Estate Planning, Technology and Ethical Issues

By: Martin M. Shenkman, Esq., Mary E. Vandenack, Esq. and Thomas Tietz, Esq.

A KEY ESTATE PLANNING GUIDE

Law Easy

ChronicIllnessPlanning.org

General Disclaimer

- The information and/or the materials provided as part of this program are intended and provided solely for informational and educational purposes. None of the information and/or materials provided as part of this power point or ancillary materials are not intended to be, nor should they be construed to be the basis of any investment, legal, tax or other professional advice. Under no circumstances should the audio, power point or other materials be considered to be, or used as independent legal, tax, investment or other professional advice. The discussions are general in nature and not person specific. Laws vary by state and are subject to constant change. Economic developments could dramatically alter the illustrations or recommendations offered in the program or materials.

Caveat and Introductory Comments

Points to consider

Are You and Your Clients Being Careful Enough?

- How many clients have all personal estate planning emails sent to their work email addresses? Many save personal estate planning documents on their office computers (do you do the same?). If the client's employment is terminated (or the company sold) what happens to all that confidential information? If the client is the company owner and there is a lawsuit does all that confidential information become discoverable? What impact might this have, if any, on attorney client privilege?
- How many clients who have state of the art protection on their office email and IT systems use an AOL or other generic personal email address for all their financial matters with no protection? (Do you do the same?). A nationally known estate planning attorney uses an AOL email address. Does he have cyber-security protection?
- Does your firm use two-factor authentication wherever possible?
- Do all staff members get cyber-security training to build awareness? (Who is the weak link that may expose your firm?).

Are You and Your Clients Being Careful Enough?

- A well-known attorney at a reputable nationally known law firm sent me a suspicious email recently. I emailed back several people at the firm asking if he had been hacked. TWO DAYS later they confirmed he had been hacked. They NEVER sent out an email informing everyone on their mailing list of the breach and to take precautions. Does that violate ethics rules (likely). What impression does that make on colleagues and clients (I suspended discussions of joining their firm because of this!).
- A well-known estate planning boutique sent out an email that their server was down, and they set up Gmail temporary email accounts. It took weeks before they resolved their issues!
- Do you have sufficient back-ups? Many do not. The time and billing system we use charges $20/month to receive an email with back up files of all data. We get that each month and save it on our cloud-based system which has its own back-up protocols. Then all of our cloud-based data is saved again on an independent cloud-based back up system. I inquired of the billing software company what percentage of professional firms (mostly lawyers) that subscribe get the monthly back-ups. I was told LESS THAN 20%!

Not Suggesting Standard of Practice

- This presentation is **not** intended to imply that any approach is essential or a standard of practice that everyone should follow. Rather the objective is merely to present points estate and other tax practitioners might consider in managing their practice as with a particular emphasis on technology and some of the ethical issues they raise. The goal is to present issues that some practitioners might wish to address in their practice, e.g., in their form retainer agreement, ancillary forms, procedures, etc.

Retainer Agreements Could Reflect Tech/Ethics Concerns

- It may be advisable for practitioners to periodically review estate planning retainer agreements (engagement letters) to update them to reflect new ethics rules, changing practices, integration of new technology into their practice, and other factors.
- Retainer agreements can be used as a framework for the discussion of a potpourri of estate and tax practice management, technology, ethics and related ideas since many of the ideas in this presentation may warrant addressing in retainer agreements/engagement letters.
- Practitioners should not ignore the changes technology and other developments are having on retainer agreements, practice forms, and related practice management steps.
- Indicating to clients some of the practice options in your retainer agreement should constitute disclosure to clients, and their executing such a retainer agreement would seem to be their agreeing to what you have disclosed.

Great Variability by Practice

- The ideas presented must be adapted and modified for every practice.
- A paperless, cloud-based practice will necessarily have to handle these issues differently than a practice that still has yellow pads and Redwelds (and why is that?).
- A practice that predominantly focuses on a large volume of flat fee, smaller wealth, clients will have a different emphasis then a boutique firm serving a limited number of ultra-high net worth clients seeking a different level of service and relationship.
- Ancillary administrative implications of many of the points addressed concerning technology and the state of practice management are adapted at different rates in different firms, some practitioners might view something as excessive, while others view it as a mundane task long ago addressed.

Paperless Practice - Audience Survey

- How many attendees would characterize their practice as paperless?
- How many attendees would characterize their practice as paper-less?
- How many attendees have eliminated all offsite paper document storage?
- How many attendees have revised their engagement letters to reflect their move towards a paperless or paper-less office?

FTC Rules Impact "Financial" Firms

Whether Or Not These Affect Your Firm They Might Be Standards to Consider

FTC New Rules - 1

- Compliance deadline for certain revised FTC Safeguards Rule provisions was extended to June 2023.
- These rules apply to financial institutions. But might these rules provide some indication of steps all companies might consider?
- The FTC Safeguards Rule purpose is to strengthen the data security safeguards that covered companies must put in place to protect customers' personal information. Last year the FTC announced updates to the Safeguards Rule and later issued a to-the-point publication to help streamline your compliance efforts, FTC Safeguards Rule: What Your Business Needs to Know.

