



## **2015 WSSFC Technology Track – Session 8**

# **Cybersecurity and SCR 20 Rules of Professional Conduct**

*Moderator:*

*Terrance L. Dunst, Bakke Norman S.C., Menomonie and New Richmond*

*Panelists:*

*William G. (Sandy) Hauserman, Digital Risk Resources, Danville, VT*

*Aviva M. Kaiser, State Bar of Wisconsin, Madison*

## About the Presenters...

**Terrence L. Dunst** is a partner with the law firm of Bakke Norman. He is a member of the firm's IT Steering Committee, and has presented seminars on various technology topics including using the internet for legal research, metadata, e-discovery, and technology and ethics. He has also given a seminar for defense lawyers on using Facebook, and is the author of the technology chapter of the Law Practice Toolkit published by Wisconsin Lawyer Mutual Insurance Company. Prior to becoming a lawyer, Terry worked for fifteen years in the software industry with Icom/Rockwell International. He has also served as the Chair of the Technology Track for the Wisconsin Solo and Small Firm Conference from 2008-2010, and 2012-2015; and in 2011 Terry was the overall Chair of the Wisconsin Solo and Small Firm.

**Sandy Hauserman** is a Founder and Managing Member of Digital Risk Resources ("DRe"). Before starting DRe, Sandy worked for Guy Carpenter & Company, a reinsurance intermediary, where he directed, the Environmental Liability Specialty Practice, was a member of the Professional Liability Specialty Group and co-led the Cyber Risk Initiative. He placed reinsurance for a number of major cyber risk insurers and developed a unique reinsurance catastrophe product that protects insurers from an accumulation of cyber-risk exposures, called a Cyber Hurricane. He is an ARIAS, U.S. certified insurance/reinsurance arbitrator and holds a J.D. from Pace University School of Law, Cum Laude and a Masters of Studies in Environmental Law from Vermont Law School, Summa Cum Laude.

**Aviva M. Kaiser** is Assistant Ethics Counsel at the State Bar of Wisconsin. She has taught at the University of Wisconsin Law School for 25 years. She teaches Professional Responsibilities and has also taught Ethical and Professional Considerations in Writing, Problem Solving, and Risk Management. From 1992 until 2002, she was the Director of the Legal Research and Writing Program. Aviva received her B.A. in Chinese from the University of Pittsburgh and her J.D. from the State University of New York at Buffalo Law School. She clerked for the Honorable Louis B. Garippo in *People v. John Wayne Gacy* and clerked for the Honorable Maurice Perlin in the Illinois Appellate Court. She practiced law in Chicago before beginning her full-time teaching career at IIT Chicago/Kent College of Law.

**Cyber Security  
and  
SCR 20: The Wisconsin Rules of Professional Conduct for Attorneys**

Along with computers comes the internet and cloud computing. The bad guys have come along too. There are new risks. There are new costs to doing business.

What do the Rules of Professional Conduct require of us?

**Wisconsin Solo and Small Firm Conference - 2015  
2:50 p.m., Friday October 23<sup>rd</sup>, 2015**

Sandy Hauserman, Attorney, Managing Member  
Digital Risk Resources (“DRe”)  
[www.digitalriskre.com](http://www.digitalriskre.com)

Aviva Kaiser, Attorney, Assistant Ethics Counsel  
Wisconsin Bar Association  
[www.wisbar.org](http://www.wisbar.org)

Terrence L. Dunst, Attorney, Partner  
Bakke Norman, S.C.  
[www.bakkenorman.com](http://www.bakkenorman.com)

**Contents:**

- Outline
- Power Point
- Appendix A: Ethics opinion on e-discovery by California State Bar.
- Appendix B: Overview of Wisconsin's Breach Notification Law.
- Appendix C: Wisconsin Lawyer article on safeguarding clients' personal information.
- Appendix D: Massachusetts Small Business Guide to drafting an information security policy.
- Appendix E: Ethics opinion on cloud computing by Wisconsin Bar.
- Appendix F: Checklist regarding computer security by Wisconsin Bar.

## I. Introduction. The Duty to Protect Client Data

Do you lock the doors to your law office when you are not there? Are you as careful with your electronically stored information (“ESI”)?

Develop a security attitude. Cyber Security is not an event, it is an ongoing process. Continue to read and learn all you can about what’s happening in technology. Watch developments outside the legal world.

## II. SCR 20 and Other Laws

### A. Competence

#### 1. SCR 20:1.1 Competence

2. The general duty of competence requires a lawyer to "...provide competent representation..." This requires not only legal knowledge; implicit is a duty to reasonably use the tools you use to provide competent representation. If you are going to use a computer, you must do so in a competent manner. If you are going to use the internet, you must do so in a competent manner. And it almost certainly requires attorneys to provide adequate confidentiality and security of a client's information.

3. California recently released Formal Ethics Opinion 11-0004 which concludes the duty of competence requires litigators to have a reasonable level of competence with respect to the technology of e-discovery, or to associate or consult with someone who does. (See Appendix A for a copy of the opinion).

a) California opines that attorneys who lack the necessary technical competence to protect client data in general terms and also in e-discovery should consult technical consultants or competent counsel or not engage in work requiring that technical competency.

4. **ABA: Comment on Rule 1.1** Maintaining Competence [8]. To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject (emphasis added).

### B. Confidentiality

1. **SCR 1.6** requires a lawyer to keep all client information confidential

2. **HIPAA** and other laws require businesses to protect personally identifiable information (“PII”).

3. **Wisconsin Statute 134.98** – Wisconsin’s Breach Notification Law. See Appendix B for an overview from the Wisconsin Department of Agriculture, Trade and Consumer Protection.

C. **SCR 20:1.15** Safekeeping property, (b)(6), combined with Wisconsin Formal Ethics Opinion. E-00-03 - Lawyers have a duty to safeguard their clients’ data, both in terms of keeping it confidential and in terms of protecting it from damage or loss. This

includes ESI. Also see November 2012 Wisconsin Lawyer article by Attorney Dean Dietrich titled Guard Clients' Personal Information. See Appendix C.

D. **SCR 20:1.4 Communication** – attorneys have a duty to keep clients reasonably informed on their case status and respond to reasonable requests for information. Especially (a)(5) which requires attorneys to keep clients informed of relevant information about their matter.

### **III. Put a Security System in Place.**

- A. It's technology (hardware, software, "old fashioned locks" and keys).
- B. It's policy.
- C. It's an attitude.
- D. What are reasonable safeguards?
- E. See Model Rule 1.6(c) and Comment 18:  
[http://www.americanbar.org/groups/professional\\_responsibility/publications/model\\_rules\\_of\\_professional\\_conduct.html](http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html).
  - 1. The sensitivity of the information.
  - 2. The likelihood of disclosure if additional safeguards are not employed.
  - 3. The cost of employing additional safeguards.
  - 4. The difficulty of implementing the safeguards.
  - 5. The extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

### **IV. Cyber Risk – a new cost of doing business.**

- A. What is cyber risk?
  - 1. The risk of inadvertently releasing confidential data, especially PII.
  - 2. The risk of confidential data/PII being stolen/hacked.
  - 3. Cyber liability – the cost of responding to a data breach can be huge.
- B. Managing cyber risk
  - 1. Technology.
    - a) Firewalls.
    - b) Anti-virus and spam filters
    - c) Backups – off site and protected.
  - 2. Insurance – Cyber Insurance – Data Breach.
    - a) Breach Notice expenses
    - b) Public Relations
    - c) Credit Monitoring

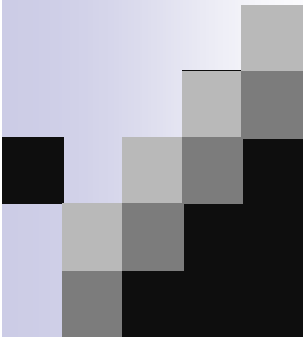
- d) Defense
- e) Liability
- 3. Policy
  - a) A written Information Security Program. See sample from Massachusetts: A Small Business Guide: Formulating a Comprehensive Written Information Security Program. See Appendix D.
  - b) Risk assessment
    - (1) Self-Assessment
    - (2) Consultants.
  - c) Strong passwords.
  - d) Vulnerability and penetration testing.
  - e) Employee termination - A disgruntled, terminated employee can be one of the biggest security threats to both a cloud service provider and law firm.
- 4. Training
  - a) Employees need to be trained to be security aware.
  - b) Employees need to be trained on technology.

## **V. Data Security in the Cloud**

- A. *Preliminary Security* – due diligence of provider’s security practices
  - 1. Read Wisconsin Formal Ethics Opinion EF-15-01, Ethical Obligations of Attorneys Using Cloud Computing. See Appendix E.
  - 2. See A Checklist: Using Reasonable Efforts (from Wisconsin State Bar). See Appendix F.
  - 3. Provider access
    - a) Physical access to server by provider employees as well as non-employees;
    - b) Who has remote access to your data? Is all administrator access to systems two factor authenticated?
    - c) Is data encrypted in transit as well as at the storage level?
  - 4. Storage location
    - a) In US or some other country? Does provider even know?
    - b) Redundancy? Geo-redundant?
  - 5. Backups and recovery
    - a) What is the backup method? Tape? Real time? Near-real time?
    - b) Do you have access to the backup records (verification)?

- c) What is recovery time?
  - d) Are all data backups stored within the US?
- 6. Certifications
  - a) Does provider have or are they working on any certifications?
- 7. Return of data and format of data
  - a) What happens to your data if the company fails?
  - b) Are you able to get data back? In what format? How long will it take?
- 8. Ownership of data
  - a) Does uploading data to the provider's server create any ownership interest in that data for the provider?
  - b) Be careful with providers that provide services to general consumers, and those service levels that are free to use. There may be language in the provider's terms of service claiming an ownership interest or license to use information uploaded to the provider's server.
  - c) The law firm should have the ability to back-up the information stored by the cloud provider on their own back-up system.





# Cyber Security and SCR 20

Wisconsin Solo and Small Firm Conference  
October 23, 2015

1



## Presented By

■ Sandy Hauserman

((•)) Digital Risk Resources  
Insuring the Digital World

■ Aviva Kaiser



■ Terrence Dunst

BAKKE ♦ NORMAN

2



At the Confluence of  
“Confidentiality” and “Competence”  
lurks a Cyber Criminal waiting to  
Destroy your Law Firm

3



Do you know what month this is?



#CyberAware

National Cyber Security  
Awareness Month

Get involved and do your part to make the Internet  
safer and more secure for everyone.

This year's NCSAM theme is Our Shared Responsibility.

StaySafeOnline.org  
Powered by National Cyber Security Alliance

4



## Security vs. Usability



5



## Many Rules Come Into Play

- SCR 1.1 – Competence
- SCR 1.6 – Communication
- SCR 1.6 – Confidentiality
- SCR 1.15 – Safeguarding Property

6



# PART I

## Safeguarding Client's Information is the Foundation Upon which Your Entire Law Practice Rests

7



### The Big Deal

Every Law Firm is now dependent on Technology and the Internet.

- This dependency creates Business & Legal risk
  - ✓ Usually not covered in E&O Policies.
  - ✓ Why so? Duty of Care/Competence and Confidentiality

#### 1. Collecting Personally Identifiable Information (PII)

- PII collection, client records & credit/debit card processing make up a significant portion of the overall risk profile. Law Firms gather and transmit PII of clients, employees, vendors and others.
- PII is the currency of the 21<sup>st</sup> century. It has value to criminals who sell it or use it to commit Identity theft. Just as a business wouldn't leave cash sitting around, PII has to be safeguarded. Law Firms collect a lot of very sensitive information which could severely damage a client's reputation.

