The Practice of Trusts and Estates in the Digital Age: Ethical Issues in Law Firm Technology and Data Security & Privacy

Jennifer A. Beckage, Esq.
Phillips Lytle LLP, Buffalo

The Practice of Trusts and Estates in the Digital Age:

Ethical Issues in Law Firm Technology and Data Security & Privacy

Presenter: Jennifer A. Beckage, CIPP/US, Partner and Leader, Data Security & Privacy Team, Phillips Lytle LLP

Summary: This session will address the ethical responsibility of trusts and estates attorneys to keep up with evolving technologies, and the potential risks and pitfalls that accompany the use of these technologies, plus data security and privacy concerns.

Overview:

I. INTRODUCTION

Jennifer A. Beckage, Partner and Leader of the Data Security & Privacy and Crisis Response Teams (Phillips Lytle LLP).

A previous technology business owner, who had a successful exit to a publically-traded company where she was retained in a VP position overseeing "e-services" products and operations.

Jennifer has significant experience responding to numerous data breaches, cyberattacks, ransomware and malware incidents and other thefts of data: from the IT response to customer reporting, litigation, and government interactions. While she is a seasoned attorney, her technology and business expertise uniquely positions her to solve complex and significant problems for her global clients. She becomes an extension of an IT department's team — mining the information necessary to solve the issue and prevent further crises.

Jennifer has appeared on behalf of clients in large and contentious matters in New York Surrogate's Court. She is a regular speaker on data security topics, including a speaker for the Erie County Bar Association's 2017 presentation of Surrogate Court Practice in the Digital Age, with speakers including Honorable Barbara Howe, Erie County Surrogate Judge.

Attached is Jennifer's profile.

II. ETHICAL RULES

Attorneys practicing trusts and estates law undoubtedly handle digital information on a daily basis, whether in electronic court filings, electronic drafts of wills and other testamentary documents, e-discovery, emails with clients and opposing counsel, and transfer of files through file transfer systems and programs.

Guided by the ethical rules, attorneys are to take reasonable care in taking steps to protect client confidences, and as explained in point III, may have other legal obligations to take steps to protect certain data. Below is a summary of the New York Rules of Professional Conduct and ethical decisions as it relates to data security and privacy.

A. Reasonableness Standard

1. Rule 1.6: Confidentiality of Information.

    - Rule 1.6(a): "A lawyer shall not **knowingly** reveal confidential information," unless there is consent or authorization to do so as set forth in the rule. (Emphasis added).
    - Rule 1.6(c): "A lawyer shall make **reasonable efforts** to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to [confidential information]." (Emphasis added).

- Rule 1.6, comment [16] Duty to Preserve Confidentiality. "Paragraph (c) imposes three related obligations. It requires a lawyer to make reasonable efforts to safeguard confidential information 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 otherwise subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3."
- Rule 1.6, comment [16] Duty to Preserve Confidentiality. "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (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). 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."

B. Ethics Decisions Addressing Five Questions Around Data Security & Privacy

1. What Data Do You Have And Is It Protected Data?

    a. Rule 1.6(a)(3) defines confidential information.

    - "'Confidential information' consists of 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. 'Confidential information' does not ordinarily include (i) a lawyer's legal knowledge or legal research, or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates." (Exceptions, see Rule 1.6(b)).
    - Comment [2], "A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, or except as permitted or required by these Rules, the lawyer must not knowingly reveal

information gained during and related to the representation, whatever its source."

b. Sensitive data may also be protected by other laws and regulations.

2. How Is Data Transferred?

a. Secure means to transfer data.

- Rule 1.6, Comment [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. Paragraph (c) does not ordinarily require that the lawyer use special security measures if the method of communication affords a reasonable expectation of confidentiality. However, a lawyer may be required to take specific steps to safeguard a client's information to comply with various laws.

b. Inadvertent disclosure.

- Rule 4.4(b): "A lawyer who receives a document, electronically stored information, or other writing relating to the representation of the lawyer's client and knows or

reasonably should know that it was inadvertently sent shall promptly notify the sender."

- Rule 4.4., Comment [2]: "A document, electronically stored information, or other writing is 'inadvertently sent' within the meaning of paragraph (b) when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or other writing is accidentally included with information that was intentionally transmitted."
- For purposes of [Rule 4.4], a "document, electronically stored information or other writing" includes not only paper documents, but also email and other forms of electronically stored information — including embedded data (commonly referred to as "metadata") — that is subject to being read or put into readable form. Rule 4.4, Comment [2].

c. Do not track electronic communications.

