions reached in this opinion do not diminish a lawyer's obligation to consider with her client the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated media of communication. Particularly strong protection measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of e-mail, just as they would warrant the avoidance of the telephone, fax and mail.

Is there a problem with this decision that is was issued so long ago? What effect do the newer Model Rules have on this opinion? Despite advances in technology, and the rules in most jurisdictions, the opinion would stand up today.

First, the same opinion is shared in well over a majority of jurisdictions, many of which had the New Model Rules already in place. Comment 17 to Rule 1.6 states:

> [17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. **Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.** A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

The ABA accepted the same approach in Comment 16 to Model Rule 1.6.

---

association amended Opinions 96-1 and 96-33 by advising that "with sensitive material to be transmitted on **e-mail** counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgement includes consent for communication thereof on the Internet or non- secure Intranet or other forms of proprietary networks to be protected as agreed between counsel and client." Iowa Bar Ass'n, Op. 97-1 (1997).

Second, email is a very efficient form of communication. Third, the same security issues exist in other forms of communication such as wiretapping phone lines or stealing U.S. mail. Fourth, any interception of email or older forms of communication such as US mail or telephone calls is illegal. Finally, there is support in case law for the proposition that a reasonable expectation of privacy may exist even though a form of communication is capable of being intercepted, citing *State v. Bidnost*, 71 Ohio St. 3d 449, 461 (1994).

Ohio accepted the same approach in Comment 19 to its rule 1.6:

[19] When transmitting a communication that includes information relating to the representation of a client, **the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients**. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. **A client may require the lawyer to implement special security measures not required by this Rule** or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Duty to Do More? … Some Say Yes

Pennsylvania and New Jersey have adopted the same rule, but added a little more stringency to it. In Pennsylvania, Informal Opinion 97-130, issued September 26, 1997, concluded:

1. A lawyer may use e-mail to communicate with or about a client without encryption;
2. A lawyer should advise a client concerning the risks associated with the use of e-mail and obtain the client's consent either orally or in writing;
3. A lawyer should not use unencrypted e-mail to communicate information concerning the representation, the interception of which would be damaging to the client, absent the client's consent after consultation;
4. A lawyer may, but is not required to, place a notice on client e-mail warning that it is a privileged and confidential communication; and,
5. If the e-mail is about the lawyer or the lawyer's services and is intended to solicit new clients, it is lawyer advertising similar to targeted, direct mail and is subject to the same restrictions under the Rules of Professional Conduct.

While other jurisdictions are not bound by rules 1 through 5, above, I recommend them as best practices to follow.

The New Jersey Advisory Committee on Professional Ethics, in Opinion 701, issued in April 2006, states in a footnote that confidential documents sent over the Internet should be password protected.

In conclusion, in light of evolving technology and rules, it is my recommendation that lawyers (1) should advise clients verbally and in their engagement letter about email, as described in the Pennsylvania opinion, and (2) should have encryption available for use in appropriate circumstances.

❷ Email Encryption Solutions

Office 365 w/hosted Exchange (with Business Premium, E3 or E5 licensing)
www.office.com

Protected Trust
www.protectedtrust.com

Mail It Safe
www.mailitsafe.com

AppRiver
http://www.appriver.com/services/email-encryption/

Send
www.sendinc.com

TrendMicro
http://www.trendmicro.com/us/enterprise/network-web-messaging-security/email-encryption/index.html

❸ Retracting Sent E-Mails

Are there times when you wish that you could UNSEND something? This is actually something that can be done to prevent a known ethical violation where it may not be possible with ordinary U.S. Mail. With U.S. Mail, once the mail is in the post box, good luck getting it back!

I have 2 suggestions in this regard:

- If your firm uses Exchange Server, ask your system administrator to set a 5-minute delay before the email is actually sent from your server. This may give a user in your office enough time to catch it before it goes out.

- You may want to try out something like www.mailitsafe.com, or similar functioning service, which is an email verification program, but also allows retraction so long as it hasn't been retrieved by the recipient. You can also encrypt emails and attachments, requiring recipients to use passwords to open. The cost is $150 per year.

❹ E-Mail Addressing: AutoComplete can be an AutoDisaster

Outlook and other popular email programs have an ”Auto-Complete” function that saves you the time of having to type out someone’s complete email address if the name already exists in the program’s address book. Once you type the first character in the TO field, Outlook starts guessing the name of the recipient and will display potential names. If to quick and careless, you could accidentally hit ENTER and auto-complete the wrong recipient. While a nifty feature if used correctly, this can get you into trouble if you are careless.

As an example, if you intend to send something to your client “Brian Cluxton”, you could accidentally send something to opposing counsel “Brian Clayton” by typing B-R-I and hitting ENTER too quickly. If you don’t catch it, you could send something really damaging to the wrong person. I don’t think this warrants disabling the feature for everyone … just be careful!

