HUME SMITH GEDDES GREEN & SIMMONS, LLP AND DIALAWG, LLC

Client and Information Security

The Business of Managing a Law Firm

Seth R. Wilson and Jeff Goens

5/25/2012

Brief overview of ethical rules relating to information and client security checklists

Information and Client Security

Seth R. Wilson, Hume Smith Geddes Green & Simmons, LLP

Seth Wilson is a Senior Associate in Indianapolis, Indiana. He serves as Chair of the Indiana State Bar Association's Law Practice Management Committee. Seth serves as the Executive Director of ILTSO.org, a non-profit dedicated to drafting technical standards for the legal profession. Seth's practice includes civil litigation, data security/liability issues for law firms and businesses, and law practice management consulting. He also handles the firm's technology issues.

Jeff Goens, Dialawg, LLC

TABLE OF CONTENTS

Introduction

Data breaches are the topic of much discussion these days. The FBI has even warned law firms about hacking attempts. In a world where information is shared almost instantly to a potentially broad audience, it is more important than ever to consider information and client security as it relates to your practice. Our presentation and these written materials will help address the practical considerations regarding securing your client and practice information.

Our presentation will cover the bulk of the "substantive" information, due to the rapidly changing technology landscape. The underlying principles are addressed in the written materials. The presentation will address cloud computing matters, device security, client security, client confidentiality, paper files, information retention and destruction, and paperless office considerations. Obviously, a 45 minute presentation cannot cover in depth all of these issues, but we hope that the written and reference materials will serve as a checklist to help secure your practice.

The Ethics Of Client And Information Security

The Indiana Rules of Professional Conduct set out the foundation for a lawyer's duties regarding client and information security.

The Preamble provides the overarching duty of communication and confidentiality "A lawyer should maintain communication with a client concerning the representation. A lawyer should keep in confidence information relating to representation of a client except so far as disclosure is required or permitted by the Rules of Professional Conduct or other law." Preamble, [4]. As professionals, we have to be competent, prompt and diligent. *Id.* We often use technology to help us meet that duty.

Where the rules are not clear, we are entitled to rely on personal conscience, as well as the "approbation of professional peers." Preamble, [7]. This is helpful and harmful when it comes to information security, since lawyers are part of a self-governing profession. If our profession fails to take information security into consideration or does not use common sense when it comes to information security, additional state and federal regulation is nearly guaranteed. The information in these materials is designed to help you meet our Indiana ethical standards.

Rule 1.0 deals with this issue, requiring lawyers to be competent in the handling of a matter, the methods and procedures meeting the standards of competent practitioners, and to keep abreast of the law and its practice.

Rule 1.6 requires us to keep our client information confidential. This includes any "information related to the representation." See especially comments 16, 17, and 18. This is arguably the most important rule when it comes to information and client security.

Rule 1.15 deals with the safekeeping of client property. There are several cases where the issue of returning files to clients put the attorney in front of the disciplinary commission. This can be extended to paper and electronic files. See 1.15(a) [1] and 1.16(d). See also *In re Golding*, 700 N.E.2d 464 (Ind. 1998) (attorney failure to return client's materials after being requested to do so violates the rule); *In re McCausland*, 605 N.E.2d 185 (Ind. 1993) (refusing to return file as requested, among other violations).

Rule 1.16 outlines the lawyer's duties regarding declining or terminating representation, including a duty to return the client's "paper and property to which the client is entitled," and take reasonable steps to protect the clients' interest and mitigate the consequences of the withdrawal or termination to the client.

Rule 1.17 deals with issues relating to the sale of a law practice, including a duty to maintain confidentiality of information relating to the representation.

Rule 1.18 deals with issues relating to prospective clients, noting that even when no client-lawyer relationship ensues, the lawyer shall not reveal or use information learned in the consultation about the client. Comment 9 makes it clear that Rule 1.15 applies to "valuables or papers" given to the lawyer by the prospective client. Thus, be aware of the type of information given or received (think attachments by e-mail) by or from a prospective client to your firm.

Rule 4.4 deals with the lawyers' duties regarding inadvertently received documents. Be aware that these documents are retained on your email servers if the information was received by e-mail. You may inadvertently retain a copy of that document in your deleted items folder or sent items folder.

Also remember the lawyer's duty to supervise non-lawyer assistants under Rule 5.1. Be aware of the growing trend to attempt place "cloud" service providers under the auspices of Rule 5.3. See also Rule 9.1 *et seq*.

In addition, the American Bar Association (ABA) has proposed additional clarifications with respect to a lawyer's responsibility to maintain the confidence of client information as a relates to the fast changing world of technology. See the ABA Commission on Ethics 20/20 Report referenced under "Resources."

Clearly, lawyers have a duty to safeguard client information under our ethical rules in Indiana. The question is: how do you do that most effectively?

The 4 K's Of Information And Client Security

The below can be used as a checklist to help you create an inventory of the information storing devices in your office. The same rules apply to both electronically stored and hard copy stored information.