#### 2. Using the Internet

- Cyber criminals want to steal data or damage IT systems. They often plant harmful software on a computer and hope it is accidentally transmitted to others – Worms, Viruses, Trojans, Botnets, Malware, etc.

8



## The Big Deal

### ➤ Legal Regime

State Breach Notice Laws establish a framework for protecting PII and reporting security breaches to the public.

- Some Law Firms collect Client's sensitive medical information and are therefore subject to HIPAA: See summary of regulations at:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>

- Notification of individuals who are victims of a security breach is expensive and disruptive to operations.
  - The average cost is between \$50 to \$214 for each affected person
  - These costs include: legal costs, notification costs to victims, investigative expenses to determine loss, & credit monitoring for managing identity theft risk.
- Increased business risk for 3<sup>rd</sup> Party Liability from hackers, viruses, Trojans, and other malware are on the rise.
- Identity Theft is the fastest growing crime in America.

9



## Privacy and Breach Notification Laws

- **47 States** in the U.S. have enacted laws that require a business suffering a security breach to notify victims so they can take action to protect themselves from Identity Theft.

The laws can vary greatly in their definitions of Personally Identifiable Information (PII) and notification requirements

- ☐ Some have "Safe Harbors" for encryption such as "NOTICE is required for breach of unencrypted data, but *not required* for encrypted data"
  - ☐ These laws and the information provided by regulatory authorities concerning best practices are establishing **STANDARDS OF CARE**
  - ☐ Not taking proper precaution to safeguard clients PII can lead to fines and penalties
- Wisconsin has an Office of Privacy Protection -  
[http://datcp.wi.gov/Consumer/Office\\_of\\_Privacy\\_Protection](http://datcp.wi.gov/Consumer/Office_of_Privacy_Protection)

10



## Wisconsin Privacy Laws for Businesses

### Primary Statute for “Breach Notification”

- ☐ Wis. Stat. § 134.98. (see attached fact sheet)
  - Wisconsin Data Breach Notification Law  
Effective March, 2006
    - ☐ Requires notice to a consumer when information is taken in a security breach that is not encrypted or redacted.
    - ☐ This includes SS#, Driver’s License or State ID #, Financial Account information, DNA and Biometric data.
  - However, if the information is rendered unreadable, it is not considered “personal information” subject to notification.

11



## Wisconsin Privacy Laws for Businesses

### Other Major Privacy Laws for Wisconsin include

- Disposal of records containing personal information; Wis. Stat. § 134.97.
- Telephone records; obtaining, selling, or receiving without consent; Wis. Stat. § 100.525.
- Nondisclosure of information on receipts; Wis. Stat. § 134.74.
- Notaries; confidentiality; Wis. Stat. § 137.01 (5m)
- Disclosure of information from vital records; Wis. Stat. § 69.20.
- Confidentiality of patient health care records; Wis. Stat. §§ 146.81 through 146.84.
- Health care services review; confidentiality of information; Wis. Stat. § 146.38.
- Unauthorized use of a business’s identifying information; Wis. Stat. § 943.203.

12



## Scary Stuff

- If a law firm unlawfully releases 100 personal records, the average amount the business would have to pay to notify the individuals would be over Five Thousand Dollars.
- If a Law Firm unlawfully released 1,000 personal records, the average amount to notify the individuals would be over Fifty Thousand Dollars.
- A modest sized breach can result in a huge legal liability that could potentially bankrupt a small law firm.
- Considering insurance coverage for “Breach Notification Expenses” is a good risk management investment to protect the law firm from having to pay for these types of unwanted expenses.

13



## Scary Stuff (Cont.)

- If an individual who has been notified actually suffers a monetary loss – (i.e. a criminal takes out a mortgage in his/her name) or more importantly if medical information collected by the law firm gets in the wrong hands

Or...

- If a Virus, Botnet, Trojan, Worm, etc. is transmitted from a law firm’s computer system to someone else’s computer system and as a result, that person/business suffers a monetary loss -

The law firm can get: Sued

- Considering Liability Insurance for law suits, whether they have merit or not, is the easiest and most efficient way to arrange for stand-by legal and other assistance and to help pay for damages inflicted on others.

14



## Scary Stuff (Cont.)

Hackers & Criminals are now targeting small to mid-sized law firms as these are often the least secure from attack – as a result **law suits are on the rise.**

“Criminals (are) changing tactics from attacking really large targets to attacking a lot of really small targets where the amount of card numbers or PII records compromised is measured in thousands instead of millions.”

\* Verizon Data Breach Investigations Report of April 2011

15



## Loss Scenarios

- ❑ An Attorney/Employee checks their personal email and unwittingly downloads malware/ransomware onto the company network.
- ❑ A company laptop containing PII is stolen from an Attorney's car.
- ❑ Customers Credit Card/Bank/Health Information is stolen by someone hacking into the law firm's system.
- ❑ Paper records containing PII are not shredded before disposing and are retrieved by criminals (Dumpster Diving).
- ❑ An Attorney researching online is directed to a website that automatically downloads a worm which turns the computer into a spamming machine.

16





## PART II

- Don't be a victim of Cyber Crime!
- Learn how to Protect PII



17



### Top Precautions for Protecting PII

1. Train Employees. Criminals are experts in exploiting people who do not know how to adequately protect PII.
2. Have a plan to secure PII - Adopt and implement a Written Information Security Plan (WISP). A WISP outlines the security controls and business practices for handling PII.
3. Encrypt the Corporate network and any mobile devices making PII only accessible by the User.
4. Store paper records in a locked file cabinet or room - backup electronic data and store offsite.
5. Maintain Firewalls on any computer device connected to the internet.
6. Use Anti-Virus software and update it no less than every 30 days.
7. Use strong passwords.
8. Dispose of unnecessary or outdated paper & Electronic PII. Erase Data from printers, cell phones, copiers, computers. Shred paper documents.

18



## APPENDIX

### Guidance for a law firm to Protect Personal Information

19



#### Guidance for a law firm to Protect Personal Information

- Know who has Access to Personal Information. Restrict access to sensitive PII such as social security, credit card numbers & financial info.
- Implement a Written Information Security Plan (WISP).  
A WISP is a program that outlines the security controls and business practices for handling PII and is designed to:
  1. ensure the security and confidentiality of personal information;
  2. protect against any anticipated threats or hazards to the security or integrity of such information; and
  3. protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.
- Conduct background checks on employees who have access to PII.

Many acts of identity theft occur from within the company. From corporate accounting to courier delivery personnel, anyone who handles personal information should be screened for criminal backgrounds and sign a commitment to uphold the company's confidentiality standards and security protocol.

20



## Guidance for a law firm to Protect Personal Information

- Train Employees. Law firm wide privacy risk and awareness training benefits the whole company. Criminals are experts in exploiting people who do not take precautions in using the company computer system.
- Keep Training Employees. Regular training updates is important for company-wide awareness to let employees know what the latest threats are and include guidance on ways to protect the company from these risks.
- Institute Good Business Practices Corporate wide. Develop a Security Plan that identifies good business practices to protect PII including plans to manage a crisis event so you know how to respond and plan to protect the company from employees in the event they leave the company.

21



## Guidance for a law firm to Protect Personal Information

- Discover where your Company holds PII.

Conduct an audit on your computers, printers, scanners, copiers, wireless devices and any other electronic devices that can store personal or sensitive information to determine if PII is unnecessarily stored in an unintended place. If so, **delete** it or **send** it to a secure place.

- Have a plan to secure Personal Information.
  - Store **Paper** based PII in a locked store room or file cabinet.
  - Install security for the building premises such as camera systems and card key access.
  - Limit access to PII to only those personnel that are required to use it.
  - Require Employees to log off computers and lock up files.
  - Track shipments and deliveries with outside contractors.
- Encrypt Electronic Data at Rest.

It is best to adopt a company wide policy of using encryption for computers, tablets, smart phones and other devices that employees use for business. Some States require the use of encryption, and others provide “safe harbor” protection to businesses that use it.

22



## Guidance for a law firm to Protect Personal Information

- Dispose of unnecessary or outdated Personal Information.

This includes both **Paper** and **Electronic** document formats

- Paper-based Personal Information:
  - Shred it. Place shredders near copiers for easy access.
    - Heavy Duty cross cut shredders are best
    - Incinerating paper based documents destroys PII
- Electronic-based Personal Information
  - Delete Data from computer devices.
  - Degauss (electromagnets) or run a “wiping” utility software program to clean hard-to-find files that might otherwise be discoverable.
  - Destroy hard drives in hardware prior to disposing or recycling (recycled computer devices is a frequent cause of PII loss).
  - Leased Equipment such as printers, copiers, scanners, faxes and phones often contain vast amounts of Personal Information. Ensure your leasing company’s policy protects you by contracting to erase all forms of PII.

**THE STATE BAR OF CALIFORNIA  
STANDING COMMITTEE ON  
PROFESSIONAL RESPONSIBILITY AND CONDUCT  
FORMAL OPINION NO. 2015-193**

**ISSUE:** What are an attorney's ethical duties in the handling of discovery of electronically stored information?

**DIGEST:** An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law. Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI. Competency may require even a highly experienced attorney to seek assistance in some litigation matters involving ESI. An attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation. Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality.

**AUTHORITIES**

**INTERPRETED:** Rules 3-100 and 3-110 of the Rules of Professional Conduct of the State Bar of California.<sup>1/</sup>

Business and Professions Code section 6068(e).

Evidence Code sections 952, 954 and 955.

**STATEMENT OF FACTS**

Attorney defends Client in litigation brought by Client's Chief Competitor in a judicial district that mandates consideration of e-discovery<sup>2/</sup> issues in its formal case management order, which is consistent with California Rules of Court, rule 3.728. Opposing Counsel demands e-discovery; Attorney refuses. They are unable to reach an agreement by the time of the initial case management conference. At that conference, an annoyed Judge informs both attorneys they have had ample prior notice that e-discovery would be addressed at the conference and tells them to return in two hours with a joint proposal.

In the ensuing meeting between the two lawyers, Opposing Counsel suggests a joint search of Client's network, using Opposing Counsel's chosen vendor, based upon a jointly agreed search term list. She offers a clawback agreement that would permit Client to claw back any inadvertently produced ESI that is protected by the attorney-client privilege and/or the work product doctrine ("Privileged ESI").

---

<sup>1/</sup> Unless otherwise indicated, all references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

<sup>2/</sup> Electronically stored information ("ESI") is information that is stored in technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities (e.g., Code Civ. Proc., § 2016.020, sub. (d) – (e)). Electronic Discovery, also known as e-discovery, is the use of legal means to obtain ESI in the course of litigation for evidentiary purposes.

Attorney believes the clawback agreement will allow him to pull back anything he “inadvertently” produces. Attorney concludes that Opposing Counsel’s proposal is acceptable and, after advising Client about the terms and obtaining Client’s authority, agrees to Opposing Counsel’s proposal. Judge thereafter approves the attorneys’ joint agreement and incorporates it into a Case Management Order, including the provision for the clawback of Privileged ESI. The Court sets a deadline three months later for the network search to occur.