Metadata Pitfall

You just hit the SEND button. You start to sweat and panic. You and your associate were revising a contract for a client. Before sending it on to your client, you forgot to accept or reject tracked changes and remove all the hidden text from the word processing document. You also forgot to remove any other "metadata" before sending it. Anyone who receives the file can easily find out the following information:

- All the people who authored any part of the document … including the original author who happens to be a managing partner at a competing law firm
- The hidden text that states the client "is a moron!"
- The suggested changes made by a 1st year associate in your office (half of which were not things you want your client to see)
- The total time you spent revising the document was only 15 minutes

This story is not fictional. It actually happened. This is just one of many bad messes that you can get yourself into if you are not using technology correctly.

The Bad News … Say goodbye to the glory days when you could simply draft and send a word processing document to opposing counsel or your client.

The Good News … Most technology-created pitfalls are easily avoidable if reasonable steps are taken.

Metadata … Is it really a "Nightmare"?

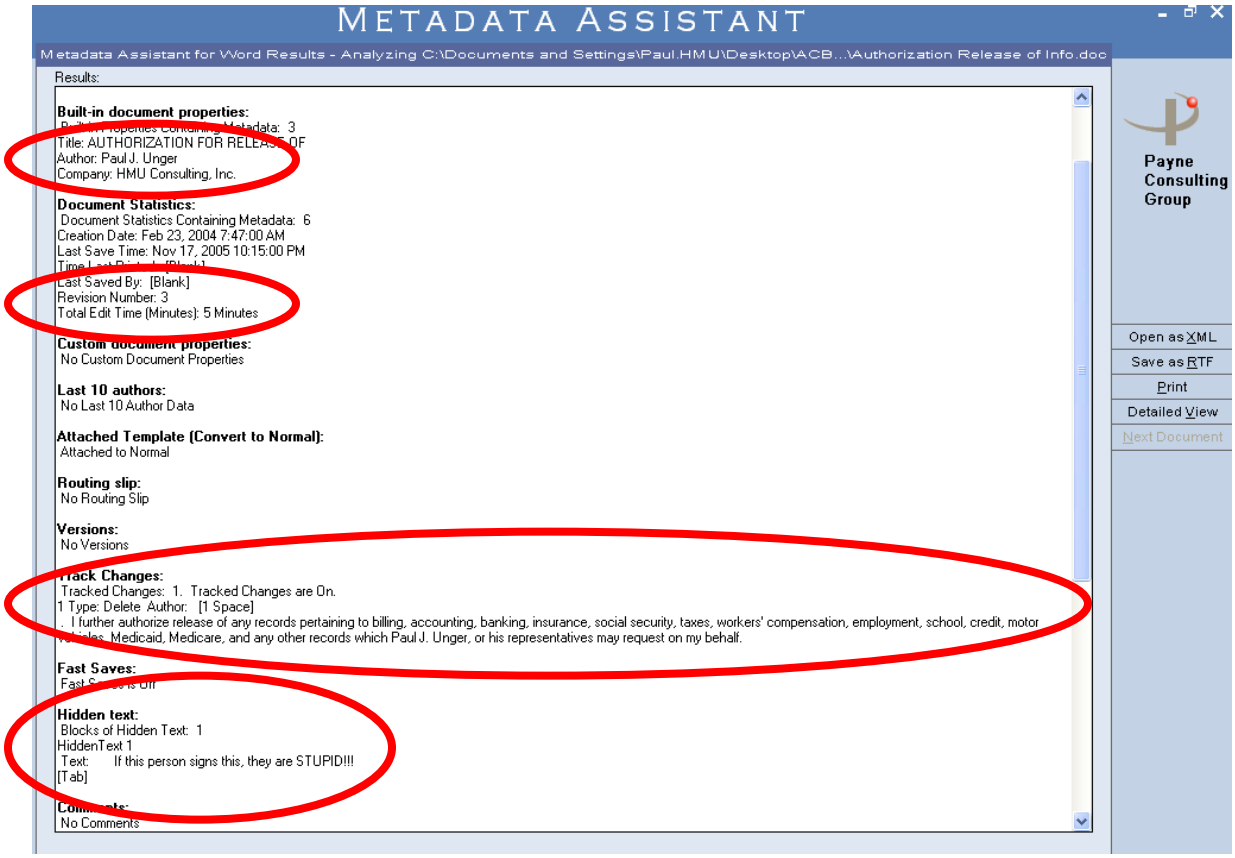
What is Metadata? Literally, metadata means "data about data." In the personal & business computing world, it is the hidden or invisible information contained within computer files. Most notably in the legal technology field, lawyers worry about metadata found in Microsoft Word, PowerPoint, Excel, Corel WordPerfect and Adobe Acrobat files.