- N.Y. St. Bar Assn. Comm. on Prof. Ethics 749 (2001). A lawyer may not ethically use available technology to surreptitiously examine and trace email and other electronic documents. A lawyer may not place a "bug"

in an email that the lawyer sends to determine the subsequent route of the email. The Rules of Professional Conduct prohibit a lawyer from engaging in conduct involving dishonesty, fraud, or deceit and there is a strong public policy benefit to preserving confidential communications.

d. Border crossing and keeping data confidential.

- N.Y. St. Bar Assn. Comm. on Prof. Ethics 2017-5 (2017). During border searches, confidential information may be on the attorney's electronic devices, which may be searched.

3. How/Where Is Data Stored?

a. Backups and record retention.

- N.Y. St. Bar Assn. Comm. on Prof. Ethics 940 (2012). "A lawyer may use off-site backup tapes to store confidential client information if the lawyer takes reasonable care to ensure that the storage system, and the arrangements for its use, adequately protect the confidentiality of such information." See also N.Y. St. Bar Assn. Comm. on Prof. Ethics 842 (2010) (same

principles addressed in determining reasonableness and use of cloud storage).

b. Paper or electronic form.

- N.Y. St. Bar Assn. Comm. on Prof. Ethics 1142 (2018). Except where documents need to be maintained in original form, a lawyer is not required to maintain a file in any particular form.
- N.Y. St. Bar Assn. Comm. on Prof. Ethics 1077 (2015). Lawyers can destroy an original retainer agreement after scanning the original executed copy and maintaining that electronic copy for the requisite period (at least seven years).
- N.Y. St. Bar Assn. Comm. on Prof. Ethics 950 (2012). There should be a reliable method to determine if a record is an original when making decisions about destruction of paper and saving only electronic copies.

c. Cloud storage.

- Jurisdictions have generally approved lawyers' use of off-site third-party providers' cloud and software as a service ("SaaS") services for creating, backing up and storing electronic versions of client files if there are

reasonable assurances that the accessibility and disclosure of information are protected.

- N.Y. St. Bar Assn. Comm. on Prof. Ethics 842 (2010). Addresses Rule 1.6 and reiterates that an attorney must take reasonable steps to protect confidential information. Reasonable care may include consideration of the following: (1) that there is a way to ensure that the provider has enforceable obligations to preserve confidential information; (2) that there is a method by which to investigate providers security measures; (3) that the provider employs technology to guard against access to data; and (4) that the provider has the ability to wipe data/move it. See, N.Y. St. Bar Assn. Comm. on Prof. Ethics 1020 (2014).

4. Who Has Access?

    - N.Y. St. Bar Assn. Comm. on Prof. Ethics 1019 (2014). In providing lawyers remote access to client files, a law firm must take reasonable steps to protect information, but: "Because of the fact-specific and evolving nature of both technology and cyber risks, [this Committee] cannot recommend particular steps that would

constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients."

- N.Y. St. Bar Assn. Comm. on Prof. Ethics 1020 (2014). Authorized persons should have access to cloud storage containing confidential information.
- N.Y. St. Bar Assn. Comm. on Prof. Ethics 939 (2012). Discusses the sufficiency of passwords where two lawyers are sharing a computer.

5. Who Is Responsible?
    - Rule 5.3(b): Responsibility Over Non-Lawyers (*i.e.*, Choosing and Supervising Vendors). A lawyer is responsible for certain conduct of a non-lawyer employed/retained by or associated with the lawyer.
    - Rule 5.3, Comment [3]: "A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client." One such example is using an Internet-based service to store client information. When using such outside services, the lawyer "must make reasonable efforts to ensure that the services are provided in a manner that is compatible

with the professional obligations of the lawyer and law firm. The extent of the reasonable efforts required under this Rule will depend upon the circumstances, including: (a) the education, experience and reputation of the non-lawyer; (b) the nature of the services involved; (c) the terms of any arrangements concerning the protection of client information; (d) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality; (e) the sensitivity of the particular kind of confidential information at issue; (f) whether the client will be supervising all or part of the non-lawyer's work . . . ." When retaining or directing a non-lawyer outside the firm, a lawyer should appropriately communicate directions to give reasonable assurance that the non-lawyer's conduct is compatible with the lawyer's professional obligations.

