New York State Bar Association Real Property Law Section Annual Meeting January 17, 2019

The Duty to Protect Client Confidences in Electronic Documents

Presented by Tony Harwood of Harwood Law PLLC

Overview

- Threats to Confidentiality
- The Rules of Professional Responsibility
- Email and Other Electronic Communication
- Remote Access
- The Cloud
- Offsite Backup
- Metadata
- Questions

FBI WARNING

"I am convinced there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

Former FBI Director Robert Mueller, RSA Cybersecurity Conference, March 2012

Risks to Law Firms

- 2016 Hack of Major Law Firms
  - "A Russian cyber criminal has targeted nearly 50 elite law firms, including four in Chicago, to collect confidential client information for financial gain." March 29, 2016, Crain's Chicago Business
  - According the Wall Street Journal, that hack included Cravath and Weil Gotshal.

Risks to Law Firms

- ABA 2017 Legal Technology Survey
  - 22% of law firms experienced a cyberattack or data breach in 2017, an increase of 14% over the prior year.
  - Includes firms of all sizes.

Risks to Law Firms

- COMMON SCAMS
  - Ransom Ware
  - Identity Theft
  - Information Theft
  - Theft Of Client Funds
    - False Wire Instructions
    - Forged Trust Account Checks
    - False Trust Account Deposits

Rules of Professional Conduct

- RULE 1.1: COMPETENCE

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Rules of Professional Conduct

- Maintaining Competence - Comment **[8]:** To maintain the requisite knowledge and skill, a lawyer should . . . (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information . . . .

Rules of Professional Conduct

- RULE 1.4: COMMUNICATION

(a) A lawyer shall:

(1) promptly inform the client of:

* * *

(iii) material developments in the matter . . . .”

Rules of Professional Conduct

- Communicating About Security Failures
- New York State Bar Ethics Opinion 842 (September 10, 2010), states that under Rule 1.4(a), a lawyer "must . . . notify any affected clients" if there has been a breach of the clients' confidential information that the lawyer stores on an online data storage system.

Rules of Professional Conduct

- RULE 1.6: CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

Rules of Professional Conduct

- RULE 1.6(a) PERMITS DISCLOSURE WHEN:

(1) the client gives informed consent, as defined in Rule 1.0(j);

(2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or

(3) the disclosure is permitted by paragraph (b) [containing six exceptions irrelevant to electronic data.]

Rules of Professional Conduct

Rule 1.6(a) defines confidential information as:

"information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

Rules of Professional Conduct

- Rule 1.6(c) addresses inadvertent or unauthorized disclosure, access to, or use of confidences.
- 1.6(c) was adopted by New York in 2017 and the ABA in 2012.
- It was intended to encompass electronic documents.

Rules of Professional Conduct

- Rule 1.6(c) requires “reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to” confidences of present, former or prospective clients.

Rules of Professional Conduct

- Rules 5.1 and 5.3 – the supervising lawyers' responsibility to protect confidences.
- Under Rules 5.1 and 5.3, lawyers have a duty to make reasonable efforts to ensure that lawyers and non-lawyers under their supervision comply with Rule 1.6 on confidentiality.

Rules of Professional Conduct

- RULE 1.6 – Comment [16]:
  - Unauthorized disclosure or access to client confidences is not a violation of Rule 1.6 if the lawyer made “reasonable efforts to prevent the unauthorized access or disclosure.”
  - Identifies five non-exclusive factors for assessing reasonable efforts.

Rules of Professional Conduct

- Rule 1.6, Comment 16 – Five non-exclusive factors for determining reasonable efforts:
  - (i) the sensitivity of the information;
  - (ii) the likelihood of disclosure without additional safeguards;
  - (iii) the cost of employing additional safeguards;
  - (iv) the difficulty of implementing the safeguards; and
  - (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or software excessively difficult to use).

Rules of Professional Conduct

- RULE 1.6 – Comment [17]
- In transmitting confidences a lawyer need not use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances and other laws, however, may warrant special precautions.

CLOUD COMPUTING IN NEW YORK – THE GOOD NEWS

- Yes you can!

Cloud Computing

- New York State Bar Opinion 842 (2010)
- Cloud storage of client data is permissible if a lawyer uses reasonable care to ensure that the system is secure and that client confidentiality will be maintained.
- Privileged information stored on the cloud remains privileged under CPLR 4548.