The kind of information that can be found under the surface a Word document, for example, might be:

- Last 10 authors
- Firm name
- File locations
- Tracked changes
- Hidden text

- Deleted document comments
- Routing slip information
- Document versions
- Revision time
- Document properties (file size, modification date, etc.)
- Fast saves
- Hyperlinks
- Linked objects

As an example, below is part of a report showing metadata using a widely-used metadata remover called "Metadata Assistant" created Payne Consulting Group.



Why have metadata if it is so bad? Well, quite frankly because metadata is typically very useful information and it was never intended to be bad. Microsoft designed its programs to store metadata for a variety of reasons, one of which was for document management.

As a very simple example, if one wanted to find all documents created or modified between July 1, 2023 and July 31, 2023 as a way to verify that you created timesheets for all your billable time in July, you would perform a search using a Microsoft Find Files or Folders utility or a third-party program like dtSearch that searches … yes … metadata.

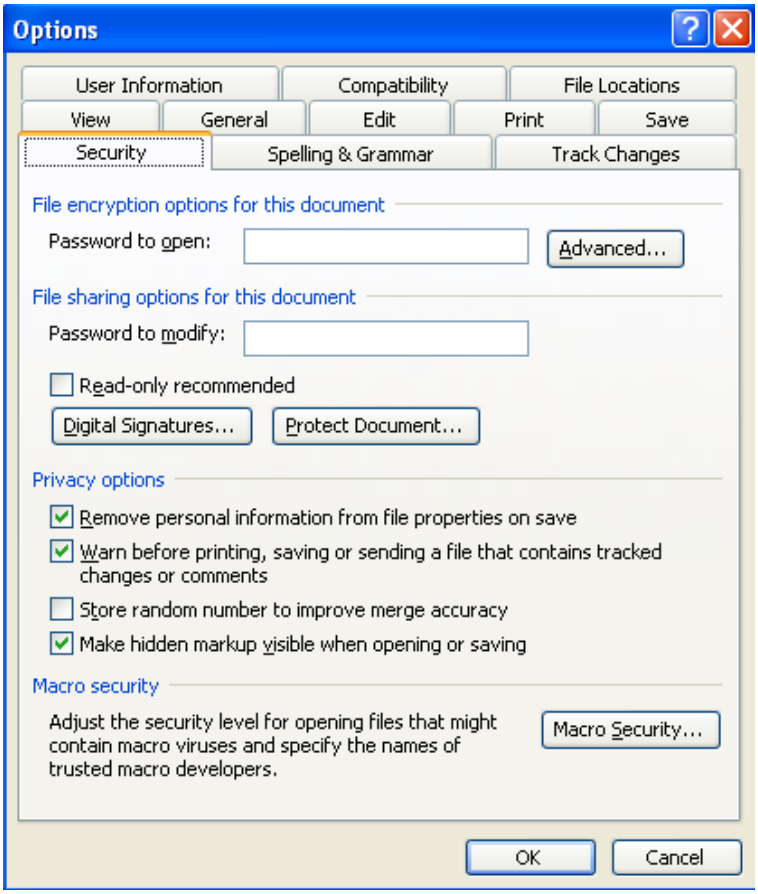
If you exchange electronic word processing files with anyone outside your office and do nothing to remove metadata it can result in a nightmare if the file contains metadata that was intended to be confidential. So, yes, it can indeed be a nightmare as many legal technologists claim. However, if you are not careless, these problems are not a nightmare at all. You just need to know what to do. Below is a list of what you need to do to avoid the word processing so-called "metadata nightmare."

❶ Learn the Security Settings within Microsoft Word

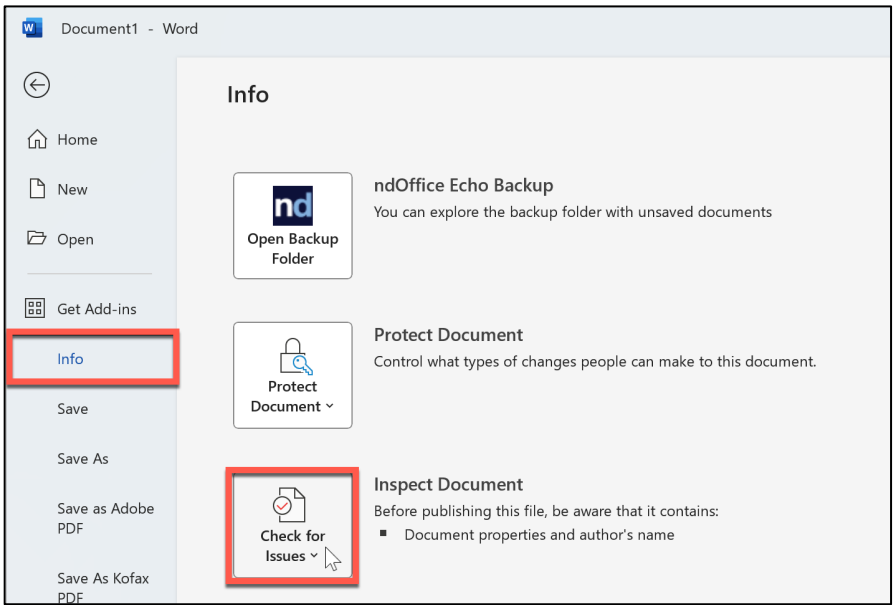
Much of the "dangerous" metadata contained in Microsoft Word documents can be prevented from transmission if certain security features are turned on.