FTC New Rules - 2

- Requires covered companies to:
  - designate a qualified person to oversee their information security program,
  - develop a written risk assessment,
  - limit and monitor who can access sensitive customer information,
  - encrypt all sensitive information,
  - train security personnel,
  - develop an incident response plan,
  - periodically assess the security practices of service providers, and
  - implement multi-factor authentication or another method with equivalent protection for anyone accessing customer information.
- Who's covered by the Safeguards Rule? The Rule applies to financial institutions, but it covers businesses like mortgage lenders, mortgage brokers, motor vehicle dealers, payday lenders, finance companies, account servicers, check cashing companies, wire transferors, collection agencies, credit counselors and other financial advisors, **tax preparation firms**, etc.

IRS Publication 4557 Safeguarding Taxpayer Data: A Guide For Your Business

Tax Preparers and Others Should Consider

Introduction

- If you are ever sued over a data breach, you cannot claim you were not aware of the issue, or the steps discussed below as they are set forth in a publicly available IRS publication. This applies not only to CPA firms but to law firms that prepare gift and estate tax returns, trust companies that prepare trust income tax returns, and perhaps even many financial planning firms as the scope of their work expands.
- Data theft against tax professionals is on the rise.
- Addressing data security is an essential step for the largest firms and firms of all sizes including solo practitioners.
- The IRS recommends that tax preparers hire data security experts, buy cyber security insurance, and educate their staff.
- Tax preparers must create written information security plans to protect client data.

Basic Security Steps Recommended for Tax Preparers

- Learn to recognize phishing emails. Remember these scams are intended to entice you to open a link or to open an attachment containing malware.
- Create a written information security plan. See Small Business Information Security - The Fundamentals by the National Institute of Standards and Technology.
- Review internal controls.
- Install anti-malware/anti-virus security software on all devices (including laptops, routers, tablets and phones).
- Encrypt all sensitive files and emails.
- Backup sensitive data.
- Wipe clean or destroy old computer hard drives.
- Withdraw from any outstanding authorizations (e.g., power of attorney for tax information) for taxpayers who are no longer clients.
- Report suspected data theft or loss to the IRS immediately.

Use Security Software

- Anti-virus prevents malware from causing damage to a computer.
- Anti-spyware prevents unauthorized software from stealing information on your computer.
- A firewall blocks unauthorized access to your system.
- Drive encryption protects information from being read if a device is lost or stolen.
- Whatever you use must be updated regularly.

Other Steps

- Use strong passwords.
- Use multi-factor authentication.
- Secure your wireless network.
  - Use a strong unique password for the administrator.
  - Use a name for your router that is not identifiable (e.g., don't call it Tina Tax Saving Service, LLC).
- Protect stored client data.
  - Backup dated to secure cloud storage.
  - Use drive encryption.
  - Don't attach USB devices with client data to public computers.
- Be careful with and perhaps never use "free" software.
- Use separate personal and business email accounts. Do you consistently do this?

Report Data Breaches

- Report data breaches to:
  - IRS.
  - FBI.
  - Police (file a police report).
  - States in which you file returns see StateAlert@taxadmin.org
  - State attorney general for states in which you prepare returns.
- Retain a cyber security expert to assess the breach.
- Report to your insurance company.

IRS Publication 5708 Creating a Written Information Security Plan for your Tax & Accounting Practice

Documentation Tax Preparers and Others Should Consider Preparing

Introduction

- IRS Publication 5708 discusses the requirements for tax preparing firms to create a Written Information Security Plan, a “WISP.”
- The Gramm-Leach-Bliley Act (GLBA) is a U.S. law that requires financial institutions to protect customer data.
- In its implementation of the GLBA, the Federal Trade Commission (FTC) issued the Safeguards Rule to outline measures that are required to be in place to keep customer data safe. One requirement of the Safeguards Rule is implementing a WISP.
- Under the GLBA, tax and accounting professionals are considered financial institutions, regardless of size. Financial institutions subject to the Safeguards Rule include mortgage brokers, real estate appraisers, universities, nonbank lenders, and check cashing businesses.

Written Information Security Plan Requirements

- As a part of the plan, the FTC requires each firm to:
  - Designate one or more employees to coordinate its information security program.
  - Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks.
  - Design and implement a safeguards program, and regularly monitor and test it.
  - Select service providers that can maintain appropriate safeguards by ensuring your contract requires them to maintain safeguards and oversee their handling of customer information.
  - Evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

What is Appropriate to Include in a WISP?

- The publication discusses that a security plan should be appropriate to the firm's size, scope of activities, complexity, and the sensitivity of the customer data it handles. There is no one-size-fits-all WISP. For example, a sole practitioner can use a more abbreviated and simplified plan than a 10-partner accounting firm (note that the publication's language directly referenced accounting firms).
- Three areas are discussed for focus in a WISP:
  - Employee management and training.
  - Information systems.
  - Detecting and managing system failures.
- It is noted that the WISP is meant to be an "evergreen" document, regularly reviewed and updated due to changes in technology and to the size, scope, and complexity of the firm's business.
- Do you consider the changes in the nature of your practice and how it may affect the data security needed? For example, if the nature of the confidential data you hold changes due to increased scope of your services, it may cause you to be in a higher "tier" of required data security to protect that data.