Back in his office, Attorney prepares a list of keywords he thinks would be relevant to the case, and provides them to Opposing Counsel as Client’s agreed upon search terms. Attorney reviews Opposing Counsel’s additional proposed search terms, which on their face appear to be neutral and not advantageous to one party or the other, and agrees that they may be included.

Attorney has represented Client before, and knows Client is a large company with an information technology (“IT”) department. Client’s CEO tells Attorney there is no electronic information it has not already provided to Attorney in hard copy form. Attorney assumes that the IT department understands network searches better than he does and, relying on that assumption and the information provided by CEO, concludes it is unnecessary to do anything further beyond instructing Client to provide Vendor direct access to its network on the agreed upon search date. Attorney takes no further action to review the available data or to instruct Client or its IT staff about the search or discovery. As directed by Attorney, Client gives Vendor unsupervised direct access to its network to run the search using the search terms.

Subsequently, Attorney receives an electronic copy of the data retrieved by Vendor’s search and, busy with other matters, saves it in an electronic file without review. He believes that the data will match the hard copy documents provided by Client that he already has reviewed, based on Client’s CEO’s representation that all information has already been provided to Attorney.

A few weeks later, Attorney receives a letter from Opposing Counsel accusing Client of destroying evidence and/or spoliation. Opposing Counsel threatens motions for monetary and evidentiary sanctions. After Attorney receives this letter, he unsuccessfully attempts to open his electronic copy of the data retrieved by Vendor’s search. Attorney hires an e-discovery expert (“Expert”), who accesses the data, conducts a forensic search, and tells Attorney potentially responsive ESI has been routinely deleted from Client’s computers as part of Client’s normal document retention policy, resulting in gaps in the document production. Expert also advises Attorney that, due to the breadth of Vendor’s execution of the jointly agreed search terms, both privileged information and irrelevant but highly proprietary information about Client’s upcoming revolutionary product were provided to Chief Competitor in the data retrieval. Expert advises Attorney that an IT professional with litigation experience likely would have recognized the overbreadth of the search and prevented the retrieval of the proprietary information.

What ethical issues face Attorney relating to the e-discovery issues in this hypothetical?

## **DISCUSSION**

### **I. Duty of Competence**

#### **A. Did Attorney Violate The Duty of Competence Arising From His Own Acts/Omissions?**

While e-discovery may be relatively new to the legal profession, an attorney’s core ethical duty of competence remains constant. Rule 3-110(A) provides: “A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence.” Under subdivision (B) of that rule, “competence” in legal services shall mean to apply the diligence, learning and skill, and mental, emotional, and physical ability reasonably necessary for the performance of such service. Read together, a mere failure to act competently does not trigger discipline under rule 3-110. Rather, it is the failure to do so in a manner that is intentional, reckless or repeated that would result in a disciplinable rule 3-110 violation. (See *In the Matter of Torres* (Review Dept. 2000) 4 Cal. State Bar Ct. Rptr. 138, 149 (“We have repeatedly held that negligent legal representation, even that amounting to legal malpractice, does not establish a [competence] rule 3-110(A) violation.”); see also, *In the Matter of Gadda* (Review Dept. 2002) 4 Cal. State Bar Ct. Rptr. 416 (reckless and repeated acts); *In the Matter of Riordan* (Review Dept. 2007) 5 Cal. State Bar Ct. Rptr. 41 (reckless and repeated acts).)

Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent. Maintaining learning and skill consistent with an attorney's duty of competence includes keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, . . ." ABA Model Rule 1.1, Comment [8].<sup>3/</sup> Rule 3-110(C) provides: "If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required." Another permissible choice would be to decline the representation. When e-discovery is at issue, association or consultation may be with a non-lawyer technical expert, if appropriate in the circumstances. Cal. State Bar Formal Opn. No. 2010-179.

Not every litigated case involves e-discovery. Yet, in today's technological world, almost every litigation matter *potentially* does. The chances are significant that a party or a witness has used email or other electronic communication, stores information digitally, and/or has other forms of ESI related to the dispute. The law governing e-discovery is still evolving. In 2009, the California Legislature passed California's Electronic Discovery Act adding or amending several California discovery statutes to make provisions for electronic discovery. See, e.g., Code of Civil Procedure section 2031.010, paragraph (a) (expressly providing for "copying, testing, or sampling" of "electronically stored information in the possession, custody, or control of any other party to the action.")<sup>4/</sup> However, there is little California case law interpreting the Electronic Discovery Act, and much of the development of e-discovery law continues to occur in the federal arena. Thus, to analyze a California attorney's current ethical obligations relating to e-discovery, we look to the federal jurisprudence for guidance, as well as applicable Model Rules, and apply those principles based upon California's ethical rules and existing discovery law.<sup>5/</sup>

We start with the premise that "competent" handling of e-discovery has many dimensions, depending upon the complexity of e-discovery in a particular case. The ethical duty of competence requires an attorney to assess at the outset of each case what electronic discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by either side. If e-discovery will probably be sought, the duty of competence requires an attorney to assess his or her own e-discovery skills and resources as part of the attorney's duty to provide the client with competent representation. If an attorney lacks such skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate or consult with someone with expertise to assist. Rule 3-110(C). Attorneys handling e-discovery should be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following:

- initially assess e-discovery needs and issues, if any;
- implement/cause to implement appropriate ESI preservation procedures;<sup>6/</sup>

---

<sup>3/</sup> Although not binding, opinions of ethics committees in California should be consulted by members for guidance on proper professional conduct. Ethics opinions and rules and standards promulgated by other jurisdictions and bar associations may also be considered. Rule 1-100(A).

<sup>4/</sup> In 2006, revisions were made to the Federal Rules of Civil Procedure, rules 16, 26, 33, 34, 37 and 45, to address e-discovery issues in federal litigation. California modeled its Electronic Discovery Act to conform with mostly-parallel provisions in those 2006 federal rules amendments. (See Evans, *Analysis of the Assembly Committee on Judiciary regarding AB 5* (2009). ([http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab\\_0001-0050/ab\\_5\\_cfa\\_20090302\\_114942\\_asm\\_comm.html](http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_0001-0050/ab_5_cfa_20090302_114942_asm_comm.html)).

<sup>5/</sup> Federal decisions are compelling where the California law is based upon a federal statute or the federal rules. (See *Toshiba America Electronic Components, Inc. v. Superior Court (Lexar Media, Inc.)* (2004) 124 Cal.App.4th 762, 770 [21 Cal.Rptr.3d 532]; *Vasquez v. Cal. School of Culinary Arts, Inc.* (2014) 230 Cal.App.4th 35 [178 Cal.Rptr.3d 10]; see also footnote 4, *supra*.)

<sup>6/</sup> This opinion does not directly address ethical obligations relating to litigation holds. A litigation hold is a directive issued to, by, or on behalf of a client to persons or entities associated with the client who may possess potentially relevant documents (including ESI) that directs those custodians to preserve such documents, pending further direction. See generally Redgrave, *Sedona Conference® Commentary on Legal Holds: The Trigger and The Process* (Fall 2010) *The Sedona Conference Journal*, Vol. 11 at pp. 260 – 270, 277 – 279. Prompt issuance of a litigation hold may prevent spoliation of evidence, and the duty to do so falls on both the party and outside counsel working on the matter. See

- analyze and understand a client's ESI systems and storage;
- advise the client on available options for collection and preservation of ESI;
- identify custodians of potentially relevant ESI;
- engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
- perform data searches;
- collect responsive ESI in a manner that preserves the integrity of that ESI; and
- produce responsive non-privileged ESI in a recognized and appropriate manner.<sup>7/</sup>

See, e.g., *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC* (S.D.N.Y. 2010) 685 F.Supp.2d 456, 462 – 465 (defining gross negligence in the preservation of ESI), (abrogated on other grounds in *Chin v. Port Authority* (2nd Cir. 2012) 685 F.3d 135 (failure to institute litigation hold did not constitute gross negligence per se)).

In our hypothetical, Attorney had a general obligation to make an e-discovery evaluation early, prior to the initial case management conference. The fact that it was the standard practice of the judicial district in which the case was pending to address e-discovery issues in formal case management highlighted Attorney's obligation to conduct an early initial e-discovery evaluation.

Notwithstanding this obligation, Attorney made *no* assessment of the case's e-discovery needs or of his own capabilities. Attorney exacerbated the situation by not consulting with another attorney or an e-discovery expert prior to agreeing to an e-discovery plan at the initial case management conference. He then allowed that proposal to become a court order, again with no expert consultation, although he lacked sufficient expertise. Attorney participated in preparing joint e-discovery search terms without experience or expert consultation, and he did not fully understand the danger of overbreadth in the agreed upon search terms.

Even after Attorney stipulated to a court order directing a search of Client's network, Attorney took no action other than to instruct Client to allow Vendor to have access to Client's network. Attorney did not instruct or supervise Client regarding the direct network search or discovery, nor did he try to pre-test the agreed upon search terms or otherwise review the data before the network search, relying on his assumption that Client's IT department would know what to do, and on the parties' clawback agreement.

After the search, busy with other matters and under the impression the data matched the hard copy documents he had already seen, Attorney took no action to review the gathered data until after Opposing Counsel asserted spoliation and threatened sanctions. Attorney then unsuccessfully attempted to review the search results. It was only then, at the end of this long line of events, that Attorney finally consulted an e-discovery expert and learned of the e-discovery problems facing Client. By this point, the potential prejudice facing Client was significant, and much of the damage already had been done.

At the least, Attorney risked breaching his duty of competence when he failed at the outset of the case to perform a timely e-discovery evaluation. Once Opposing Counsel insisted on the exchange of e-discovery, it became certain that e-discovery would be implicated, and the risk of a breach of the duty of competence grew considerably; this should have prompted Attorney to take additional steps to obtain competence, as contemplated under rule 3-110(C), such as consulting an e-discovery expert.

---

[Footnote Continued...]

*Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2003) 220 F.R.D. 212, 218 and *Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2004) 229 F.R.D. 422, 432. Spoliation of evidence can result in significant sanctions, including monetary and/or evidentiary sanctions, which may impact a client's case significantly.

<sup>7/</sup> This opinion focuses on an attorney's ethical obligations relating to his own client's ESI and, therefore, this list focuses on those issues. This opinion does not address the scope of an attorney's duty of competence relating to obtaining an opposing party's ESI.



Had the e-discovery expert been consulted at the beginning, or at the latest once Attorney realized e-discovery would be required, the expert could have taken various steps to protect Client's interest, including possibly helping to structure the search differently, or drafting search terms less likely to turn over privileged and/or irrelevant but highly proprietary material. An expert also could have assisted Attorney in his duty to counsel Client of the significant risks in allowing a third party unsupervised direct access to Client's system due to the high risks and how to mitigate those risks. An expert also could have supervised the data collection by Vendor.<sup>8/</sup>

Whether Attorney's acts/omissions in this single case amount to a disciplinable offense under the "intentionally, recklessly, or repeatedly" standard of rule 3-110 is beyond this opinion, yet such a finding could be implicated by these facts.<sup>9/</sup> See, e.g., *In the Matter of Respondent G.* (Review Dept. 1992) 2 Cal. State Bar Ct. Rptr. 175, 179 (respondent did not perform competently where he was reminded on repeated occasions of inheritance taxes owed and repeatedly failed to advise his clients of them); *In re Matter of Copren* (Review Dept. 2005) 4 Cal. State Bar Ct. Rptr. 861, 864 (respondent did not perform competently when he failed to take several acts in single bankruptcy matter); *In re Matter of Layton* (Review Dept. 1993) 2 Cal. State Bar Ct. Rptr. 366, 377 – 378 (respondent did not perform competently where he "recklessly" exceeded time to administer estate, failed to diligently sell/distribute real property, untimely settled supplemental accounting and did not notify beneficiaries of intentions not to sell/lease property).