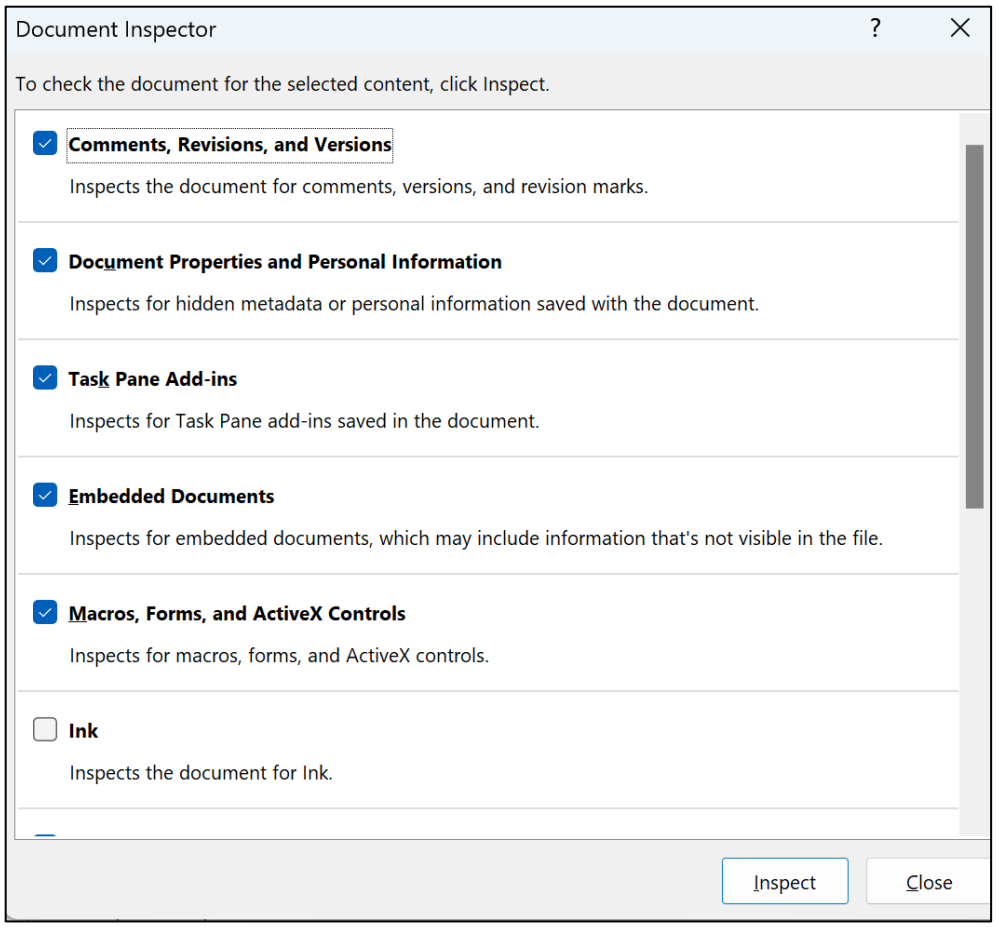
In Word 2003 and earlier, open Word and select **Tools** and then **Options** and select the **Security** tab:

- Check "Remove personal information from file properties on save"
- Check "Warn before printing, saving or sending a file that contains tracked changes or comments"
- Check "Make hidden markup visible when opening or saving"