Cloud Computing

- CPLR 4548: the privilege is not waived "for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication."

Cloud Computing

- Reasonable Care under New York Opinion 842
- The online data storage provider must have an enforceable obligation to:
  - Preserve confidentiality;
  - Preserve security;
  - Notify the lawyer if served with process requiring the production of the client's data.

Cloud Computing

- Reasonable Care Under New York Opinion 842
- A lawyer must investigate the adequacy of the storage provider's:
  - Security measures;
  - Policies;
  - Recoverability methods;
  - Technology to guard against reasonably foreseeable attempts to infiltrate;
  - Ability to purge and move data to another host.

Cloud Computing

- Reasonable Care Under New York Opinion 842
- A lawyer must:
  - periodically reconfirm the effectiveness of the provider's security measures;
  - stay abreast of rapid changes in the law relating to technology and the protection of privileged information;
  - act diligently to address security failures.
  - Discontinue use of the service absent assurances of remediation of security issues.

Cloud Computing

- Client Consent – NYSBA OPINION 1020
- If the system for storing or sharing documents on the cloud does not provide reasonable protection to confidential client information, the lawyer may still use the system if the lawyer obtains the client's informed consent. See Rule 1.6(a)(1).
- To obtain informed consent the lawyer must disclose the risks that the system does not provide reasonable assurances of confidentiality. See Rule 1.0(j).

Offsite Backup Tapes

- NYSBA 940 (2012): Same rule as for cloud computing. The lawyer must use reasonable care to protect the confidentiality of the client's information.
- Applied the same considerations in determining reasonable care as NYSBA 842.

Remote Access – NYSBA Opinion 1019

- Lawyers may remotely access client files if:
  - "the particular technology used provides reasonable protection to client confidential information, or"
  - "if the law firm obtains informed consent from the client, after informing the client of the risks."
- Because of the rapid evolution of technology and cyber risks, the opinion declined to opine on what constitutes reasonable protection.

Email and Other Electronic Communications

- New York State Bar Opinion 709, September 16, 1998
- There is a reasonable expectation of privacy in email communications.
- “lawyers may in ordinary circumstances utilize unencrypted Internet e-mail to transmit confidential information without breaching their duties of confidentiality . . . .”

Email and Other Electronic Communications

- NYSBA Opinion 709
- When the lawyer is on notice of a heightened risk of interception, or where the confidential information is extraordinarily sensitive nature that "the lawyer must select a more secure means of communication than unencrypted Internet e-mail."

Email and Other Electronic Communications

- NYSBA Opinion 709 :
  - A lawyer must stay abreast of technology to assess any changes in the likelihood of interception and the ability to reduce such risks at reasonable cost.
  - “It is also sensible for lawyers to discuss with clients the risks inherent in the use of Internet e-mail, and lawyers should abide by the clients’ wishes as to its use.”

Email and Other Electronic Communications

- New York State Opinion 820
- "A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to human beings other than the sender and recipient."

Email and Other Electronic Communications

- New York State Opinion 820
- “We would reach the opposite conclusion if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender’s permission (or lawful judicial order).”

Email and Other Electronic Communications

- New York State Opinion 820
- “A lawyer must exercise due care in selecting an e-mail service provider to ensure that its policies and stated practices protect client confidentiality.”

Email and Other Electronic Communications

- ABA Opinion 11-459
- When representing an employee the lawyer should warn the employee of the risk that communications sent on the employer's business device will be read by the employer or another third party.

Email and Other Electronic Communications

- ABA Opinion 11-459
- Other situations in which the lawyer should warn the client of the risk of interception:
  - Use of public computers may lead to interception;
  - Use of a home computer by a client in a matrimonial dispute.

Metadata

- NYSBA 782 (2004)
- Metadata defined: "data hidden in documents that is generated during the course of creating and editing such documents"
- Metadata may reveal "editorial comments, strategy considerations, legal issues raised by the client or the lawyer, legal advice of the lawyer" and other things.
- Must use reasonable care to prevent disclosure of client confidences in metadata.

Metadata

- NYSBA 782 (2004)
- Reasonable care with metadata varies depending on:
  - Subject matter of document
  - Use of templates
  - Number of drafts and comments
  - Recipients
- Must stay abreast of technological advances and potential risks.

Questions

- Thank you!