## **B. Did Attorney Violate The Duty of Competence By Failing To Supervise?**

The duty of competence in rule 3-110 includes the duty to supervise the work of subordinate attorneys and non-attorney employees or agents. See Discussion to rule 3-110. This duty to supervise can extend to outside vendors or contractors, and even to the client itself. See California State Bar Formal Opn. No. 2004-165 (duty to supervise outside contract lawyers); San Diego County Bar Association Formal Opn. No. 2012-1 (duty to supervise clients relating to ESI, citing *Cardenas v. Dorel Juvenile Group, Inc.* (D. Kan. 2006) 2006 WL 1537394).

Rule 3-110(C) permits an attorney to meet the duty of competence through association with another lawyer or consultation with an expert. See California State Bar Formal Opn. No. 2010-179. Such expert may be an outside vendor, a subordinate attorney, or even the client, if they possess the necessary expertise. This consultation or association, however, does not absolve an attorney's obligation to supervise the work of the expert under rule 3-110, which is a non-delegable duty belonging to the attorney who is counsel in the litigation, and who remains the one primarily answerable to the court. An attorney must maintain overall responsibility for the work of the expert he or she chooses, even if that expert is the client or someone employed by the client. The attorney must do so by remaining regularly engaged in the expert's work, by educating everyone involved in the e-discovery workup about the legal issues in the case, the factual matters impacting discovery, including witnesses and key evidentiary issues, the obligations around discovery imposed by the law or by the court, and of any relevant risks associated with the e-discovery tasks at hand. The attorney should issue appropriate instructions and guidance and, ultimately, conduct appropriate tests until satisfied that the attorney is meeting his ethical obligations prior to releasing ESI.

Here, relying on his familiarity with Client's IT department, Attorney assumed the department understood network searches better than he did. He gave them no further instructions other than to allow Vendor access on the date of the network search. He provided them with no information regarding how discovery works in litigation, differences

---

<sup>8/</sup> See Advisory Committee Notes to the 2006 Amendments to the Federal Rules of Civil Procedure, rule 34 ("Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) . . . is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems."). See also The Sedona Principles Addressing Electronic Document Production (2nd Ed. 2007), Comment 10(b) ("Special issues may arise with any request to secure direct access to electronically stored information or to computer devices or systems on which it resides. Protective orders should be in place to guard against any release of proprietary, confidential, or personal electronically stored information accessible to the adversary or its expert.").

<sup>9/</sup> This opinion does not intend to set or define a standard of care of attorneys for liability purposes, as standards of care can be highly dependent on the factual scenario and other factors not applicable to our analysis herein.

between a party affiliated vendor and a neutral vendor, what could constitute waiver under the law, what case-specific issues were involved, or the applicable search terms. Client allowed Vendor direct access to its entire network, without the presence of any Client representative to observe or monitor Vendor's actions. Vendor retrieved proprietary trade secret and privileged information, a result Expert advised Attorney could have been prevented had a trained IT individual been involved from the outset. In addition, Attorney failed to warn Client of the potential significant legal effect of not suspending its routine document deletion protocol under its document retention program.

Here, as with Attorney's own actions/inactions, whether Attorney's reliance on Client was reasonable and sufficient to satisfy the duty to supervise in this setting is a question for a trier of fact. Again, however, a potential finding of a competence violation is implicated by the fact pattern. See, e.g., *Palomo v. State Bar* (1984) 36 Cal.3d 785, 796 [205 Cal.Rptr. 834] (evidence demonstrated lawyer's pervasive carelessness in failing to give the office manager any supervision, or instruction on trust account requirements and procedures).

## **II. Duty of Confidentiality**

A fundamental duty of an attorney is "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client." (Bus. & Prof. Code, § 6068 (e)(1).) "Secrets" includes "information, other than that protected by the attorney-client privilege, that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client." (Cal. State Bar Formal Opinion No. 1988-96.) "A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1), without the informed consent of the client, or as provided in paragraph (B) of this rule." (Rule 3-100(A).)

Similarly, an attorney has a duty to assert the attorney-client privilege to protect confidential communications between the attorney and client. (Evid. Code, §§ 952, 954, 955.) In civil discovery, the attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure *only if* the attorney and client act reasonably to protect that privilege. See *Regents of University of California v. Superior Court (Aquila Merchant Services, Inc.)* (2008) 165 Cal.App.4th 672, 683 [81 Cal.Rptr.3d 186]. This approach also echoes federal law.<sup>10/</sup> A lack of reasonable care to protect against disclosing privileged and protected information when producing ESI can be deemed a waiver of the attorney-client privilege. See *Kilopass Tech. Inc. v. Sidense Corp.* (N.D. Cal. 2012) 2012 WL 1534065 at 2 – 3 (attorney-client privilege deemed waived as to privileged documents released through e-discovery because screening procedures employed were unreasonable).

In our hypothetical, because of the actions taken by Attorney prior to consulting with any e-discovery expert, Client's privileged information has been disclosed. Due to Attorney's actions, Chief Competitor can argue that such disclosures were not "inadvertent" and that any privileges were waived. Further, non-privileged, but highly confidential proprietary information about Client's upcoming revolutionary new product has been released into the hands of Chief Competitor. Even absent any indication that Opposing Counsel did anything to engineer the overbroad disclosure, it remains true that the disclosure occurred because Attorney participated in creating overbroad search terms. All of this happened unbeknownst to Attorney, and only came to light after Chief Competitor accused Client of evidence spoliation. Absent Chief Competitor's accusation, it is not clear when any of this would have come to Attorney's attention, if ever.

The clawback agreement on which Attorney heavily relied may not work to retrieve the information from the other side. By its terms, the clawback agreement was limited to inadvertently produced Privileged ESI. Both privileged information, and non-privileged, but confidential and proprietary information, have been released to Chief Competitor.

---

<sup>10/</sup> See Federal Rules of Evidence, rule 502(b): "Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)."

Under these facts, Client may have to litigate whether Client (through Attorney) acted diligently enough to protect its attorney-client privileged communications. Attorney took no action to review Client's network prior to allowing the network search, did not instruct or supervise Client prior to or during Vendor's search, participated in drafting the overbroad search terms, and waited until after Client was accused of evidence spoliation before reviewing the data – all of which could permit Opposing Counsel viably to argue Client failed to exercise due care to protect the privilege, and the disclosure was not inadvertent.<sup>11/</sup>

Client also may have to litigate its right to the return of non-privileged but confidential proprietary information, which was not addressed in the clawback agreement.

Whether a waiver has occurred under these circumstances, and what Client's rights are to return of its non-privileged/confidential proprietary information, again are legal questions beyond this opinion. Attorney did not reasonably try to minimize the risks. Even if Client can retrieve the information, Client may never "un-ring the bell."

The State Bar Court Review Department has stated, "Section 6068, subdivision (e) is the most strongly worded duty binding on a California attorney. It requires the attorney to maintain 'inviolable' the confidence and 'at every peril to himself or herself' preserve the client's secrets." (See *Matter of Johnson* (Rev. Dept. 2000) 4 Cal. State Bar Ct. Rptr. 179.) While the law does not require perfection by attorneys in acting to protect privileged or confidential information, it requires the exercise of reasonable care. Cal. State Bar Formal Opn. No. 2010-179. Here, Attorney took only minimal steps to protect Client's ESI, or to instruct/supervise Client in the gathering and production of that ESI, and instead released everything without prior review, inappropriately relying on a clawback agreement. Client's secrets are now in Chief Competitor's hands, and further, Chief Competitor may claim that Client has waived the attorney-client privilege. Client has been exposed to that potential dispute as the direct result of Attorney's actions. Attorney may have breached his duty of confidentiality to Client.

## CONCLUSION

Electronic document creation and/or storage, and electronic communications, have become commonplace in modern life, and discovery of ESI is now a frequent part of almost any litigated matter. Attorneys who handle litigation may not ignore the requirements and obligations of electronic discovery. Depending on the factual circumstances, a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced. It also may result in violations of the duty of confidentiality, notwithstanding a lack of bad faith conduct.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Trustees, any persons or tribunals charged with regulatory responsibilities, or any member of the State Bar.

*[Publisher's Note: Internet resources cited in this opinion were last accessed by staff on June 30, 2015. Copies of these resources are on file with the State Bar's Office of Professional Competence.]*

---

<sup>11/</sup> Although statute, rules, and/or case law provide some limited authority for the legal claw back of certain inadvertently produced materials, even in the absence of an express agreement, those provisions may not work to mitigate the damage caused by the production in this hypothetical. These "default" claw back provisions typically only apply to privilege and work product information, and require both that the disclosure at issue has been truly inadvertent, and that the holder of the privilege has taken reasonable steps to prevent disclosure in the first instance. See Federal Rules of Evidence, rule 502; see also generally *State Compensation Insurance Fund v. WPS, Inc.* (1999) 70 Cal.App.4th 644 [82 Cal.Rptr.2d 799]; *Rico v. Mitsubishi Motors Corp.* (2007) 42 Cal.4th 807, 817 – 818 [68 Cal.Rptr.3d 758]. As noted above, whether the disclosures at issue in our hypothetical truly were "inadvertent" under either the parties' agreement or the relevant law is an open question. Indeed, Attorney will find even less assistance from California's discovery clawback statute than he will from the federal equivalent, as the California statute merely addresses the procedure for litigating a dispute on a claim of inadvertent production, and not the legal issue of waiver at all. (See Code Civ. Proc., § 2031.285.)

# Office of Privacy Protection

*Safeguarding Information for Your Future*



## Wisconsin's Data Breach Notification Law

Section 134.98 of the Wisconsin Statutes requires most businesses to notify individuals if an unauthorized person has acquired their personal information. The business must be operating in Wisconsin and maintaining personal information about individuals who reside in Wisconsin. This law also applies to Wisconsin state government agencies, cities, towns, villages, and counties.

### What personal information is covered

The law defines personal information to mean an individual's last name and first name or first initial in combination with and linked to any of the following elements, if the element is not publicly available information, and is not encrypted, redacted or altered in a manner that renders the element unreadable:

- 🔒 Social security number.
- 🔒 Driver's license number or state identification number.
- 🔒 Financial account number including a credit or debit card account number or any security code, access code or password that would permit access to the individual's financial account.
- 🔒 DNA profile.
- 🔒 Any unique biometric data including fingerprint, voiceprint, retina or iris image, or any other unique physical representation.

### Who is required to give notice

Among those required to give notice are:

- 🔒 Businesses that conduct business in the state and maintain personal information in the ordinary course of business.
- 🔒 Businesses that license personal information in the state.
- 🔒 Businesses that maintain a depository account for Wisconsin residents.
- 🔒 Businesses that lend money to Wisconsin residents.
- 🔒 The state and any office, department, independent agency, authority, institution, association, society or other body in state government created or authorized by Wisconsin law including the courts and the legislature.
- 🔒 A city, village, town or county.