Addressing the WISP with Employees

- The IRS references creating an Employee/Contractor Acknowledgment of Understanding document for all personnel to keep a record of training and understanding of the policies in your WISP.
- The publication references “contractors.” Consider whether this means any third-party contractors that are provided access to the firm’s technology infrastructure must be included in training and implementing a WISP.
- Signing and dating training creating a documentation trail a firm can keep on file for several reasons.
  - Show your adherence to the spirit of compliance and to have an enforceable accountability point in the event of a negligent employee.
  - The publication recommends that these acknowledgments be updated at annual training intervals and kept on file.
  - Query as to how many firms have signed training documents on file, let alone update them annually?
- Once completed, the WISP should be maintained in a format that others can easily read, such as PDF or Word. Making a WISP available to employees for training purposes is encouraged.
- Storing a copy offsite or in the cloud is a recommended best practice in the event of a physical disaster.

Addressing the WISP with Third-Party Vendors

- The sample WISP provided in the publication includes the following statements regarding third-party vendors:
  - "…Requiring third-party service providers to implement and maintain appropriate security measures that comply with this WISP…"
  - "…Any third-party service provider that does require access to information must be compliant with the standards contained in this WISP at a minimum..."
- Exceptions listed are are tax software vendors and e-Filing transmitters, state and federal tax authorities. IRS Publication 1345 is referenced for more information.
- There is no additional information provided in the publication regarding vetting third-party vendors. Consider what would be reasonable for confirming a third-party vendor has "appropriate security measures?"
- What is the standard? How should the security measures of a third-party vendor be evaluated to determine if they meet or exceed the WISP requirements?
- For smaller firms, will relying on the advice of an IT consultant be sufficient? These questions do not appear to be answered in the publication.

Sample Outline for a WISP- 1

- A sample outline is provided in the publication.
- Define the WISP objectives, purpose, and scope.
- Identify responsible individuals.
  - List individuals who will coordinate the security programs as well as responsible persons.
  - List authorized users at your firm, their data access levels, and responsibilities.
- Assess Risks.
  - Identify Risks.
  - List types of information your office handles.
  - List potential areas for data loss (internal and external).
  - Outline procedures to monitor and test risks.
- Inventory Hardware.
  - List description and physical location of each item.
  - Record types of information stored or processed by each item.

Sample Outline for a WISP- 2

- Document Safety Measures in place
  - Suggested policies to include in your WISP:
    - Data collection and retention
    - Data disclosure
    - Network protection
    - User access
    - Electronic data exchange
    - Wi-Fi access
    - Remote access
    - Connected devices
    - Reportable Incidents
  - Draft Employee Code of Conduct
- Draft an implementation clause
- Attachments

Sample Template for a WISP

- The publication includes a 12-page template of language to incorporate into a WISP. It also includes numerous sample attachments, including rules of behavior for protected information, security breach procedures, an employee acknowledge of understanding, and more.
- A PDF of the publication and sample documents can be accessed at https://www.irs.gov/pub/irs-pdf/p5708.pdf

Communications

Rules Affect Lawyers But May be Worth Consideration by Others

Communication – RPC 1.4

- A lawyer shall fully inform a prospective client of how, when and where the client may communicate with the lawyer.
- A lawyer shall keep a client reasonably informed about the status of a matter and promptly comply with reasonable requests for information.

Ethics Opinion 477

- Ethics Opinion 477 updates Ethics Opinion 99-413 to reflect the now common use of tech such as tablet devices, smartphones, and cloud storage.
- Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties under Rule 1.1 of the ABA Model Rules concerning competency, confidentiality, and communication.
- Comment 8: Modified to include **that lawyers should keep abreast of changes in the law and its practice "including the benefits and risks associated with relevant technology."**
- Lawyers must take reasonable efforts to ensure that communications with clients are secure and not subject to inadvertent or unauthorized security breaches.

Ethics Opinion 477 (Cont'd)

- Lawyers must use "**reasonable efforts**" to ensure the security of client information. Citing the ABA Cybersecurity Handbook, the opinion explains that the reasonable efforts standard is a fact-specific inquiry that requires examining the sensitivity of the information, the risk of disclosure without additional precautions, the cost of additional measures, the difficulty of adding more safeguards, and whether additional safeguards adversely impact the lawyer's ability to represent the client.
- The opinion notes that generally lawyers may use unencrypted email when communicating routinely with clients. **But what does this mean, and doesn't it depend on what is being sent?**

Ethics Opinion 477 (Cont'd)

- The opinion included several aspects to consider when sending unencrypted emails:
  - Understand the nature of the threat.
  - Understand how client confidential information is transmitted and where it is stored.
  - Understand and use reasonable electronic security measures.
  - Determine how electronic communications about clients should be protected.
  - Label client confidential information. This should include digital files.
  - Train lawyers and non-lawyer assistants in technology and information security.
  - Conduct due diligence on vendors providing communication technology.

Communication – Use Technology To Quickly and Efficiently Corroborate That You Have Met Ethics Requirements

- Use regular monthly billing as a means of communication, not only as a means of billing. **Example**: Footers with information about new tax developments.
- Save covering emails into the client file to corroborate communications.
- Use the calendaring system to document efforts to communicate with clients. For example, if a client cancels a meeting do not delete that meeting entry from the calendar. Rather, mark it as "Cancelled by Client." Perhaps minimize the calendar entry. Consider excluding historical calendar data from document destruction policies, saving calendar data indefinitely. **Example**: Searching the client's name in a case management system, or even Outlook, can provide a history of meetings, attempted meetings, etc.
- Mark all client follow up in the billing system even if as a no charge notation entry to create a history of efforts to communicate with the client. **Example**: Administrative staff calling a client to schedule an update meeting should note the call in the billing system "no charge" so that there is a record of efforts to reach the client.