III. LEGAL LANDSCAPE

In addition to ethical rules, there are other laws and regulations that guide the protection of data that may be in the hands of attorneys.

A. Patchwork of Laws

1. International. Lawyers in trusts and estates may be impacted by international data security laws based upon the individual's residence and other factors (*e.g.*, see GDPR below).
2. Federal. Trust and estate lawyers may be subject to federal requirements, such as HIPAA.
3. State. If a trust and estate lawyer's practice suffers a data security incident, there may be state law reporting obligations, which are primarily driven by where the potentially-impacted persons reside. So, even if the lawyer's practice is primarily in New York, its contacts may reside out of the state, and those state laws would apply for notification purposes.
4. Not all laws are the same: privacy laws, security laws, breach notification laws, and more.
5. Guidance is not uniform, and much is driven by industry and the types of data that are held by the law firm or organization.

B. New Regulations Having Impact On Legal Services

1. General Data Protection Regulation ("GDPR").
    a. Lawyers practicing in trusts and estates may be practicing in a manner and holding onto data concerning persons located in the European Union ("EU"), which would trigger

GDPR. Such personal EU data may appear in wills or in client files, or as a result of the law firm operating in or soliciting work from persons in the EU, and would require attention to GDPR.

b. Overview.

   i. The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation will take effect after a two-year transition period and will be in force May 25, 2018.

   ii. The GDPR applies to all companies located in the EU and members of the European Economic Area (Liechtenstein, Iceland and Norway), as well as companies that control or process the personal data of data subjects located in the EU, regardless of the company's location or citizenship of the individuals.

   iii. Organizations that violate GDPR can be fined the greater of up to 4% of annual global sales or €20M.

   iv. Personal data includes any information related to a natural person that can be used to directly or indirectly identify the person, including a name, a photograph, an

email address, location tracking information, an identification number, biometric data, or an IP address.

v. Some key provisions.

- Breach Notification: Data controllers are required to notify the relevant supervisory authority within 72 hours of having first become aware of a breach. Data processors are required to notify the relevant controllers "without undue delay."
- Right to be Forgotten: Also known as Data Erasure, individuals have the right to require a data controller to erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data, if having the data is no longer required for the original purposes for processing, if an individual withdraws consent, or if the use falls into one of the other enumerated exceptions.
- Right to Access: Data subjects have the right to obtain confirmation as to whether or not their personal data is being processed, including where, by whom, and for what purpose.

- Right to Portability: Individuals can request that their data be provided in a commonly used and machine readable format and transmitted to another controller, if certain conditions are met.
- Lawful basis for processing data. These bases are set out in Article 6 of the GDPR. At least one of these must apply, many will use Consent (Art. 6(1)(a)). Other bases include: Contract (Art. 6(1)(b)); Legal Obligation (Art. 6 (1)(c)); Vital Interests (Art. 6(1)(d)); Public Task (Art. 6(1)(e)); and Legitimate Interests (Art. 6(1)(f)).

c. Lawyers impacted by GDPR should develop internal policies for compliance, including, *e.g.*, privacy policies, privacy notices, incident response plan, and contract negotiation strategy.

2. New York State Department of Financial Services ("NYSDFS") Cybersecurity Regulation.

a. Law firms, including those practicing in trusts and estates, may be subject to the NYSDFS Cybersecurity Regulation, which requires certain data security and privacy safeguards.

b. Overview.

i. Became effective March 1, 2017.

ii. Applies to those regulated by New York banking, financial, and insurance laws.

iii. Focus on protecting non-public information ("NPI"), i.e., business-sensitive information, personal identifiable information ("PII"), and personal health information ("PHI").

iv. Based upon an organization's risk management.

v. 72 hour reporting requirement for qualified cybersecurity events after a determination is made, inter alia, that there is a reportable incident.

vi. Requires certain cybersecurity practices be put in place, including data security policies, with oversight of third-party vendors.

vii. First set of compliance measures was to be satisfied by August 28, 2017, with first compliance certificate due February 15, 2018.

viii. "Covered Entity" is "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization

under the Banking Law, the Insurance Law or the Financial Services Law" (§ 500.01).

ix. Ripple effect to third-party vendors. Covered Entities must evaluate third-party providers. Note, a business can be a Covered Entity and Third-Party Vendor.

x. Regulation contemplates cybersecurity events.

xi. Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information systems.

xii. There is an enhanced role of risk management and how it affects cybersecurity practices.

xiii. Timeline for compliance.