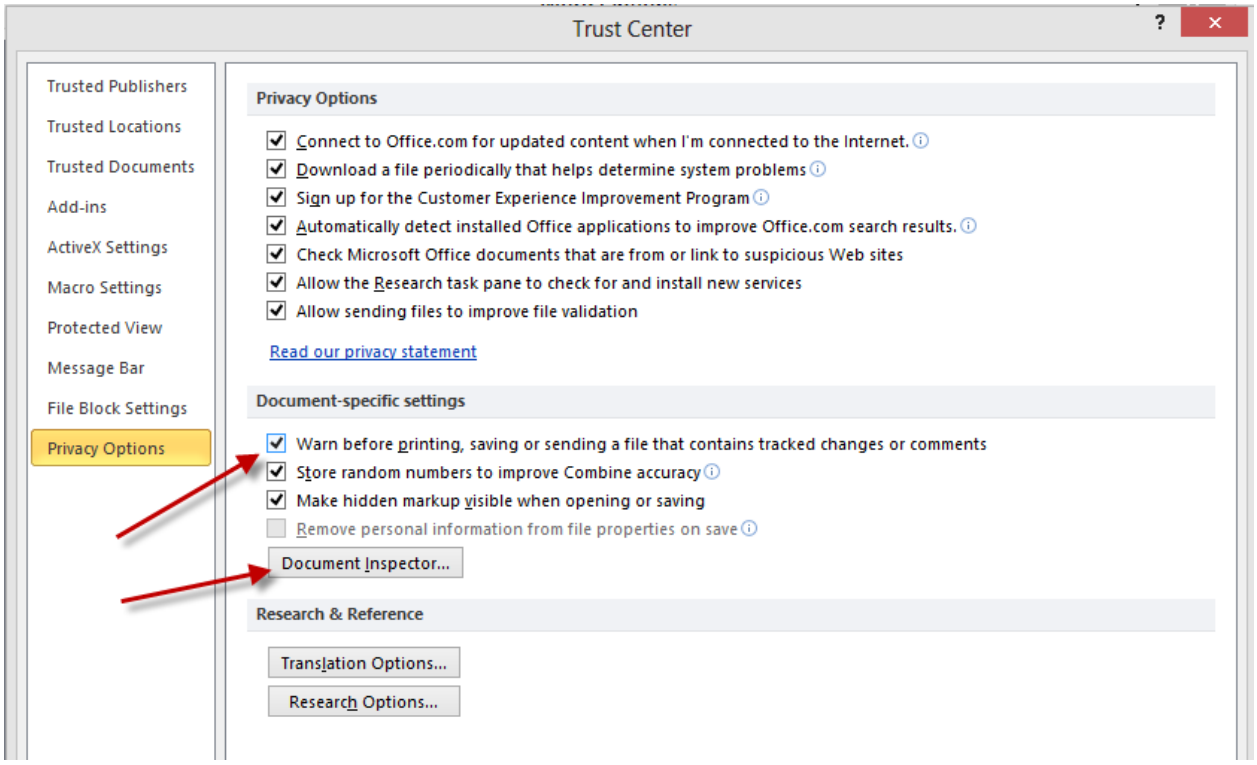


In Word 2016 and later, you must run the document inspector, which is most easiest found at **File > Info > Check for Issues > Inspect Document.**




Document Inspector
To check the document for the selected content, click Inspect.
Comments, Revisions, and Versions
Inspects the document for comments, versions, and revision marks.
Document Properties and Personal Information
Inspects for hidden metadata or personal information saved with the document.
Task Pane Add-ins
Inspects for Task Pane add-ins saved in the document.
Embedded Documents
Inspects for embedded documents, which may include information that's not visible in the file.
Macros, Forms, and ActiveX Controls
Inspects for macros, forms, and ActiveX controls.
Ink
Inspects the document for Ink.
Inspect
Close

You may want to have Word warn you if there are tracked changes comments on save, print or send commands. It is found under **File** and then **Options**, **Trust Center, Trust Center Settings**, and then **Privacy Settings**.



You can also download and install a free add-in from Microsoft - Office 2003/XP Add-in: Remove Hidden Data. CAUTION: This will not remove <u>all</u> metadata. Metadata still exists. The question is whether it is benign or damaging metadata.

❷ Learn About Tracked Changes in Word

"Track Changes" is a fantastic feature available in Microsoft Word that allows multiple reviewers of a document to literally track changes or compare documents electronically to see what edits have been made to a document. My first suggestion is to start using it if you have the need for that type of feature. My second suggestion is to learn how to use it correctly so those internally tracked changes do not end up in the hands of opposing counsel or even your own client. Here is an example of a paragraph that has tracked changed turned on.

"Track Changes" is a fantastic feature available in Microsoft Word that allows multiple reviewers of a document to literally track changes or compare documents electronically to see what edits have been made to a document. My first suggestion is to start using it if you have the need for that type of feature. My second suggestion is to learn how to use it correctly so those internally tracked changes do not end up in the hands of opposing counsel or even your own client so you don't look like a freaking idiot. ~~Here is an example of a paragraph that has tracked changed turned on.~~