Communication - Audience Survey

- How many attendees use email blasts to inform clients of new changes in the law?
- How many attendees send an email newsletter?
- How many attendees use billing to communicate with footers, enclosed articles or other adaptions?

Communication – RPC 1.4

- “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.”

Communication – Using Technology

- Use web meetings to provide a convenient and cost-effective means to provide clients an overview of complex documents. Document the review to corroborate what was discussed. We save the document with notes of the meeting and an indication “mtg with client” and a date.
- Provide a summary of key provisions of complex documents. Document generation systems may provide this automatically.
- Use schematics to illustrate transactions. These can readily be created in Excel or estate planning software.
- Email drafts of documents in advance of meetings and signings and save the covering email as proof that the clients were provided documents to review in advance.

Communication - Audience Survey

- How many attendees commonly use web meetings as the primary means of meeting with clients rather than in-person meetings?
- How many attendees commonly use web meetings to communicate with a client's other advisers?

Communication – Using Technology

- Use email marketing tools, e.g., MailChimp, to inexpensively and quickly disseminate updates, planning information and other communications to educate and inform clients.
- What if regulations or other change may affect past transactions? What can practitioners do? Attorneys have an ethical obligation to keep clients informed of significant changes in the law. Use client communications above (e.g., firm newsletters), footers on bills (see sample provisions), and enclosed articles, sample checklists or memorandum with all bills and reference the materials provided in the footers on the bills.
- **The key is that technology makes it easy and inexpensive to communicate information to clients and to corroborate that you have done so. The common thread of many significant malpractice cases is "the advisers never told me…." Tell them and save proof.**

Email Retention And Other Policies

- Rules based on paper file storage no longer make sense

Email Retention – Pre-Seminar Survey

- I asked 12 practitioners about their email retention policies:
  - One knew and said they keep every email forever.
  - 3 had their IT people get back to me and the policies ranged from 90-days to forever, from emails saved to the DMS to all emails.
  - 7 had no idea.
  - 1, a partner in a 10-person firm replied, “What is an email retention policy.”

Email Retention – Audience Survey

- How many attendees have firm email retention policies?
- What are they?

Email Retention Policies

- Software/tech options.
- Litigation considerations.
- From one firm's document retention policy statement: "For efficient identification, retrieval, and deletion of email and other electronic documents pursuant to this policy, attorneys and staff are required to organize and store all business record email and other electronic documents in separate folders designated for each client matter in the firm's electronic document management system."

Client Property

The thorn in going paperless

Safekeeping of Client Property - RPC 1.15

- ABA Model Rule 1.15(a) provides that complete records of client trust account funds and other property shall be kept and preserved by the lawyer for a certain period of time after the termination of the representation. The number of years varies by jurisdiction, e.g., 7 years.
- A lawyer must hold client entrusted property separate from lawyer's property, e.g., client trust accounts, and original documents, e.g., a will. Original documents retained are subject to RPC 1.15, e.g., storing wills.

Client records – File Destruction

- Simply because you can destroy the file after 7 years does not mean that you should. Consider self-protection when deciding to what to do with the file. If there is the possibility of a malpractice claim at some point, might the file be critically important for the lawyer's defense? Or might it be harmful? But the policy should be consistent.
- If any portions of the file are destroyed, care should be taken to preserve the confidentiality of the information contained in the documents.
  - If there is a litigation hold all electronic records should be preserved until the litigation has been concluded.
- An index of the file records that have been delivered to the client or destroyed should be maintained.
- One large firm's retention/destruction policy: "Unless otherwise specified by the Billing Partner, a destruction date equal to ten years from the date the matter is designated closed will be assigned to all files, **with the following exceptions…estate plan, estate administration, ….files will be permanently retained**."
- See NJ Ethics Opinion 692 and RPC 1.4.

Personal Laptops

- If an attorney or staff member creates or edits an electronic business record using a home computer, laptop, or other device, that person must save the record on the firm's electronic document management system as soon as possible. No firm attorney or staff member is permitted to store electronic business records anywhere other than the firm's electronic document management system.
- Another view, we have most documents stored on laptops to facilitate working during power outages, internet interruptions, on 10-hour plane rides when internet is not accessible, etc.

File Destruction - Audience Survey

- How many attendees retain files longer than 7 years?
- How many attendees have electronic files deleted automatically after 7 years?

Safekeeping of Client Property - Technology

- In a paperless office is there any client property?
- During the process of going paperless care should be taken to avoid accidental destruction of client property. See sample memorandum of taking an estate planning practice paperless.
- Record retention rules evolved in a paper environment. As the cost of electronic storage becomes insignificant (as contrasted with in-office and offsite paper storage) will the ethical rules evolve to require permanent storage of client data?
- Is electronic storage really moving to no cost? Consider the cost of finding relevant information if everything is saved forever.