Certain financial institutions that are subject to and in compliance with the privacy and security requirements of

federal law, as well as businesses that have contractual arrangements with such institutions and have a policy in effect regarding security breaches, are exempt from Wisconsin's law. Similarly, certain health plans and health care providers are not covered by Wisconsin's law.

## **When is notice required**

Generally, the law requires the business or governmental entity to notify an individual whenever personal information held by the business or governmental entity is acquired by an unauthorized person. However, no notice is required if the unauthorized acquisition does not create a material risk of identity theft or fraud, or if the information was acquired in good faith by an employee or agent and is used for a lawful purpose of the entity.

## **What notice is required**

In general, any entity that is required to give notice of the unauthorized acquisition of personal information must provide notice of that fact to persons whose information was acquired. The notice must be given within a reasonable time, not to exceed 45 days after the entity learns of the unauthorized acquisition. The notice must be given by mail or by a method that the entity has previously used to communicate with the subject of the information. For example, if a business has communicated with a customer by email, notice may be given by email. Upon written request of the person whose information was acquired, the entity must also identify the nature of the personal information acquired.

If an entity cannot determine the mailing address of the person whose information was acquired, and if the entity has not previously communicated with that person, the entity must give notice in a manner that is reasonably calculated to provide notice. Such methods might include notice in the newspaper or on television or radio.

In cases where the personal information of more than 1,000 individuals was acquired at one time, the entity from which the information was required must also give notice to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. This would include the major credit reporting agencies.

A law enforcement agency may request that an entity not provide notice in order to protect an investigation or homeland security. In such cases, the entity may not provide notice until permitted by the law enforcement agency.

## **Two-factor authentication**

Safeguard your information. Use two-factored authentication if offered. Two factor authentication is a security process in which you, the user, provide two means of identification – something you have and something you know. Something you have is typically a physical token, such as a card or a code sent to your smartphone. Something you know is something memorized, such as a personal identification number (PIN) or password.

For more information visit our website or contact the Office of Privacy Protection.

**Bureau of Consumer Protection  
Office of Privacy Protection  
2811 Agriculture Drive  
PO Box 8911  
Madison WI 53708-8911**

**E-MAIL:  
DATCPWisconsinPrivacy@Wisconsin.gov**

**WEBSITE: [privacy.wi.gov](http://privacy.wi.gov)**

**Toll-free in WI: (800) 422-7128**

**(608) 224-5163**

**FAX: (608) 224-4677**

**TTY: (608) 224-5058**



# Wisconsin Lawyer™

THE OFFICIAL PUBLICATION OF THE STATE  
BAR OF WISCONSINNOVEMBER   VOLUME   NUMBER  
2012   85   11**WISCONSIN**Lawyer™  
YOUR PRACTICE. OUR PURPOSE.™

## Ethics: Guard Client's Personal Information

Lawyers must keep confidential all client information, including personal information such as Social Security numbers, credit card numbers, and any other information learned or received during the representation. Lawyers must tell clients immediately if their information is lost or breached.

DEAN R. DIETRICH

Comments (0)

SHARE THIS:

A A A

### Question

I require my clients to give me personal information, such as Social Security numbers and credit card numbers for payment of fees. What happens if this information is compromised or lost?

### Answer

A lawyer who obtains personal information from a client is obligated to communicate with the client if that information is lost (or taken). This requirement exists under state law as well as under the Rules of Professional Conduct.

SCR 20:1.6 covers confidentiality of client information. A lawyer is obligated to keep all client information confidential – this means anything learned or received by the attorney during the course of the representation. This would include personal information that the lawyer receives, including credit card information or personal identification information such as a Social Security number or a driver's license number. It is not often that a lawyer will request a Social Security number or a driver's license number (except when representing a client in a traffic matter), but if that information is received, it is considered attorney-client confidential information and must be protected by the lawyer.

The lawyer is also obligated to notify the client if that information is compromised in some fashion, such as by loss of a laptop or someone hacking into the lawyer's computer network. SCR 20:1.4 requires that a lawyer communicate with the client about all things related to the representation and necessary for the client to make decisions regarding the representation. The disclosure of personal information relates to the representation and is something that must be communicated to the client if it occurs.

A Wisconsin statute also affects lawyers' obligations related to client information. Section 134.98 of the Wisconsin Statutes, known as the data breach notification law, requires any business that obtains personal information to notify the individual if that information is somehow disclosed or compromised. This would include information such as a credit card number, a driver's license number, or a Social Security number. The statute specifically defines *personal information* as the following:

"(b) 'Personal information' means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

"1. The individual's [S]ocial [S]ecurity number.

"2. The individual's driver's license number or state identification number.

"3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.

"4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a).

"5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation."

A business is obligated to notify the individual within 30 days of becoming aware that the information has been compromised or disclosed in some manner, whether by negligence or by some intentional act of another person. To comply with this law, a lawyer is required, for example, to notify the client if the lawyer loses a laptop or some other computer equipment that contains a client's personal information. Notification may also be required if a laptop is lost but it does not contain or give access to information that would be considered personal information.



**Dean R. Dietrich,**  
*Marquette 1977, of  
Ruder Ware, Wausau, is  
past chair of the State  
Bar Professional Ethics  
Committee. He can be  
reached at  
ddietrich@ruderware.com.*

Lawyers must be careful to protect any information learned during the course of representation, including clients' personal information, whether obtained for purposes of representation or for purposes of obtaining payment for fees. Lawyers should exercise caution in all respects to ensure that this information is protected from either inadvertent disclosure or some type of unauthorized disclosure.

For more information on protecting client information, see "25 Tips to Prevent Law Firm Data Breaches" elsewhere in this issue.



# COMMONWEALTH OF MASSACHUSETTS

## OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION

10 Park Plaza – Suite 5170, Boston MA 02116  
(617) 973-8700 FAX (617) 973-8799  
[www.mass.gov/consumer](http://www.mass.gov/consumer)

DEVAL L. PATRICK  
GOVERNOR

TIMOTHY P. MURRAY  
LIEUTENANT GOVERNOR

GREGORY BIALECKI  
SECRETARY OF HOUSING AND  
ECONOMIC DEVELOPMENT

BARBARA ANTHONY  
UNDERSECRETARY

### **A Small Business Guide: Formulating A Comprehensive Written Information Security Program**

While the contents of any comprehensive written information security program required by 201 CMR 17.00 must always satisfy the detailed provisions of those regulations; and while the development of each individual program will take into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information, the Office of Consumer Affairs and Business Regulation is issuing this guide to help small businesses in their compliance efforts. **This Guide is not a substitute for compliance with 201 CMR 17.00.** It is simply a tool designed to aid in the development of a written information security program for a small business, including the self employed, that handles “personal information.”

Having in mind that wherever there is a conflict found between this guide and the provisions of 201 CMR 17.00, it is the latter that will govern. We set out below this “guide” to devising a security program (references below to “we” and “our” are references to the small business to whom the real WISP will relate):

## **COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM**

### **I. OBJECTIVE:**

Our objective, in the development and implementation of this comprehensive written information security program (“WISP”), is to create effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts, and to comply with obligations under 201 CMR 17.00. The WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts. For purposes of this WISP, “personal information” means a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c)





financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

## **II. PURPOSE:**

The purpose of the WISP is to:

- (a) Ensure the security and confidentiality of personal information;
- (b) Protect against any anticipated threats or hazards to the security or integrity of such information
- (c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

## **III. SCOPE:**

In formulating and implementing the WISP, (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (4) design and implement a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and (5) regularly monitor the effectiveness of those safeguards:

## **IV. DATA SECURITY COORDINATOR:**

We have designated \_\_\_\_\_ to implement, supervise and maintain the WISP. That designated employee (the "Data Security Coordinator") will be responsible for:

- a. Initial implementation of the WISP;
- b. Training employees;
- c. Regular testing of the WISP's safeguards;
- d. Evaluating the ability of each of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, consistent with 201 CMR 17.00; and requiring such third party service providers by contract to implement and maintain appropriate security measures.
- e. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.
- f. Conducting an annual training session for all owners, managers, employees and independent

contractors, including temporary and contract employees who have access to personal information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the firm's requirements for ensuring the protection of personal information.

## **V. INTERNAL RISKS:**

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately. To the extent that any of these measures require a phase-in period, such phase-in must be completed on or before March 1, 2010:

### **Internal Threats**

- A copy of the WISP must be distributed to each employee who shall, upon receipt of the WISP, acknowledge in writing that he/she has received a copy of the WISP.
- There must be immediate retraining of employees on the detailed provisions of the WISP.
- Employment contracts must be amended immediately to require all employees to comply with the provisions of the WISP, and to prohibit any nonconforming use of personal information during or after employment; with mandatory disciplinary action to be taken for violation of security provisions of the WISP (*The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the personal information affected by the violation*).
- The amount of personal information collected should be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to us to comply with other state or federal regulations.
- Access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish your legitimate business purpose or to enable us comply with other state or federal regulations.
- Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.
- All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Coordinator shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.



- Terminated employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
- A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys.
- Current employees' user ID's and passwords must be changed periodically.
- Access to personal information shall be restricted to active users and active user accounts only.
- Employees are encouraged to report any suspicious or unauthorized use of customer information.
- Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.
- Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.
- At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with the WISP's rules for protecting the security of personal information.
- Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers.
- Access to electronically stored personal information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.
- Visitors' access must be restricted to one entry point for each building in which personal information is stored, and visitors shall be required to present a photo ID, sign-in and wear a plainly visible "GUEST" badge or tag. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with M.G.L. c. 93I.

## **VI. EXTERNAL RISKS**

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures must be completed on or before March 1, 2010:

### **External Threats**

- There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.
- There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.
- To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.
- All computer systems must be monitored for unauthorized use of or access to personal information.
- There must be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location.



---

**Wisconsin Formal Ethics Opinion EF-15-01:  
Ethical Obligations of Attorneys Using Cloud Computing**

**March 23, 2015**

---

**Synopsis**

*A lawyer may use cloud computing as long as the lawyer uses reasonable efforts to adequately address the risks associated with it. The Rules of Professional Conduct require that lawyers act competently to protect client information and confidentiality as well as to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed.*

*To be reasonable, the lawyer's efforts must be commensurate with the risks presented. Among the factors to be considered in assessing that risk are the information's sensitivity; the client's instructions and circumstances; the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party; the attorney's ability to assess the technology's level of security; the likelihood of disclosure if additional safeguards are not employed; the cost of employing additional safeguards; the difficulty of implementing the safeguards; the extent to which the safeguards adversely affect the lawyer's ability to represent clients; the need for increased accessibility and the urgency of the situation; the experience and reputation of the service provider; the terms of the agreement with the service provider; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.*

*To determine what efforts are reasonable, lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication, and encryption for information stored both in the cloud and on the ground. Lawyers should also understand the dangers of using public Wi-Fi and file sharing sites. Lawyers who outsource cloud computing services should understand the importance of selecting a provider that uses appropriate security protocols. Lawyers should also understand the importance of regularly backing up data and storing data in more than one place. A lawyer may consult with someone who has the necessary knowledge to help determine what efforts are reasonable.*

**Introduction**

Technology has dramatically changed the practice of law in many ways, including the ways in which lawyers process, transmit, store, and access client information. Perhaps no area has seen greater change than "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your

computer.”<sup>1</sup> In other words, cloud computing includes the processing, transmission, and storage of the client’s information using shared computer facilities or remote servers owned or leased by a third-party service provider.<sup>2</sup> These facilities and services are accessed over the Internet by the lawyer’s networked devices such as computers, tablets, and smart phones.<sup>3</sup>

Many lawyers welcome cloud computing as a way to reduce costs, improve efficiency, and provide better client service. The cloud service provider assumes responsibility for infrastructure, application software, development platforms, developer and programming staff, licensing, updates, security and maintenance, while the lawyer enjoys access to the client information from any location that has Internet access. Along with the lawyer’s increased accessibility comes the loss of direct control over the client’s information. The provider of cloud computing adds a layer of risk between the lawyer and client’s information because most of the physical, technical, and administrative safeguards are managed by the cloud service provider. Yet the ultimate responsibility for insuring the confidentiality and security of the client’s information lies with the lawyer.