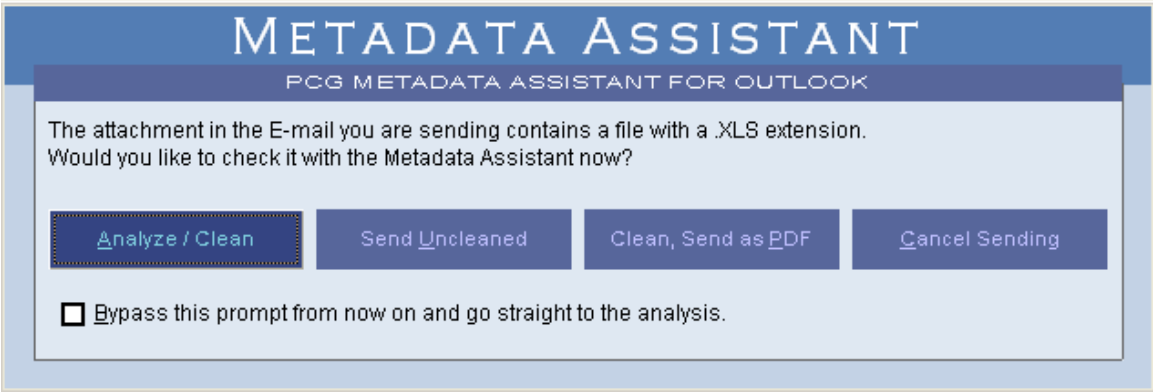
Added Text & Deleted Text

The first big mistake that people make is not accepting or rejecting all changes before sending the document on to opposing counsel for their review. It is imperative that you go through the entire document and accept or reject all the changes made in the document. Changes that were made between versions that are not **accepted** or **rejected** will show up in a metadata analysis. This may expose your thought process or a weakness that you knew about, but the other side didn't think of … at least until now!

The second critical thing that you do is make sure that you can see the tracked changes (the marked up or redlined version). Be sure that you select **Final Showing Markup** in the reviewing toolbar. Otherwise, you may not even realize that there are tracked changes in the document. Also remember in the security settings (discussed above) there is an option that will warn you before printing, saving or sending a document that has tracked changes.

❸ Consider a Third-Party Meta Data Removal Tool

Another option which I generally favor is investing in a metadata removal tool. These are programs that strip the metadata out of electronic documents before you send it to another party. You can either run the cleaner manually on a document OR intercept, evaluate and clean all attached documents when you are emailing it to the outside world. This makes the process much easier and requires no working knowledge of how tracked changes work or security settings within the program. As an example, Donna Payne's Metadata Assistant intercepts attachments with this dialog box when you hit the **Send** key from Outlook's email:



I suggest a metadata remover for those people who actually exchange electronic documents containing potentially harmful metadata. Many lawyers don't do this. If you do not exchange documents, don't spend the money.

Metadata removal tools to consider:

- CleanDocs (www.cleandocs.com)
- Workshare Protect (www.workshare.com). Cost is $29.95 per year.
- iScrub by Esquire Innovations (www.esqinc.com).
- Out-of-Sight by SoftWise (www.softwise.net). Cost is $30 per user.
- ezClean by KKL Software (www.kklsoftware.com). You must buy at least 20 licenses at $20 per license.

❹ Exchange PDF Documents

Although PDF documents do contain some metadata, they do not contain as much. Tracked changes can indeed be passed on from a Word document to PDF, but you would have to do it one of two ways. First, the person converting the document would have to attach the Word file into the PDF in its native format (Acrobat allows you to attach files into a PDF document). While possible, I know of no one who uses that function. So…just don't do it that way. A second way is if you have the tracked changes visible when you convert to PDF. That would create a PDF with the tracked changes blatantly showing. You would have to be blind or extremely careless not to see the tracked changes in the Word document and the resulting PDF. Also, if you have your printing configuration in Word set to print 'tracked changes' along with the document. In this instance, again, you would have to be blind and 100% careless by failing to review the newly created PDF before sending it.

Another benefit sending a PDF is that PDF documents are less editable, especially if you have security turned on. This has less to do with metadata, but it is a nice benefit if you send a PDF to a client, for instance, and tell them to print and sign the attached. If the document is editable, the client could change the text using Adobe Acrobat and then sign it (and not tell you). If the PDF document is secure, the signing party would have to go to greater lengths to make a deceptive change that is not noticeable.

❺ WordPerfect also contains Meta Data

Contrary to popular belief, WordPerfect also contains metadata. Examples of metadata stored in WordPerfect documents include:

- Authors
- Tracked changes
- Comments and hidden text
- Document revision annotations
- Undo/Redo history
- Usernames, initials and company
- Document summary information
- Header/Footer information
- Hyperlinks

See Minimizing Metadata in WordPerfect 12 Documents, Corel Corporation, copyright 2004.

Like Microsoft, Corel also made available a metadata removal tool which is available on their website. Also check WordPerfect Universe (www.wpuniverse) which offers a metadata removal tool for WordPerfect.

Keeping Information Safe from Disaster, Accidental Loss, Theft, Viruses and Malicious Intruders

ABA Model Rule 1.6 also imposes a duty upon lawyer to keep their technology in safe and working order to protect client information. Similarly, in Canada, Section 3.3 of the Rules of Professional Conduct requires competence and confidentiality.

As an example, section 5.7 of the Law Society of Upper Canada's Technology Practice Management Guidelines states:

5.7 Confidentiality

Lawyers using electronic means of communications shall ensure that they comply with the legal requirements of confidentiality or privilege. (Section 3.3 of the Rules of Professional Conduct).