The Client “File”

- The contents of a client’s file belongs to the client and, upon request, an attorney must provide the client with the file.
- Rule 1.16(d) governs what a lawyer must do when asked by the client for the file. When a lawyer withdraws from representation, he or she must take reasonable steps to avoid foreseeable prejudice to the client’s rights, which includes delivering to the client all papers and property to which the client is entitled. The rule does not specify what papers and property the client is entitled to receive. What is a “client file” in a paperless office?
- Maintaining a client file has historically been an important part of the service counsel provided clients, but electronic storage is essential free for clients as well. So, clients can also readily store all their documents permanently.
- **If a client has all original documents, has received all memorandum, letters and emails, what is left that the lawyer has that must ever be turned over to the client?**

Cloud Storage

- A law firm is permitted to store the electronic materials relating to the client on a remote server under third-party control as long as the law firm carefully selects the third-party company to ensure that the information is kept confidential.
- **What should be done to corroborate the selection**?
- Attorneys must take reasonable care to protect a client's information in a cloud environment. See NYSBA Ethics Opinion 842 (9/10/10).

Client Property - Audience Survey

- How many attendees have no original client property?
- How many attendees have no in office paper document storage?
- How many attendees have no offsite paper document storage?

Office Sharing; Virtual Offices; Office of the Future

Applying Ethics Rules to Evolving Physical Practices

Office Sharing Arrangements and the Virtual Office

- **ABA Formal Opinion 507 was issued July 12, 2023**, and addresses office sharing arrangements. Opinion 507 creates issues that should be considered as more firms become virtual and use office sharing rental arrangements when they have in-person meetings. The Opinion expressly contemplates virtual practice as it applies to "…lawyers sharing an office suite, receptionist, and conference room as part of a virtual law practice…"
- Opinion 507 introduction states: "It is **generally permissible for lawyers to participate in office sharing arrangements with other lawyers** under the ABA Model Rules of Professional Conduct. At the same time, office sharing lawyers should appreciate that such arrangements will require them to take appropriate measures to comply with their ethical duties concerning the confidentiality of information, conflicts of interest, supervision of non-lawyers, and communications about their services. The nature and extent of any additional safeguards will necessarily depend on the circumstances of each arrangement."

Comments on Opinion 507

- Opinion 507, while contemplating virtual practice, does seem somewhat focused on firms sharing permanent physical offices, and may be less clear as to how it should be applied to a firm that is virtual based that rents office space from time to time through an office rental/sharing service. Perhaps that is because such practice models are likely still a small part of the overall practice of law and are relatively new. The latter may grow in use especially as technology has made it so easy for firms to transform to paperless and virtual practices. Further, such arrangements may be more cost effective and nimble, especially for smaller or solo practitioners.
- For those types of arrangements, the Opinion may not provide specific enough guidance. For example, virtual firms cannot have a different lobby area to greet clients. You can't do that if you're renting for a day or perhaps a few hours. But the concepts of Opinion 507 can and should be addressed.
- Thus, as explained further below, practices that are virtual or moving in that direction may have to interpret Opinion 507 and endeavor to apply it to their circumstances.

Comments on Opinion 507

- The standard in Opinion 507 uses similar and vague "reasonableness" standards like that in various Opinions governing the use of technology generally. That is a positive and should be lauded because what is "reasonable" will vary based on practice and circumstance. But, that type of standard might suggest that firms and practitioners might consider taking steps to corroborate that what they are doing to address the points of Opinion 507 are in fact "reasonable."
- If you are or plan to become a virtual and rely on office sharing/rental arrangements precautions might be advisable considering Opinion 507. Note that some firms, even those heavily reliant on physical offices may leverage technology and office sharing arrangements in jurisdictions where partners are admitted and may visit or have vacation homes to have a presence in those jurisdictions. If that is done consider creating a firm memorandum to discuss technology, how you use it, how you intend to use the office sharing, and that no confidential client data would be left in the office sharing facility at any time (especially if the firm is paperless and cloud based), that data (e.g., documents to be signed at an in-person meeting) will only be in the office at the same time the firm is, etc.

Comments on Opinion 507

- "Lawyers participating in these arrangements must take appropriate steps to secure client information and clearly communicate the nature of the relationship to the public and their clients."
- Might this suggest that firms should **communicate in their retainer agreement,** firm brochures and/or the firm website, how their firm operates. "The firm uses office rental sharing arrangements to accommodate clients and can meet at any such location that is most convenient for the client. These arrangements, however, entail outside firms, law or other, using the same facilities at the same time. While conference rooms are private, reception and other common areas are not occupied only by our firm. Thus, confidential discussions and display of confidential materials should be done only with caution, if at all, in such areas." Might that be the type of disclosure that is appropriate?

Comments on Opinion 507

- Opinion 507 states: “The physical arrangement of the shared office space, however, must not expose client information to other office-sharing lawyers and their staff. Everyone should also avoid discussing cases in or near common areas, which could lead to the disclosure of client information.” This may present yet another issue. Office sharing/rental arrangements have common work areas. If a staff member or attorney will be working before or after a client meeting in a common area, caution is in order. Perhaps private rooms in some instances may warrant renting for such use and staff and attorneys might be prohibited from using common work areas unless those work areas provide sufficiently privacy that non-firm personnel cannot view client confidential materials.
- Opinion 507 states: “…installing privacy screens on computer monitors and locking down computers when not actively in use; clean desk policies; and regular training and reminders to staff of the need to keep all client information confidential…”
- Privacy screens advertise: “Our advanced multi-layered film filter blacks out your screen when viewing from the side, while maintaining a crystal-clear screen straight-on.” But they are not compatible for use with touch screens and the implication is that someone is viewing your screen from an angle. That may be relevant sitting on an airplane but may not be helpful or even necessary in an office sharing arrangement.