As cloud computing becomes more ubiquitous and as clients demand more efficiency, the question for counsel is no longer whether to use cloud computing, but how to use cloud computing safely and ethically. Lawyers may disagree about how to balance the competing risks of security breaches and provider outages, on the one hand, and the convenience of access and protection from natural or local disasters, on the other. Yet, whatever decision a lawyer makes must be made with reasonable care, and the lawyer should be able to explain what factors were considered in making that decision.

Ethics opinions from other states that have addressed the issue of cloud computing have generally concluded that a lawyer may use cloud computing if the lawyer uses reasonable efforts to adequately address the risks in doing so.<sup>4</sup> But the definition of what is reasonable varies.

The State Bar’s Standing Committee on Professional Ethics (the “Committee”) agrees with the conclusion of ethics opinions from other states that cloud computing is permissible as long as the lawyer uses reasonable efforts to adequately address the potential risks associated with it. Part I of this opinion

---

<sup>1</sup> Pennsylvania Bar Ass’n Comm. on Legal Ethics and Professional Responsibility Formal Ethics Opinion 2011-200 (2011), at 1 (quoting Quinn Norton, “Byte Rights,” *Maximum PC*, September 2010, at 12). A more detailed definition is difficult to formulate because cloud computing is not a single system, but includes different technologies, configurations, service models, and deployment models. For example, cloud computing encompasses web-based email, online data storage, software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). Deployment models include public clouds, private clouds, hybrid clouds, and managed clouds.

<sup>2</sup> “These remote servers may be hosted in data centers worldwide, allowing cloud service providers to distribute computing power, storage capacity and data across their data centers dynamically to provide fast delivery and on-demand bandwidth.” Stuart D. Levi and Kelly C. Riedel, “Cloud Computing: Understanding the Business and Legal Issues,” *Practical Law*, <http://us.practicallaw.com/8-501-5479>

<sup>3</sup> The National Institute of Standards and Technology defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Wayne Jansen & Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, Special Publication # 800-145 (September 2011). Almost any information technology or computing resource can be delivered as a cloud service.

<sup>4</sup> Appendix A to this opinion provides a brief description of the ethics opinions from other states.

identifies the specific rules of Wisconsin's Rules of Professional Conduct for Attorneys that are implicated by cloud computing and the duties imposed by those rules. Part II of this opinion discusses what constitutes reasonable efforts to protect the lawyer's access to and the confidentiality of client information.

## **Part I: The Applicable Rules**

Several rules are implicated by the use of cloud computing. These rules are SCR 20:1.1 Competence, SCR 20:1.4 Communication, SCR 20:1.6 Confidentiality, and SCR 20:5.3 Responsibilities regarding nonlawyer assistants.

### **A. SCR 20:1.1 Competence**

SCR 20:1.1 requires a lawyer to perform legal services competently.<sup>5</sup> ABA Comment [8] to Model Rule 1.1, amended in 2012, recognizes that technology is an integral part of contemporary law practice and explicitly reminds lawyers that the duty to remain competent includes keeping up with technology.

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Moreover, ABA Comment [5] recognizes that competency also requires the "use of methods and procedures meeting the standards of competent practitioners."

Lawyers who use cloud computing have a duty to understand the use of technologies and the potential impact of those technologies on their obligations under the applicable law and under the Rules. In order to determine whether a particular technology or service provider complies with the lawyer's professional obligations, a lawyer must use reasonable efforts. Moreover, as technology, the regulatory framework, and privacy laws change, lawyers must keep abreast of the changes.

### **B. SCR 20:1.4 Communication**

SCR 20:1.4(b) requires that a lawyer explain a matter to the extent reasonably necessary to permit the client to make informed decisions concerning the representation.<sup>6</sup> While it is not necessary for a

---

<sup>5</sup> SCR 20:1.1 Competence

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

<sup>6</sup> SCR 20:1.4 Communication

(a) A lawyer shall:

(1) Promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in SCR 20:1.0(f), is required by these rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests by the client for information; and

lawyer to communicate every detail of a client's representation, the client should have sufficient information to participate intelligently in decisions concerning the objectives of representation and the means by which they are to be pursued.<sup>7</sup> Of concern is whether a lawyer must inform the client of the means by which the lawyer processes, transmits, and stores the client's information in all representations or only when the circumstances call for it, such as where the information is particularly sensitive.

None of the ethics opinions have suggested that a lawyer is required in all representations to inform the client of the means by which the lawyer processes, transmits, and stores information. One ethics opinion, however, suggests that a lawyer should consider giving notice to the client about the proposed method for storing client information.<sup>8</sup> Yet, lawyers' remote storage of client information is not a new occurrence: lawyers have been using off-site brick-and-mortar storage facilities for many years. Another opinion suggests that "it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of 'cloud computing' and the advantages as well as the risks endemic to online storage and transmission."<sup>9</sup>

While none of the ethics opinions have suggested that a client's informed consent is required in all instances before a lawyer may use cloud computing, one opinion has suggested that client consent may be necessary to use a third-party service provider when the information is highly sensitive.<sup>10</sup> If consent is required, SCR 20:1.4(a)(1) requires that the lawyer promptly inform the client.

The Committee agrees with other ethics opinions that a lawyer is not required in all representations to inform the client that the lawyer uses the cloud to process, transmit or store information. SCR 20:1.4 does not require the lawyer to inform the client of every detail of representation. It does, however, require the lawyer to provide the client with sufficient information so that the client is able to meaningfully participate in his or her representation. "The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation."<sup>11</sup>

While a lawyer is not required in all representations to inform clients that the lawyer uses the cloud to process, transmit or store information, a lawyer may choose, based on the needs and expectations of the clients, to inform the clients. A provision in the engagement agreement or letter is a convenient way to provide clients with this information.

---

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

<sup>7</sup> SCR 20: 1.4 ABA Comment [5].

<sup>8</sup> Vt. Ethics Op. 2010-6 (2011) at 7.

<sup>9</sup> Pa. Ethics Op. 2011-200 at 6.

<sup>10</sup> N.H. Ethics Op. 2012-13/4 at 2.

<sup>11</sup> SCR 20:1.4 ABA Comment [5] (2012).



If there has been a breach of the provider's security that affects the confidentiality or security of the client's information, SCR 20:1.4(a)(3) and SCR 20:1.4(b) require the lawyer to inform the client of the breach.

### **C. SCR 20:1.6 Confidentiality**

The duty to protect information relating to the representation of the client is one of the most significant obligations imposed on the lawyer. SCR 20:1.6(a) prohibits a lawyer from revealing information relating to the representation of a client unless that client gives informed consent or unless the disclosure is impliedly authorized in order to carry out the representation.<sup>12</sup> The processing, transmission, and storage of information in the cloud may be deemed an impliedly authorized disclosure to the provider as long as the lawyer takes reasonable steps to ensure that the provider of the cloud computing services has adequate safeguards.<sup>13</sup>

Although a lawyer has a professional duty to protect information relating to the representation of the client from unauthorized disclosure, this duty does not require any particular means of handling protected information and does not prohibit the employment of service providers who may handle documents or data containing protected information. Lawyers are not required to guarantee that a breach of confidentiality cannot occur when using a cloud service provider, and they are not required to use only infallibly secure methods of communication.<sup>14</sup> They are, however, required, to use reasonable efforts to protect information relating to the representation of their clients from unauthorized disclosure.

The 2012 revision of ABA Model Rule 1.6 and its Comment made "clear that a lawyer has an ethical duty to take reasonable measures to protect a client's confidential information from inadvertent disclosure, unauthorized disclosure, and unauthorized access, regardless of the medium used."<sup>15</sup> A new

---

<sup>12</sup> The provisions in SCR 20:1.6(b) and (c) are not implicated in cloud computing.

#### SCR 20:1.6 Confidentiality

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in pars. (b) and (c).

(b) A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent the client from committing a criminal or fraudulent act that the lawyer reasonably believes is likely to result in death or substantial bodily harm or in substantial injury to the financial interest or property of another.

(c) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably likely death or substantial bodily harm;

(2) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(3) to secure legal advice about the lawyer's conduct under these rules;

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(5) to comply with other law or a court order.

<sup>13</sup> Pa. Ethics Op. 2011-200 at 6.

<sup>14</sup> A.B.A. Comm'n on Ethics 20/20 *Introduction & Overview*, at 8 (August 2012).

<sup>15</sup> A.B.A. Comm'n on Ethics 20/20 *Introduction & Overview*, at 8 (August 2012).

paragraph was added to Model Rule 1.6 stating that “[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.”<sup>16</sup>

Moreover, the 2012 revision of ABA Comment [18] to Model Rule 1.6 emphasizes that unauthorized access to or the inadvertent or unauthorized disclosure of information relating to the representation of a client does not constitute a violation of the rule “if the lawyer has made reasonable efforts to prevent the access or disclosure.” The comment identifies a number of factors to be considered in determining the reasonableness of the lawyer’s efforts. These factors “include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).”<sup>17</sup>

---

<sup>16</sup> Model Rules of Prof’l Conduct R. 1.6(c) (2012). The numbering for SCR 20:1.6 differs from the Model Rule 1.6 because Wisconsin retains in our paragraph (b) the mandatory disclosure requirements that have been a part of the Wisconsin Supreme Court Rules since their initial adoption. SCR 20:1.6(c) contains the discretionary disclosure requirements. Wisconsin Committee Comment to SCR 20:1.6.

<sup>17</sup> ABA Comment [18] to Model Rule 1.6 states:

Acting Competently to Preserve Confidentiality

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

Similarly, the 2012 revision of ABA Comment [19] requires a lawyer, when transmitting a communication that includes information relating to the representation of the client, to take reasonable precautions to prevent the information from coming into the hands of unintended recipients. ABA Comment [19] to Model Rule 1.6 states:

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

A lawyer using cloud computing may encounter circumstances that require unique considerations to secure client confidentiality. For example, if a server used by a cloud service provider is physically located in another country, the lawyer must be sure that the data on that server are protected by laws that are as protective as those of the United States. Whether a lawyer is required to take additional precautions to protect a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.<sup>18</sup>

#### **D. SCR 20:5.3 Responsibilities regarding nonlawyer assistants**

Although a lawyer may use nonlawyers outside the firm to help provide legal services, SCR 20:5.3 requires the lawyer to make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer.<sup>19</sup> The extent of this obligation when using a cloud service provider to process, transmit, store, or access information protected by the duty of confidentiality will depend greatly on the experience, stability, security measures and reputation of the provider as well as the nature of the information relating to the representation of the client.