When using electronic means to communicate in confidence with clients or to transmit confidential messages regarding a client, a lawyer should

- develop and maintain an awareness of how to minimize the risks of disclosure, discovery or interception of such communications
- discuss the inherent security risks associated with each technology with the client and confirm in writing that the client wishes to communicate using that method
- use firewalls and security software to protect at-risk electronic information
- use and advise clients to use encryption software to assist in maintaining confidentiality and privilege
- take appropriate measures to secure confidential information when using cloud-based services
- develop and maintain law office management practices that offer reasonable protection against inadvertent discovery or disclosure of electronically transmitted confidential messages.

ABA Model Rule 1.6(a) states:

> (a) A lawyer shall not reveal information relating to the representation of a client, including information protected by the attorney-client privilege under applicable law, unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by division (b) or required by division (c) of this rule.

Comment 16 further states:

> Acting Competently to Preserve Confidentiality [16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3.

The State Bar of Arizona issued an opinion in response to an inquiry about the steps a law firm must take to safeguard data from hackers and viruses. They stated:

> ER's 1.6 and 1.1 require that an attorney act competently to safeguard client information and confidences. It is not unethical to store such electronic information on computer systems whether or not those same systems are used to connect to the internet. However, to comply with these ethical rules as they relate to the client's electronic files or communications, **an attorney or law firm is obligated to take competent and reasonable steps to as-sure that the client's confidences are not disclosed to third parties through theft or inadvertence.** In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information **is not lost or destroyed.** In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence. (Emphasis added.)

State Bar of Arizona, Opinion No 05-04, July, 2005.

The ABA Standing Committee on Ethics and Professional Responsibility has stated something similarly. In Opinion 95-398, they concluded "[a] lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of the client information."

In 2006, Nevada spoke to a similar issue relating to offsite storage of data and reached a consistent conclusion. They stated that a lawyer may store confidential information electronically with a third party to the same extent and subject to the same standards as storing confidential paper in a third party warehouse. In doing so, the lawyer must act" competently and reasonably to ensure the confidentiality of the information. Opinion 33 (February 9, 2006), Nevada Standing Commission on Ethics and Professional Responsibility.

David Reis, a partner with Thorp, Reed & Armstrong, LLP in Pittsburgh, PA, and a colleague legal technologist suggests the following basic steps:

1. Keep your operating systems patched.

2. Install and use anti-virus and spyware protection on all computers (and keep them all current with updates).

3. Use Care with Email attachments and Embedded Links.

4. Make backups of important files and folders.

5. Use strong passwords or other authentication (combine numbers and characters).

6. Use care when downloading and installing programs.

7. Install and use a hardware firewall.

8. Install and use a file encryption program.

Additionally, I recommend:

1. Apply the above principles to laptops and PCs that are used at home for business purposes.

2. Have a secondary backup system (consider an online backup service like Iron Mountain, MozyPro or Carbonite).

3. Encrypt laptops and external hard drives or flash drives where you store or transfer client information.

4. Use Adobe Acrobat Pro (or similar competing products like Kofax PowerPDF Advanced, pdfDocs, etc.) to redact important client information (social security numbers, billing information, etc.) contained in documents that you may have to file with the court electronically.

Disposing of Old Computer Equipment

You just got all new workstations for your staff. What do you do with the old workstations? What about all the confidential information contained on the hard drives? If you think that you deleted the information, think again! You may be violating Model Rule 1.6, HIPAA and opening yourself up to liability.

According to a study performed at the Massachusetts Institute of Technology (MIT), two graduate students scavenged through the data inadvertently left on 158 used disk drives. They found more than 5,000 credit card numbers, detailed personal and corporate financial records, numerous medical records, gigabytes of personal email and pornography. The disk drives were purchased for less than $1,000 from eBay and other sources of used computer hardware. Only 12 were properly sanitized (http://web.mit.edu/newsoffice/2003/diskdrives.html) .

❶ Avoiding the Ethical Pitfall – What is Required?

A lawyer must act reasonably to preserve confidences and secrets of his/her client. The rules in the U.S. and Canada impose the same duty. ABA Rule 1.6 (and old rule DR 4-101) imposes a duty to preserve confidences and secrets. In all likelihood, disposing of employee workstations was not contemplated when DR 4-101 was adopted by the Supreme Court of Ohio on October 5, 1970 and likewise in other jurisdiction following suit; nevertheless, the rule applies. The New Rule as written, establishes a broad duty to preserve confidences and secrets that applies to all methods of communication. The duty clearly extends to disposing of client information and communication.

What does this mean in practical terms? Reasonableness, in my opinion, requires one of the following:

(A) Retain the hard drive(s) of the computer(s) for safe keeping; or
(B) Hire a company to erase and reformat the hard drives[2]; or
(C) Hire a company that uses a special data erasing program.

[2] Erasing and reformatting hard drives will not completely protect the data. A skilled computer technician or forensic expert can likely recover some (not all) data from that hard drive using specialized software. This process is time-consuming and expensive.