Comments on Opinion 507

- Opinion 507 states: “locking down computers when not actively in use; clean desk policies; and regular training and reminders to staff of the need to keep all client information confidential. Office sharing lawyers can also restrict access to client-related information by securing physical client files in locked cabinets.”
- When working in a shared rental office environment if the firm is not paperless, then precautions will be required to secure paper/physical documents if ever left unattended. If staff or an attorney goes to lunch or a meeting outside the virtual office location, there may not be any practical means of locking or securing a temporary office so that computers may have to be locked/password protected to open or taken physically with the staff or attorney leaving and returning.

Applying Opinion 507 to One Firm's Office Sharing Offerings

- Following is a list of services from a company that provides physical office shared space for this environment: https://www.davincivirtual.com/

Davinci has thousands of virtual office locations available. Pick what best suits your business, then decide which features work with your needs and budget. **Considerations in light of Opinion 507 are added in green**.

- Davinci's virtual office benefits include:
  - A physical address.
  - A lobby greeter – **limit information and request that client names not be announced in a public space.**
  - A lobby directory listing.
  - A business support center – **consider whether confidential client information can be processed in a central support center where the firm has no control over the personnel, cannot train the personnel as to confidentiality and may not be able to control whether physical documents or even typing is visible by unknown people.**
  - Mail services – **Is there a concern of confidential client mail being handled by non-staff persons?**
  - High-speed internet – **precautions and safeguards on software used by firm members on public internet must be considered.**
  - Presentation tools.
  - Catering.

Applying Opinion 507 to One Firm's Office Sharing Offerings

- **Considerations in light of Opinion 507 are added in green**.
- Physical Benefits.
  - The physical benefits of a virtual office differentiate them from the characteristics typical of a fully remote office. These features include:
  - A physical business address.
  - A place to receive mail and mail services – **consider the possible impact of non-firm personnel handling mail that may include client confidential information and whether that is an issue.**
  - A live receptionist – **if a receptionist is to handle client phone calls how might that be addressed to control the dissemination of confidential client information. That may be no different then the common use of answering services and virtual receptionists that have been common for many years.**
  - The ability to rent meeting rooms – **individual meeting rooms may be secure when in use, but caution may have to be taken if a lunch or other break is taken to assure that any physical papers or devises that might be left in the room are secured.**
  - Copying and printing services -- **as with the business support center on the prior page consideration should be given to who has access to the center where printing and copying are handled and how confidential client information may be protected. But is that really any different than law firms using independent copy centers that have been in use for many decades?**

Confidentiality

Challenges to address

Confidentiality of Information - RPC 1.6

- “A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized to carry out the representation, and except as stated in paragraphs (b), (c) and (d).”

Confidentiality of Information - RPC 1.6(c)

- ABA Model Rule 1.6(c): "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.“
- Comment 18, paragraph (c): Requires a lawyer to competently act to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure.
- What is reasonable efforts? This is a nebulous statement that needs both common sense applications, best judgment, and to review what opinions consider reasonable to determine your technology policies moving forward.
- Reasonable efforts may be interpreted to include due diligence regarding technology procedures. Required training for employees, thoughtful policies implemented and followed, etc. all show that due diligence and that reasonable efforts were made to prevent disclosure.

Confidentiality of Information – Technology Crime Statistics

- Every day, about 7 million data records are lost or stolen.
  - 72% of breaches are done by a malicious outsider.
  - 18% are result of accidental loss.
  - 9% are result of malicious insider.
- The FBI's Internet Crime Complaint Center in 2022 received 800,944 complaints. In 2017 there were only 301,850 malicious incidents, so in 5 years it almost tripled!
- The potential total loss has grown from $6.9 billion in 2021 to more than $10.2 billion in 2022. This was only $1.4 billion in 2017.
- The chance of arresting a cybercriminal was 0.31% in 2018.

Confidentiality of Information – Technology Crime Statistics Cont.

- Social Catfish, a website that works to identify online scams, posted an analysis of the state of internet scamming in 2023.
- The top 10 most-scammed countries in the world were found to be:
  - United States: 479,181
  - United Kingdom: 284,291
  - Canada: 5,517
  - India: 2,550
  - Australia: 2,489
  - France: 2,061
  - South Africa: 1,929
  - Germany: 1,494
  - Brazil: 1,181
  - Mexico: 1,119
- Based upon these statistics, the United States may have more scamming victims than **the rest of the world combined**.
- The report can be accessed at https://socialcatfish.com/scamfish/state-of-internet-scams-2023/

Confidentiality of Information - Technology

- Consider using encrypted emails, e.g., Sharefile, to transmit documentation with TINs, etc.
- Take precautions to protect the physical office facilities, alarm systems, etc.
- Take precautions to protect the integrity of electronic data. This might include:
  - Encryption and password protection of laptops, smartphones and other equipment.
  - Providing an internet access, password protected, outside the firm firewall, for clients and other visitors.
  - Protect all systems with appropriate virus protection, spam filters, intrusion protection,etc.