ABA Comment [3], added as part of the 2012 revisions, identifies distinct concerns that arise when services are performed outside the firm. It recognizes that nonlawyer services can take many forms, such as services performed by individuals and services performed by automated products. It identifies the factors that determine the extent of the lawyer's obligations when using such services, and it also references other Rules of Professional Conduct that the lawyer should consider when using such services. Comment [3] also emphasizes that the lawyer has an obligation to give appropriate instructions to nonlawyers outside the firm when retaining or directing those nonlawyers. For example, when a lawyer retains an investigative service, the lawyer may not be able to directly supervise how a particular investigator completes an assignment, but the lawyer's instructions must be reasonable under the circumstances to provide reasonable assurance that the investigator's conduct is compatible with the lawyer's professional obligations.<sup>20</sup>

---

<sup>18</sup> Model Rules of Prof'l Conduct R. 1.6 Comment [18] (2012).

<sup>19</sup> SCR 20:5.3 Responsibilities regarding nonlawyer assistants

With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

<sup>20</sup> ABA Comment [3] to Model Rule 5.3 states:

[3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When

ABA Comment [4], also added as part of the 2012 revisions, recognizes that clients sometimes direct lawyers to use particular nonlawyer service providers.<sup>21</sup> In such situations, the Comment advises that the lawyer should ordinarily consult with the client to determine how the outsourcing arrangement should be structured and who will be responsible for monitoring<sup>22</sup> the performance of the nonlawyer services.

## **Part II: Reasonable Efforts**

The Rules of Professional Conduct do not impose a strict liability standard on lawyers who use cloud computing, and none of the ethics opinions require extraordinary efforts or a guarantee that information will not be inadvertently disclosed or that the information will always be accessible when needed.<sup>23</sup> Instead, the Rules require that lawyers act competently to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed, as well as to protect client information from unauthorized access and disclosure, whether intentional or inadvertent. Competency requires the lawyer to make reasonable efforts; and to be reasonable, those efforts must be commensurate with the risk presented.

---

using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

<sup>21</sup> ABA Comment [4] to Model Rule 5.3 states:

[4] Where the client directs the selection of a particular nonlawyer service provider outside the firm, the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer. See Rule 1.2. When making such an allocation in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

<sup>22</sup> The ABA Commission on Ethics 20/20 acknowledged that the word "monitoring" reflects "a new ethical concept," but concluded that the new concept was needed because it may not be possible for the lawyer to "directly supervise" a nonlawyer when the nonlawyer is performing the services outside the firm. Report to the House of Delegates Resolution 105C, Report p. 8. The word "monitoring" makes it clear that the lawyer has an obligation to remain aware of how nonlawyer services are being performed. The Comment also reminds lawyers that they have duties to tribunal that may not be satisfied through compliance with this Rule. For example, if a client instructs a lawyer to use a particular electronic discovery vendor, the lawyer cannot cede all monitoring responsibility to the client because the lawyer may have to make certain representations to the tribunal regarding the vendor's work. *Id.*

<sup>23</sup> As one ethics opinion stated: "Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file room, or that someone will not illegally intercept his mail or steal a fax." N.J. Advisory Committee on Professional Ethics Op. No. 701 (2006).

What constitutes reasonable efforts has been the subject of much discussion. It has been suggested that some of the ethics opinions may place unrealistic demands on attorneys.<sup>24</sup> At the same time, it has been suggested that “[i]n sum, basic knowledge of cybersecurity has become an essential lawyer competency.”<sup>25</sup>

This Committee agrees with other ethics opinions that lawyers cannot guard against every conceivable danger when using the cloud to process, transmit, store and access client information. This Committee concludes that lawyers must make reasonable efforts to protect client information and confidentiality as well as to protect the lawyer’s ability to reliably access and provide information relevant to a client’s matter when needed. To be reasonable, those efforts must be commensurate with the risks presented. Because technologies differ and change rapidly, the risks associated with those technologies will vary. Moreover, because the circumstances of each law practice vary considerably, the risks associated with those law practices will also vary. Consequently, what may be reasonable efforts commensurate with the risks for one practice may not be for another. And even within a practice, what may be reasonable efforts for most clients may not be for a particular client.

#### **A. Factors to Consider when Assessing the Risks**

To be reasonable, the lawyer’s efforts must be commensurate with the risks presented by the technology involved, the type of practice, and the individual needs of a particular client. The ABA in its Comments to Model Rules 1.6 and 5.3 as well as other ethics opinions have identified factors for lawyers to consider when assessing the risks. These factors, which are not exclusive, include:

- the information’s sensitivity;<sup>26</sup>
- the client’s instructions and circumstances;<sup>27</sup>

---

<sup>24</sup> One expert in the field of data security, Stuart L. Pardau, points out that some ethics opinions, such as Pennsylvania Ethics Op. 2011-200, direct attorneys to negotiate favorable terms of use with the cloud service providers, even though the opinions acknowledge that the providers’ terms are usually “take it or leave it” and that a typical attorney is powerless to require a cloud provider to do anything beyond the boilerplate terms. Stuart L. Pardau, “But I’m Just a Lawyer: Do Cloud Ethics Opinions Ask Too Much?” *The Professional Lawyer*, Vol. 22, Number 4 2014. Pardau also notes that some opinions require attorneys to know information that they have no practical way of knowing. As examples, Pardau cites Nevada Formal Ethics Op. 33 (2006), which concludes that the attorney will not be responsible for a cloud service provider’s breach of confidentiality if the attorney “instructs and requires the third party contractor to keep the information confidential and inaccessible,” and New Hampshire Ethics Op. 2012-13/4 opinion, which advises that the attorney “must know at all times where sensitive client information is stored, be it in the cloud or elsewhere.” Pardau further observes that “[s]ome of the state bar ethics opinions go too far in requiring attorneys to understand cloud security and monitor providers,” citing Alabama Formal Ethics Op. 2010-02, which states that a lawyer has “a continuing duty to stay abreast of the appropriate safeguards that should be employed by ... the third-party vendor.”

<sup>25</sup> Andrew Perlman, “The Twenty-First Century Lawyer’s Evolving Ethical Duty of Competence” *The Professional Lawyer*, Vol. 22, Number 4 2014. Perlman, a law school professor who directs an institute on law practice technology, observes that lawyers “store a range of information in the ‘cloud’ (both private and public) as well as on the ‘ground’ using smartphones, laptops, tablets, and flash drives.” He further observes that this “information is easily lost or stolen; it can be accessed without authority (e.g., through hacking); it can be inadvertently sent; it can be intercepted in transit; and it can be accessed without permission by foreign governments or the National Security Agency.” He concludes that “[i]n light of these dangers, lawyers need to understand how to competently safeguard confidential information.”

<sup>26</sup> ABA Model Rule 1.6 Comment [18]. The more sensitive the information, the less risk an attorney should take.

<sup>27</sup> Calif. Formal Ethics Op. 2010-179 (2010). A lawyer must follow the client’s instructions unless doing so would cause the lawyer to violate the Rules of Professional Conduct or other law. Moreover, a lawyer should consider any circumstances that may be

- the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party;<sup>28</sup>
- the attorney's ability to assess the technology's level of security;<sup>29</sup>
- the likelihood of disclosure if additional safeguards are not employed;<sup>30</sup>
- the cost of employing additional safeguards;<sup>31</sup>
- the difficulty of implementing the additional safeguards;<sup>32</sup>
- the extent to which the additional safeguards adversely affect the lawyer's ability to represent clients;<sup>33</sup>
- the need for increased accessibility and the urgency of the situation;<sup>34</sup>
- the experience and reputation of the service provider;<sup>35</sup>
- the terms of the agreement with the service provider;<sup>36</sup> and
- the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.<sup>37</sup>

---

relevant. For example, if the attorney is aware that other people have access to the client's devices or accounts and may intercept client information, the attorney should consider that in assessing the risk.

<sup>28</sup> ABA Model Rule 1.6 Comment [18].

<sup>29</sup> Calif. Formal Ethics Op. 2010-179 (2010). The opinion concludes:

Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.

Similarly, Iowa Ethics Op. 11-01 (2011) concludes:

The Committee recognizes that performing due diligence regarding information technology can be complex and requires specialized knowledge and skill. This due diligence must be performed by individuals who possess both the requisite technology expertise and as well as an understanding of the Iowa Rules of Professional Conduct. The Committee believes that a lawyer may discharge the duties created by Comment 17 by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees.

<sup>30</sup> ABA Model Rule 1.6 Comment [18].

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*

<sup>34</sup> Calif. Formal Ethics Op. 2010-179 (2010).

<sup>35</sup> ABA Model Rule 5.3 Comment [3].

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

Once the lawyer has assessed the risks by considering the various factors, the lawyer is able to determine what efforts are reasonable to protect against those risks.

## **B. General Guidance**

It is impossible to provide specific requirements for reasonable efforts because lawyers' ethical duties are continually evolving as technology changes. Specific requirements would soon become obsolete. Moreover, the risks vary with the technology involved, the type of practice, and the individual needs of a particular client.<sup>38</sup> Lawyers must exercise their professional judgment in adopting specific cloud-based services, just as they do when choosing and supervising other types of service providers, and specific requirements would do little to assist the exercise of professional judgment. It is possible, however, to provide some guidance.

- Lawyers should have "at least a base-level comprehension of the technology and the implications of its use."<sup>39</sup> While attorneys are not required to understand precisely how the technology works, competence requires at least a cursory understanding of the technology used. Such a cursory understanding is necessary to explain to the client the advantages and risks of using the technology in the representation.<sup>40</sup>
- Lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication,<sup>41</sup> and encryption for information stored both in the cloud and on the ground.<sup>42</sup> Lawyers should also understand the security dangers of using public Wi-Fi and file sharing sites.
- Lawyers who outsource cloud-computing services should understand the importance of selecting a provider that uses appropriate security protocols. "While complete security is never achievable, a prudent attorney will employ reasonable precautions and thoroughly research a cloud storage vendor's security measures and track record prior to utilizing the service."<sup>43</sup> Knowing the qualifications, reputation, and longevity of the cloud-service provider is necessary, just like knowing the qualifications, reputation, and longevity of any other service provider.

---

<sup>38</sup> For example, the efforts required of a lawyer whose practice is limited to patent law will vary from the efforts required of a lawyer whose practice is limited to family law because the risks presented by a patent law practice differ from risks presented by a family law practice. Even within the patent law practice, the efforts may vary depending on the needs of a particular client.

<sup>39</sup> Joshua H. Brand, "Cloud Computing Services – Cloud Storage," *Minnesota Lawyer* (01/01/2012) at 1. Accessed at [http://www.docstoc.com/docs/117971742/Cloud-Computing-Services-\\_-Cloud-Storage-by-Joshua-H-Brand](http://www.docstoc.com/docs/117971742/Cloud-Computing-Services-_-Cloud-Storage-by-Joshua-H-Brand).

<sup>40</sup> *Id.*

<sup>41</sup> Multifactor authentication ensures that data can be accessed only if the lawyer has the correct password as well as another form of identification, such as a code sent by text message to the lawyer's mobile phone.

<sup>42</sup> "On the ground" refers to the use of smart phones, tablets, laptops, and flash drives.

<sup>43</sup> Brand at 2.