K1: Know What You Have

- Software
  - Antivirus
  - Operating systems
  - Microsoft office or equivalent
  - document management
  - practice management
  - contact management
  - specialty software
  - Most recent security patches applied?
- Desktop Computers
- Servers
  - Email
  - File server
- Laptops
- iPad/tablet

- Mobile Phones
- PDAs
- Disk Drives (USB, SD, Camera Cards, external hard drives)
- Cameras
- Printers (harddrive or not?)
- Copiers (harddrive or not?)
- Scanners (harddrive or not?)
- Edge Devices
    - Firewalls
    - Modems
    - Routers
    - Inbound Internet Connections
    - Unified Threat Manager
- Data Room
    - What is it?
    - Who has access?
- File room/file cabinets/file locations
- Off-site storage facility
- Backup files (electronic and paper)
- Policies and procedures
    - Document retention policy (electronic and paper)
    - Disaster planning policy
    - IT policies and procedures document (see iltso.org standards for more information)
    - Password policy

- Physical access security policy
  - keys to the office
  - keys to the storage facilities
  - office security issues
  - policies relating to cleaning vendor and other outside vendors

K2: Know What Your Devices Do

- Access the internet?
- Access the file server?
- Access email?
- Access contacts?
- Access calendars?
- Access to do records?
- Access billing records/timekeeping software?
- Hold client files?
- Remote access to the office?
- Keep back up copies of files?

K3: Know Where Your Devices Are

- Who uses them?
- Who has access? (Clients and staff)
- Who can grant/remove access?
- What happens when they go outside the 4 walls of the office?
- What happens when someone who has access leaves the firm?

K4: Know What You Store

- Define your client data (any information relating to the representation, paper or electronic)
- Define all data you keep
  - Operating Files
  - Financial records
  - Client files
  - Client information(Calendar, contact, digital, paper)
  - Firm/practice information
- What kinds of backups
  - Onsite
  - Automatic (RAID is not a backup)
  - Cloud
  - Offsite
- What do you store, but don't know about?
  - Personal files of staff
  - Cached records from Internet site visits

Enhanced Security Considerations

The following are additional measures for the security conscious.

- Penetration Testing
- Physical and Secondary Authentication Security Measures
- Connection Redundancy (e.g. two Internet connections)
- Wired v. Wireless Connections (wired is generally more secure; watch out for unsecured wireless connections)

Cloud Computing Matters

The topic of cloud computing is a hot topic within the legal community. Several state bar associations have adopted ethics opinions addressing the issue.[1] Generally, it is okay for a lawyer to utilize a cloud provider, provided that lawyer exercises reasonable care to ensure the safety and security of data hosted and transmitted to or by the cloud provider (although caveats and refinements to this position have been recently adopted in a number of states).

There are many opinions defining what is reasonable. A lawyer must read and review terms and conditions of the cloud service he or she wants to use (often referred to as Software as a Service "SAAS" provider). In addition, there must be an agreement between the lawyer and the SAAS provider outlining the duties of each party.

The ILTSO Standards contain a list of things to consider before utilizing a cloud service provider. A Google search will reveal a number of blog articles and opinions on the subject as well. The most important considerations are the encryption of data, who can decrypt the data, where the data is stored, and how you can get access to it (e.g., uptime guarantees, internet connection issues).

An important component to utilizing a cloud service provider is informed consent of your client. If the client understands how you are storing and accessing their data and indicates that he or she is comfortable with that, that written consent can help show that you acted reasonably with respect to the client's data, if there is ever a question.

Device Security

Encryption is critical regardless of the device you are using to store/transmit client data. The information on the device should be encrypted to prevent further damage in the event of theft or loss of the device. This should be a minimum requirement for all devices that access firm and client data. Be aware of the growing trend (and obvious associated risks) of Bring Your Own Device (BYOD), where client and personal information often sit side-by-side on a device.

Device security issues may also be governed by state law. For example, like many states, Indiana has a data breach notification law. See Ind. Code § 24-4.9, et seq. Indiana's law does not apply to any state agency or judicial or legislative department of state government. Ind. Code § 24-4.9-1-1.

[1] For example, Clio, a cloud based law practice management software provider, maintains a list of states with cloud computing ethics opinions: http://www.goclio.com/blog/2011/12/state-bar-cloudcomputing-ethics-opinion-roundup/ (visited May 25, 2012).

Indiana's statute defines a "breach of the security of data" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person," and includes that computerized information that has been "transferred" to another medium (e.g., paper, microfilm, even that no longer in computerized format). Ind. Code § 24-4.9-2-2(a).

There are two exceptions. First, an employee or agent of an individual may make a "good faith acquisition of personal information," if the personal information "is not used or subject to further unauthorized disclosure. *Id.* at (b)(1).

Second, if there is "unauthorized acquisition" of a portable electronic device containing stored personal information, there is no breach if the personal information stored on the device was "protected by encryption," and the encryption key is not compromised or disclosed and the encryption key is not "in the possession of or known to the person who" has access to the portable electronic device. *Id.* at (b)(2)(A) and (B).