Confidentiality of Information - Technology

- Consider the use of a third-party password manager to store passwords, allowing “strong” passwords (i.e., a long string of random letters, numbers, characters such as !,@,$, etc.) to be employed on programs used by the firm in an easier manner, including those that store confidential client information.
- Professionals should exercise caution in using built-in password managers on web-browsers such as Google Chrome, as third-party programs may have greater encryption protections (such as the use of two-factor authentication to access the passwords stored in the program).
- Examples of third-party password managers include:
  - Last Pass- https://www.lastpass.com/ (However they had a recent major hack)
  - 1Password- https://1password.com/ Our firm uses this program.
  - NordPass- https://nordpass.com/
  - Keeper Security- https://www.keepersecurity.com/
  - Dashlane- https://www.dashlane.com/

Confidentiality of Information - Technology

- Use best judgment regarding when you need to take extra security measures. Consider the following reasonable effort factors:
  - Sensitivity of Information.
  - Likelihood of disclosure if you do not employ additional safeguards.
  - Cost of employing additional safeguards.
  - Difficulty of implementing additional safeguards.
  - Extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., difficult to use).

Confidentiality of Information-Breach

- ABA formal opinion 483 states that if a data breach occurs that involves client information, lawyers have a duty to notify current clients of that data breach.
- Attorneys have a requirement to monitor for data breaches so current clients can be informed if one is discovered.
- Interestingly, there is no requirement to notify former clients.

Confidentiality - Audience Survey

- How many attendees use secure/encrypted email regularly?
- How many attendees use secure cloud-based portals to store client documents (e.g., Sharefile)?
- How many attendees are aware of a Data Loss Policy (DLP) at your firm?

Collaboration and Attorney Client Privilege

The world is too complex and inter-related to practice without collaboration

Privilege

- Attorneys are obligated to safeguard the confidences of their clients.
- Generally, the attorney is responsible to protect all communications between the client and the attorney from disclosure without the permission of the client.
- The Privilege belongs to the client as opposed to the lawyer. The communication of confidential information and the privilege can both play an important role in a range of estate planning matters. Address, with some specificity, in the engagement agreement and other communications.
- See Model Rules of Professional Conduct ("MRPC") §1.6 *Cohen v. Jenkentown Cab Co*., 238 Pa. Super. Ct. 456, 357 A.2d 689 (Pa. Super. Ct. 1976).

Privilege

- Technology has complicated the potential implications of Privilege in designating acceptable forms of communication. Technology has also provided some solutions to these challenges as well. In an age where many routine communications occur electronically, the client might not pause to consider the implications of a mode of communication. For example, a client might communicate with her personal (not business) counsel through her company email account, saving documents on a company file server, or using a company computer to engage in such communications.

Collaboration

- Collaboration might have been merely a footnote not too many years ago.
- Today it warrants prominent consideration and is an integral part of many estate planning practices.
- Estate planning is more complex and intricate considering changing demographics and what seems to be a permanent state of uncertainty as to the tax laws.

Collaboration

- A client intake form might include an authorization to be certain clients understand the importance of collaborative disclosures and provide the relevant contact at the outset of the engagement.
- The mere fact that the estate planner has authorization to collaborate does not mean other advisers have done so. Other advisers may refuse to collaborate until they have authorization from the client.
- Counsel could prepare a letter from the client to all advisers authorizing and directing collaboration that the client can sign, and counsel can distribute.

Collaboration and Privilege – Power of Attorney

- **Sample Clause**: “By executing this Power of Attorney the Principal agrees and acknowledges that Principal hereby waives the attorney client privilege with the law firm who prepared this document, solely for the purposes of permitting said attorneys and firm, or its employee attorneys and any successor firm (collectively, "Attorney") to communicate with the Agent and Alternate Agents hereunder, including disclosing Principal's confidential information to them, and providing Principal's confidential documents to them with respect to their carrying out their duties hereunder. Attorney shall have the right, but no obligation under any circumstance, to act hereunder (including but not limited to distributing any copy or original of this Power of Attorney). Attorney shall be held harmless for any good faith action, or refusal to act, hereunder.”

Collaboration and Privilege

- Carefully consider if any exceptions should be made to the waiver of conflicts discussed. Another approach might be to have another Agent or successor Agent act with respect to a business, for example, in which the Agent holds an interest. Alternatively, the interested Agent could be permitted to act but could be required to give notice of the actions to a successor agent and/or at least one person (or more than one) who could be a beneficiary of the Gift provisions in this Power (presuming that such persons are objects of your largess).
- Consider whether the client is or should be willing to waive the attorney client privilege. If not, there may be an issue with you as attorney disclosing information to the agent which may become essential for the agent to have to act to protect your interests under this Power.

Collaboration and Privilege

- The attorney's duty to represent does not end merely because of the client's disability. See Model Rules of Professional Conduct 1.14(a). An attorney, as far as reasonably possible, is to maintain a normal client-lawyer relationship. An attorney can take protective actions for their client depending on the circumstances. Model Rule 1.14(b).
- An attorney may reveal confidential information about you when doing so to the extent reasonably necessary. Model Rule 1.14(c). This is generally limited to situations where you are at risk for substantial physical, financial or other harm. Therefore, it may be advisable to authorize greater latitude in order for the attorney to take steps you might wish taken in less onerous circumstances.

Privilege can Affect the Attorney Personally

- Similar issues can also affect practitioners. If the attorney sends personal emails from a work email address or stores personal documents or communications on a laptop that is a practice laptop, in later litigation, discovery and data searches might reveal the practitioner's personal emails and estate planning documents.
- If a personal laptop is used consider a written policy to save no client work there, transfer it all to the office system to be saved in accord with whatever the firm document retention policy is (see below). Consider documenting the characterization of personal equipment as personal in the firm's technology records. But again, there are different views as noted above.