❷ Use a Computer/Electronics Recycling Service

Seek out a reputable computer disposal vendor in your area. In Canada and U.S., and depending on your location, Global E Waste Solutions (www.globalewaste.net) offers these services, as well as Iron Mountain (www.ironmountain.com). Both companies are reputable vendors who are committed to proper data destruction and not filling up landfills with electronics.

In the U.S., PCDisposal, IT AMG Disposal Services, and Retire-IT offer these services nationwide. They will pick up your units (or have them shipped), properly delete data, and provide a certified report.

PCDisposal.com
Toll Free: 877-244-0250
www.pcdisposal.com

I.T. AMG Disposal Services
Toll Free: 877-625-4872
www.itmag.com

Retire-IT
Toll Free: 888-839-6555
www.retire-it.com

Local Vendors: Similarly, there may be numerous local vendors in your area who provide these services if you prefer to support local businesses. A quick Google search will identify potential candidates.

Get Multiple Quotes: This is a competitive business, so it is to your benefit to obtain quotes from more than one vendor!

IMPORTANT: Many computer recycling companies will not sanitize data. Make sure that you specifically request this, or it may not be done.

❸ Do-It-Yourself

You could do the DOD-level data destruction yourself with programs like the ones listed below, OR simply take out your screwdriver and physically remove the hard drive and throw it in a locked file cabinet. Programs that you can buy to erase data yourself are:

- cyberCide Data Destruction (www.cyberscrub.com) offers a product for $29.00.
- Active@ Kill Disk - Hard Drive Eraser (www.killdisk.com/eraser.htm) offers a free version and a professional version for about $30.
- OnTrack DataEraser™ (www.ontrack.com) offers a personal version for $29.

IMPORTANT NOTE: If trying to **sanitize data on a solid state drive (SSD)** (most hard drives after 2013), I recommend that you use Parted Magic (www.partedmagic.com), or rely on an expert to do it for you and provide written certification. The above tools will not work on SSDs.

❹ Don't Forget Smartphones, Tablets, and Copy Machines!!

Be sure to follow manufacturer's instructions on wiping all data from smartphones and tablets.

Copy machines are the most often forgotten about devices that contain an enormous amount of potentially confidential client information. Copy machines just don't copy anymore. They first take a snapshot image of the document, stores it on a hard drive, and then prints a copy per your instructions. Depending on the size of the hard drive and the volume you scan, your machine can hold days, weeks, months, and potentially years of "copied" documents.

CBS did an excellent story on copy machines that is quite alarming:
http://www.youtube.com/watch?v=iC38D5am7go

Password Management and Two-Factor Authentication

In short, passwords need to be (1) unique; (2) strong; and (3) stored safely. With as many passwords that we maintain, personally and professionally, there are some very inexpensive, but fantastic solutions that can provide you with relief.

❶ Two-Factor Authentication is Critical

Putting in place two-factor (or multi-factor) authentication (also known as 2FA) is more important today than changing passwords or using unique passwords. I still think unique passwords is important, but changing passwords every 30 days has recently been regarded as a waste of time by some experts. 2FA is more important because without the second method of authentication (usually a text message notification requiring your intervention, like entering a code, providing a PIN, proving your fingerprint from your smartphone) a cybercriminal will not be able to login to an important account even if they have your password. See this regarding Microsoft finally acknowledging this year that 2FA is critical and changing passwords is not very important anymore: https://www.cnet.com/news/microsoft-admits-expiring-password-rules-are-useless/.

❷ Make Passwords Strong and Unique

Passwords should not be re-used. If your credentials are compromised, they could be sold on the dark web. If you used the same password at another site (i.e. Dropbox, a client portal, your bank, etc.) your information (potential confidential information or documents) is now compromised. Moreover, most cybersecurity experts now advise people to use long phrases that combine letters, numbers and characters. I generally aim for at least 12 characters.

❸ Safely Store your Passwords

If you don't have a password manager, I recommend saving your passwords in an encrypted Word or Excel file (see above how to encrypt Word & Excel files).

❹ Password Management Programs

I strongly recommend investing in a password manager. In fact, I believe in this technology so much, that our company now provides a password manager to every employee in our organization. The good news is that the above 3 objectives can be

achieved with some very inexpensive solutions. Here are some of the common features:

- Automatic password generators for unique passwords that never repeat
- Automatic password generators that create insanely strong & cryptic passwords
- Cloud encrypted storage of passwords
- Access to passwords from all mobile and desktop devices
- Integration with all major browsers
- Works on a Mac or PC
- Apps for iPhone, Android-based phones, iPads, Android tablets
- Safe storage of financial and estate information
- Ability to share with loved ones or individuals at work

Highly Rated Password Managers

1. **Roboform** (www.roboform.com)
2. **Dashlane** (www.Dashlane.com)
3. **1Password** (www.1password.com)
4. **Keeper** (www.keepersecurity.com)