Encryption is defined as data transformed through an "algorithmic process into a form in which there is low probability of assigning meaning without the use of a confidential process or key," or where "secured by another method that renders the data unreadable or unusable." Ind. Code § 24-4.9-2-5.

Personal information includes:

> Unencrypted/unredacted SSN number; or
> An individuals first and last names, or first initial and last name and one or more of the following unencrypted/unredacted:
>
> > Driver's license number
> > State identification card number
> > Credit card number
> > Financial account number/debit card number "in combination with a security code, password, or access code that would permit access to the person's account."

Personal information does not include lawfully obtained information from "publicly available information or from federal, state, or local government records lawfully made available to the general public." Ind. Code § 24-4.9-2-10.

Unredacted data for the purpose of this statue is data which has no more than the last four (4) digits of the driver's license number, state identification card number, or account number accessible. With the social security number, five (5) digits can be accessible. Ind. Code § 24-4.9-2-11.

If there is a breach, the "database owner" must notify the Indiana resident about the breach if the information "was or may have been" acquired or exposed. Ind. Code § 24-4.9-3-1(a). If the disclosure affects more than 1,000 consumers, the data base owner must disclose to consumer reporting agencies. *Id.* at (b). Finally, the breach must be disclosed to the attorney general. *Id.* at (c).

The notification requirements flow down the chain to those who maintain the computerized data, but do not own the data base. Ind. Code § 24-4.9-3-2.

Only the attorney general may enforce this statute, and the data base owner can be subject to a penalty of $5,000 per "deceptive act." Ind. Code § 24-4.9-3-3.5. If the database owner fails to comply, the penalty can reach $150,000 per deceptive act, plus the attorney general's costs. Ind. Code § 24-4.9-4-2.

Most mobile devices such as smart phones and tablets (iPads, etc.) have built in encryption and remote-deleting capabilities. Traditional laptops generally require additional software to encrypt the hard drive, but there are open source software options that will encrypt the laptop drive, or at least that portion which stores confidential information. At a minimum, your laptop should have a strong password before allowing a login.

Information Retention And Destruction

Every firm should have an information retention and destruction policy. This information should be reviewed and updated regularly. The policy should be tailored to the firm's practice area and based on the type of information retained by the firm. The policy should consider both paper and electronic storage of information.

In addition, having a backup policy for electronic information is critical. The firm should have a backup policy for its servers and computers. The ILTSO standards contain helpful information relating to these types of policies.

Paperless Office Considerations

It seems like everything has a "e-" component today (e-discovery; e-mail; e-filing, etc.), but it's important to remember thatsuch data is still client information, regardless of it if is "e-" paper or physical paper. Thus, the same considerations mentioned above will generally apply.

There are certain things that must be maintained as originals and the practitioner must be careful to retain copies of original documents as appropriate.

The main benefit of a paper-less office is easier access, but there are certain things that must be maintained as originals (and the practitioner must be careful to retain copies of original documents as appropriate).

As with all things security-related, the general rule is that the easier the access, the less secure it the data may prove to be. Lawyers and their staff must be careful about the ways they access the electronic information. As with all things "cloud," the lawyer must understand the risks and proceed appropriately. Obtaining client consent can go a long way toward showing the reasonableness of a lawyer's action.

Conclusion

Information and client security is a key component to successful practice. Clients will be more willing to trust those firms who take security seriously, both from a physical and electronic standpoint. Further, given the lawyer's duty to stay abreast of technology changes to ensure its appropriate use in the practice of law, each attorney should continue to research and understand these issues, or at a minimum ensure that they have someone dedicated to the protection of client information as part of their overall law firm strategy.

Resources

- The Indiana Rules of Professional Conduct (available at http://www.in.gov/judiciary/rules/prof_conduct/index.html#_Toc313019170
- ABA Practice Management Resources (available at http://www2.americanbar.org/sitetation/Lists/Posts/Post.aspx?List=4370fbab-8631-414e-8bd9-67726fd9c700&ID=781&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A%20ABASitetation%20%28ABA%20Site-tation%29)
- International Legal Technical Standards Organization (iltso.org). ILTSO is a nonprofit organization of attorneys, IT professionals, and business leaders who

are dedicated to providing current information and a suggested set of standards designed to help the profession on a path toward greater technological clarity.

- Indiana State Bar Association's Law Practice Management Committee: (http://www.inbar.org/ISBALinks/Committees/LawPracticeManagement/tabid/144/Default.aspx)

- Recent ABA ethics opinion on using email: (http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_11_459.authcheckdam.pdf)

- ABA Commission on Ethics 20/20 Report: (http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf at page 7-8) recommending modification of the model rules of professional conduct relating to a lawyers use of technology and protection of client information. This includes updating the comments to the rules to make it clear that a lawyer has a duty to stay abreast of technological changes and advances.