- August 28, 2017:
  - Cybersecurity program (§ 500.02).
  - Cybersecurity policy (§ 500.03).
  - Chief Information Security Officer ("CISO") (§ 500.04).
  - Access privileges (§ 500.07).
  - Cybersecurity personnel and intelligence (§ 500.10).

- Incident response plan (§ 500.16).
- Notice of cybersecurity event (§ 500.17(a)).

- February 15, 2018:
  - Annual certification.

- March 1, 2018:
  - CISO report (§ 500.04(b)).
  - Risk assessment (§ 500.09).
  - Annual penetration testing and bi-annual vulnerability assessments or continuous monitoring (§ 500.05).
  - Multi-factor authentication (§ 500.12).
  - Training and monitoring (§ 500.14(b)).

- September 1, 2018:
  - Audit trail (§ 500.06).
  - Application security (§ 500.08).
  - Limitations on data retention (§ 500.13).
  - Training and monitoring (§ 500.14(a)).
  - Encryption of non-public information (§ 500.15).

- March 1, 2019:

- Third-party service provider security policy requirements (§ 500.11).

- February 15, 2019:
  - Annual certification (§ 500.17(b)). And continue to provide annual certifications thereafter.

xiv. Exemptions.

- Limited and non-limited exemptions.
- The DFS has been sending email notices to those who did not file an exemption or certification.

IV. TECHNOLOGY LANDSCAPE

There are new, emerging, and disruptive technologies that are changing how trust and estate lawyers, and their clients do business.

- Digital assets in estate planning.
- The transfer of digital assets — systems still available to support them.
- Passwords/access to social media and other online accounts.
- Online/electronic wills.
- Smart contracts.
- Blockchain technology.
- Bitcoin and other crypto currencies in estate planning.
- Internet of Things (IOT).

- Artificial intelligence.

V. DATA SECURITY & PRIVACY PRACTICES

Knowing the ethical rules, what laws and regulations apply, and technology available to the attorney, what is the next step to develop a practical and defensible practice to address ethics and data security and privacy? Typical lawyer answer: "It depends." There is no "one-size-fits all" cybersecurity program. Also, there is no prescriptive rule for technical controls. It is a case-by-case analysis. However, no matter what the size of the organization, the approach is the same and can be approached by addressing five key questions (which were addressed in section II):

A. What Data Do You Have and Is It Protected Data?

1. Privileged.
2. Personal Identifiable Information (PII).
3. Personal Health Information (PHI).
4. Non-Public Information (NPI).
5. Sensitive.
6. Such data may appear in wills, trust drafts, estate tax filings, communications, and other files.

B. How Is Data Transferred?

1. Avoid where possible using unencrypted methods to transfer sensitive data, such as web-based email or document share programs to transfer protected data.
2. Emails.
3. Document share programs.
4. Portable devices.
5. Discovery/exchange with opposing counsel.
6. Internally (using web or unsecured mail).
7. Court (efiling and communications).

C. Where Is It Stored?

1. Internally.
    a. Software.
    b. Scanning trust and estate file documents.
2. Externally with vendors.
    a. Cloud.
    b. Contracts.
    c. NDAs.
3. Portable devices.
    a. Monitoring mobile device use.
    b. Home computing.
4. For how long is it stored?

a. De-duplicate.

b. Record retention periods.

D. Who Has Access?

1. Access controls.
2. Strong passwords.
3. Multi-factor authentication.

E. Who is Responsible?

1. Who is monitoring/testing?
2. Staff.
3. Vendors.
4. What does incident response look like?
5. Are there policies and procedures in place?

VI. DEFINITIONS

A. Audit Trail: Listing of activity, information that is used to monitor or validate activity concerning data and systems.

B. Big Data: Large data sets.

C. Biometrics: Data concerning the physical characteristics of an individual (*e.g.*, retina scan).

D. Caching: Saving information about content downloaded so the next time a website is visited, the same information does not need to be downloaded again, which provides for faster page display.

E. **Cloud**: Storing information on a network of locations instead of on your business's network.

F. **Cookie**: A file stored on a user's device that allows another web server to track user activity on the internet and can be used to remember the user to prevent the user from having to log into and authenticate every time the user visits a website.