Billing Rates and Methods and the Impact of Technology

Hourly may not be fair to the practitioner

Billing and Technology

- Technology is changing how some practitioner's bill.
- Various tasks that use to be quite costly, may be more efficient and routine because of technological changes. Thus, some tasks that had been billed on an hourly basis might now be billed on a flat fee or hybrid basis in order to be fair to the practitioner/client.
- As practices evolve to paperless, cloud-based document generation driven models, the traditional paradigms for billing will be unfair to clients in some instances, and unfair to practitioners in others. Modifications to billing practices may continue to evolve over time.
- Assure that the client has a clear understanding of how they will be billed specified in a written retainer agreement.

Billing and Technology - Audience Survey

- How many attendees routinely use anything other than hourly billing ?
- How many attendees practicing estate planning use document generation software?
- Of those that using document generation software, how has it changed your billing?

Billing and Technology

- When rates or fee structures are changed, a footer could be incorporated on the bill explaining that an increase or other change has been put into effect. Many billing systems easily accommodate the addition of standard footers to some or all bills to facilitate such communication. In fact, footers designed to appear on all bills can provide an important and no-cost way to communicate important billing, administrative and even tax development information to many clients.
- Firm newsletters and announcements can also be put to similar use. If the latter is done, consider saving copies of all such general client communications in a single file.

Possible Provision in Engagement Letters

- The following fees will be charged as supplemental fees, in addition to regularly hourly rates for work completed, for the preparation of the documents indicated below. These fees are charged in addition to our regular hourly fees to address the substantial and ongoing investment of time and cost we have, and continue to make, in technology, forms, and other matters that have and continue to provide substantial efficiencies to clients. If you wish to discuss the rationale or application of these fees, please call.

Vetting the Prospective Client

Internet changes the dynamic

Technology Changes Client Vetting

- Some practitioners take steps in advance of being retained. Some refer to these preliminary steps as “pre-engagement.”
- Turning away a bad case or client is important to the security, success and atmosphere of every firm.
- Example: if the prospect has significant assets overseas what issues might this suggest? Has the prospect complied with all the requisite reporting requirements?

Technology Changes Client Vetting

- It may be advisable to perform some due diligence on a prospective client before the prospect becomes an actual client.
- The internet has made it easy and, other than staff time, cost free.
- Have staff search the client's names, and business names, prior to accepting the engagement.
- If issues are identified, address them before accepting the prospect as a client.

Technology Changes Client Vetting

- If a prospective client searches raise worries, e.g., a physician prospect who has scores of negative complaints that sound substantive, perhaps the firm should consider whether that reputation risk is something it is willing to take on in the context of estate planning that typically will entail transferring assets into entities and irrevocable trusts. If the firm is willing to accept the client, it might choose to discuss these concerns up front as well as steps and costs of addressing them.
- To avoid any prospective client claiming that for an inappropriate reason they were singled out, it may even be advisable to perform the same procedures for all clients.

Technology Changes Client Vetting - Audience Survey

- How many attendees routinely vet clients?
- What websites or services are used? Google Search? What else?
- Of those that vet clients how many acknowledge that in their engagement letter?
- How else do you inform prospective clients?

Document Generation Transforms Estate Planning

How document generation changes drafting and practice

Introduction to Automation - 1

- Estate plan deliverables often involve complex documents.
  - Initial intake forms.
  - Recommendations with asset schedules and flowcharts.
  - Trusts, wills, and asset transfer documents.
- What's wrong with the status quo?
  - Lawyers often draft new documents by pulling up an existing document from a previous matter or transaction.
  - In 2023, no lawyer should ever draft by pulling up a document prepared for another client and using that as a starting point.
    - Finding the right document can be time consuming.
    - There is a high likelihood that you will leave something in that shouldn't be in the document.
    - There is a high likelihood that something that should be in the document won't make it in.
    - Find and Replace rarely finds everything.

Introduction to Automation - 2

- Using an old document means you will need to keep fixing formatting issues that are carried forward.
- Many of these “starting point” documents were designed very specifically, and revised based on discussions, with regard to the specific client the document was drafted for. Such provisions could be “landmines” in another client’s document.

Upgrading Skills For Document Drafting

- Lawyers (and staff) should improve their own word processing proficiency or use speech recognition technology.
- Lawyers should recognize the limitations of using other client documents and dictation/transcription and seek new and efficient tools.

Purchase Subscription Drafting System

- Subscription drafting systems automate document generation, but they include the documents that you will use. That is, you use the forms developed by the subscription service rather than the documents that you developed.
  - WealthDocx.
  - Interactive Legal.
  - ElderDocx.
  - Practical Planning System.
  - Lawgic.
  - ADAPT Solutions (formerly Fore Trust Software).

Outsourcing

Simple, Cost Effective, Transformative

Outsourcing

- Email communications make it seamless.
- Outsourcing saves money since you don't need extra staff to deal with upswings in workload.
- Cost is substantially less than American workers.
- Time difference can permit getting work back more quickly compared to a US outsource service.
- Use transcribing team that are native English speakers so “tone” and “style” are consistent.
- Confidentiality agreements can be used if desired, e.g., for client matters.

Conclusion and Additional Information

Lots to know!

Additional Information

- Martin M. Shenkman
  shenkman@shenkmanlaw.com
- Mary E. Vandenack
  mvandenack@vwtlawyers.com
- Thomas A. Tietz
  tietz@shenkmanlaw.com