G. **Encryption**: Converting data using an algorithm into ciphertext, which can only be deciphered (converted back into a readable message) with a "key."

H. **Metadata**: Data that is often hidden from plain view but provides additional information about data. For example, for emails there is hidden metadata that provides the date and time the email was sent and received.

I. **Spam**: Unsolicited emails sent to many addresses.

1. Email Spoofing: Registered domain names may closely resemble a company's legitimate domain name; for instance, with the difference being a single altered letter or character, to target the legitimate domain. Cybercriminals then send a fraudulent or "spoofed" email to employees or customers of the target company, hoping to acquire inadvertently sent out financial information.

2. Phishing: A type of “social engineering” used to trick people into sharing information through, for example, emails using personal information learned from social media in an attempt to give the hacker credibility. Phisher obtains information from the individual in their response to the email, or the individual may unknowingly, by opening the email, open an application that sends the phisher data.

J. **Malware**: Software inadvertently downloaded that can negatively affect your network and systems.

1. Computer Virus: A computer program that can copy itself and cause harm in various ways, such as stealing private information or destroying data.
2. Keylogger: A program that records every keystroke on a keyboard and sends that information to an attacker.
3. Ransomware: A type of malware that usually holds victims’ computer files hostage by locking access to them or encrypting them.
4. Trojan Horse: Malware that appears to be a valid, and not malicious, software.

K. **Multi-factor Authentication**: Process for individuals to validate their identities that requires more than one level of identification

(*e.g.*, a password plus a biometric scan or a message to another device linked to the individual).

L. **Internet of Things**: Internetworking of multiple physical devices, each having network connectivity that enables these devices to collect and exchange data.

M. **Worm**: A malicious program that replicates over a network.

This presentation is an overview of some of the potentially applicable laws and rules and possible exposures and risks and best practices, of which Phillips Lytle strives to achieve and which must be evaluated on a case-by case basis by each firm/business.

The foregoing is for informational and advertising purposes only. The information provided is not legal advice for any specific matter, and does not create an attorney-client relationship. The recipient of this publication cannot rely on its contents. If legal advice is required for any specific matter, please consult with qualified legal counsel. We would be pleased to assist you.

If you would like further information or believe you have a data security incident that requires response and evaluation of notification and reporting requirements, please contact Jennifer A. Beckage, Team Leader of the Data Security & Privacy Team. 716-847-7093.

Phillips Lytle LLP

The Practice of Trusts and Estates in the Digital Age: Ethical Issues in Law Firm Technology and Data Security and Privacy

Jennifer A. Beckage, CIPP/US
Partner and Leader of the
Data Security & Privacy Team

May 4, 2018

Phillips Lytle LLP

I. INTRODUCTION

Phillips Lytle LLP

II. ETHICAL RULES

A. Reasonableness Standard
B. Ethics Decisions Addressing Five Questions Around Data Security and Privacy
   1. What Data Do You Have And Is It Protected Data?
   2. How Is Data Transferred?
   3. How/Where Is Data Stored?
   4. Who Has Access?
   5. Who Is Responsible?

Phillips Lytle LLP

III. LEGAL LANDSCAPE

A. Patchwork of Laws
B. New Regulations Having An Impact On Legal Services
   1. General Data Protection Regulation ("GDPR")
   2. New York State Department of Financial Services ("NYSDFS") Cybersecurity Regulation

Phillips Lytle LLP

IV. TECHNOLOGY LANDSCAPE

- Digital Assets In Estate Planning
- The Transfer of Digital Assets – Systems Still Available to Support Them
- Passwords/Access to Social Media and Other Online Accounts
- Online/Electronic Wills
- Smart Contracts

Phillips Lytle LLP

IV. TECHNOLOGY LANDSCAPE

(cont'd)

- Blockchain Technology
- Bitcoin and Other Crypto Currencies in Estate Planning
- Internet of Things (IOT)
- Artificial Intelligence

Phillips Lytle LLP

V. DATA SECURITY & PRIVACY PRACTICES

A. What Data Do You Have And Is It Protected Data?
B. How Is Data Transferred?
C. Where Is It Stored?
D. Who Has Access?
E. Who Is Responsible?

Phillips Lytle LLP

VI. DEFINITIONS

Phillips Lytle LLP

Thank You

For more information please contact
Jennifer A. Beckage, CIPP/US
(716) 847-7093
jbeckage@phillipslytle.com