- Lawyers should read and understand the cloud-based service provider's terms of use or service agreement.<sup>44</sup>
- Lawyers should also understand the importance of regularly backing up data and storing data in more than one place.
- Lawyers who do not have the necessary understanding should consult with someone who has the necessary skill and expertise, such as a technology consultant, to help determine what efforts are reasonable.<sup>45</sup>
- Lawyers should also consider including a provision in their engagement agreements or letters that, at the least, informs and explains the use of cloud-based services to process, transmit, store and access information. Including such a provision not only gives the client an opportunity to object, but it also provides an opportunity for the lawyer and client to discuss the advantages and the risks.

---

<sup>44</sup> Lawyers should pay particularly close attention to the following terms:

*Ownership of the Information*

Do the terms of use specifically state that the provider has no ownership interest in the information? What happens to the information if the provider goes out of business or if the lawyer decides to terminate the business relationship, or if the lawyer defaults on payments?

*Location of the Information*

Where is information stored? Many providers replicate the information to data centers or servers in other countries with less stringent legal protections. What is the provider's response to government or judicial attempts to obtain client information?

*Security and Confidentiality of Information*

What safeguards does the provider have to prevent security breaches? What obligations does the provider have to protect the confidentiality of information? Does the provider agree to promptly notify the lawyer of known security breaches that affect the confidentiality of the lawyer's information?

*Service Level*

Does the service provider have an uptime guarantee? Most providers agree to a 99.9% uptime, although some providers agree to a higher uptime approaching 99.999%.

*Backups*

How frequently does the provider backup the information? How easy is it to restore the information from the backup?

*Disaster Recovery*

Does your provider have a secondary data center or redundant storage that automatically assumes control if disaster strikes the data center or server?

<sup>45</sup> Wa. Ethics Op. 2215 (2012) concludes:

It is also impractical to expect every lawyer who uses such services to be able to understand the technology sufficiently in order to evaluate a particular service provider's security systems. A lawyer using such a service must, however, conduct a due diligence investigation of the provider and its services and cannot rely on lack of technological sophistication to excuse the failure to do so.

Similarly, the California ethics opinion acknowledges that an attorney need not "develop a mastery of the security features and deficiencies of each technology available," but advises that if an attorney lacks the expertise to evaluate cloud providers, "he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant." Calif. Formal Ethics Op. 2010-179. Likewise, the Arizona ethics opinion concludes that lawyers must "recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field." Ariz. Ethics Op. 09-04 (2009).



## **Conclusion**

Ethics opinions from other states that have addressed the issue of cloud-based services have generally concluded that a lawyer may use cloud computing if the lawyer takes reasonable care in doing so. This Committee agrees with the opinions issued by other states that cloud computing is permissible as long as the lawyer adequately addresses the potential risks associated with it. The Committee concludes that lawyers must make reasonable efforts to protect client information and confidentiality as well as to protect the lawyer's ability to reliably access and provide information relevant to a client's matter when needed. To be reasonable, those efforts must be commensurate with the risks presented. Lawyers must exercise their professional judgment when adopting specific cloud-based services, just as they do when choosing and supervising other types of service providers.

## **Appendix A**

### **Cloud Ethics Opinions**

#### **Alabama**

Alabama State Bar Disciplinary Commission

Ala. Ethics Op. 2010-02 (2010)

Lawyers may outsource the storage of client files through cloud computing if reasonable steps are taken to make sure the information is protected. Lawyers must be knowledgeable about how the data will be stored and its security, and must reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Lawyers must also stay abreast of security safeguards.

#### **Arizona**

State Bar of Arizona Committee on the Rules of Professional Conduct

Ariz. Ethics Op. 09-04 (2009)

Lawyers may use an online file storage and retrieval system that enables clients to access their files as long as the lawyers take reasonable precautions to protect the security and confidentiality of the information. Lawyers must “recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.” Lawyers must also periodically review the security measures. “If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider.”

#### **California**

State Bar of California Standing Committee on Professional Responsibility and Conduct

Calif. Formal Ethics Op. 2010-179 (2010)

A lawyer’s duties of confidentiality and competence require the lawyer to take appropriate steps to ensure that his or her use of technology does not subject client information to an undue risk of unauthorized disclosure. Among the factors to be considered are the technology’s level of security, the information’s sensitivity, the urgency of the matter, the possible effect inadvertent disclosure or unauthorized interception could pose to a client or third party, as well as client instructions and circumstances.

With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client’s matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall. Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.

## **Connecticut**

Connecticut Bar Association Professional Ethics Committee

Conn. Informal Ethics Op. 2013-07(2013)

A “lawyer outsourcing cloud computing tasks (of transmitting, storing and processing data) must exercise reasonable efforts to select a cloud service provider whose conduct is compatible with the professional obligations of the lawyer and is able to limit authorized access to the data, ensure that the data is preserved (“backed up”), reasonably available to the lawyer, and reasonably safe from unauthorized intrusion.” The Professional Ethics Committee acknowledged that although the technology examined by it in 1999 might now be obsolete, “the need for a lawyer to thoughtfully and thoroughly evaluate the risks presented by the use of current technology remains as vital as ever.” As concluded by the Committee in 1999, the lawyer’s efforts must be commensurate with the risk presented. “The lawyer should be satisfied that the cloud service provider’s (1) transmission, storage and possession of the data does not diminish the lawyer’s ownership of and unfettered accessibility to the data, and (2) security policies and mechanisms to segregate the lawyer’s data and prevent unauthorized access to the data by others including the cloud service provider.”

## **Florida**

The Florida Bar Professional Ethics Committee

Fla. Ethics Op. 12-3 (2013)

Relying on the New York State Bar Ethics Opinion 842 (2010) and Iowa Ethics Opinion 11-10 (2011), the opinion concludes that lawyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained, that the service provider maintains adequate security, and that the lawyer has adequate access to the information stored remotely. Lawyers should research the service provider used and also consider backing up the data elsewhere as a precaution.

## **Iowa**

Iowa State Bar Association Committee on Ethics and Practice Guidelines

Iowa Ethics Op. 11-01 (2011)

The opinion concludes that the lawyer is obligated “to perform due diligence to assess the degree of protection that will be needed and to act accordingly.” The opinion gives basic guidance by listing questions that the lawyer should ask:

### **Accessibility**

1. *Access:*  
Will I have unrestricted access to the stored data? Have I stored the data elsewhere so that if access to my data is denied I can acquire the data via another source?
2. *Legal Issues:*  
Have I performed “due diligence” regarding the company that will be storing my data? Are they a solid company with a good operating record and is their service recommended by others in the field? What country and state are they located and do business in? Does their end user’s licensing agreement (EULA) contain legal restrictions regarding their responsibility or liability, choice of law or forum, or limitation on damages? Likewise does their EULA grant them proprietary or user rights over my data?

3. *Financial Obligations:*

What is the cost of the service, how is it paid and what happens in the event of non-payment? In the event of a financial default will I lose access to the data, does it become property of the SaaS company or is the data destroyed?

4. *Termination:*

How do I terminate the relationship with the SaaS company? What type of notice does the EULA require? How do I retrieve my data and does the SaaS company retain copies?

#### Data Protection

1. *Password Protection and Public Access:*

Are passwords required to access the program that contains my data? Who has access to the passwords? Will the public have access to my data? If I allow non-clients access to a portion of the data will they have access to other data that I want protected?

2. *Data Encryption:*

Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?

The opinion recognizes that performing due diligence can be complex and requires specialized knowledge and skill. The opinion also acknowledges that a law firm may discharge the duties “by relying on the due diligence services of independent companies, bar associations or other similar organizations or through its own qualified employees.”

#### Maine

Maine State Bar Association Professional Ethics Committee

Maine Ethics Op. 194 (2008)

Lawyers may use third-party electronic back-up and transcription services as long as appropriate safeguards are taken, including reasonable efforts to prevent the disclosure of confidential information, and an agreement with the vendor that contains “a legally enforceable obligation” to maintain the confidentiality of the client’s information.

#### Massachusetts

Massachusetts Bar Association Committee on Professional Ethics

Mass. Ethics Op. 12-03 (2012)

A lawyer may generally store and synchronize electronic work files containing client information across different platforms and devices using the Internet as long as the lawyer undertakes reasonable efforts to ensure that the provider’s terms of use, privacy policies, practices and procedures are compatible with the Lawyer’s professional obligations. Reasonable efforts would include:

- (a) examining the provider’s terms of use and written policies and procedures with respect to data privacy and the handling of confidential information;
- (b) ensuring that the provider’s terms of use and written policies and procedures prohibit unauthorized access to data stored on the provider’s system, including access by the provider for any purpose other than conveying or displaying the data to authorized users;

- (c) ensuring that the provider's terms of use and written policies and procedures, as well as its functional capabilities, give the Lawyer reasonable access to, and control over, the data stored on the provider's system in the event that the Lawyer's relationship with the provider is interrupted for any reason (e.g., if the storage provider ceases operations or shuts off the Lawyer's account, either temporarily or permanently);
- (d) examining the provider's existing practices (including data encryption, password protection, and system back ups) and available service history (including reports of known security breaches or "holes") to reasonably ensure that data stored on the provider's system actually will remain confidential, and will not be intentionally or inadvertently disclosed or lost; and
- (e) periodically revisiting and reexamining the provider's policies, practices and procedures to ensure that they remain compatible with Lawyer's professional obligations to protect confidential client information reflected in Rule 1.6(a).

The lawyer should follow the client's express instructions regarding the use of cloud technology to store and transmit data; and for particularly sensitive client information, the lawyer should obtain client approval before using cloud technology to store or transmit the information.

### **Nevada**

State Bar of Nevada Standing Committee on Ethics and Professional Responsibility

Nev. Formal Ethics Op. 33 (2006)

A lawyer may store client files electronically on a remote server controlled by a third party as long as the firm takes reasonable precautions, such as obtaining the third party's agreement to maintain confidentiality, to prevent both accidental and unauthorized disclosure of confidential information.

### **New Hampshire**

New Hampshire Bar Association Ethics Committee

N.H. Ethics Op. 2012-13/4 (2013)

A lawyer may use cloud computing consistent with his or her ethical obligations, as long as the lawyer takes reasonable steps to ensure that client information remains confidential. The opinion lists ten issues the lawyer must consider: (1) whether the provider is a reputable organization; (2) whether the provider offers robust security measures; (3) whether the data is stored in a retrievable format; (4) whether the provider commingles data belonging to different clients or different lawyers; (5) whether the provider has a license and not an ownership interest in the data; (6) whether the provider has an enforceable obligation to keep the data confidential; (7) whether the servers are located in the United States; (8) whether the provider will retain the data, and for how long, when representation ends or the agreement between the lawyer and the provider terminates; (9) whether the provider is required to notify the lawyer if the information is subpoenaed, if the law permits such notice; and (10) whether the provider has a disaster recovery plan with respect to the data.

### **New Jersey**

Advisory Committee on Professional Ethics (appointed by the Supreme Court of New Jersey)

N.J. Ethics Op. 701 (2006)

When using electronic filing systems, lawyers must exercise reasonable care against unauthorized access. "The touchstone in using 'reasonable care' against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider under circumstances in which there is an enforceable

obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data.”

### **New York**

New York State Bar Association Committee on Professional Ethics

N.Y. State Bar Ethics Op. 842 (2010)

A lawyer may use an online computer data storage system to store client files provided “the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained.” Reasonable care includes “(1) ensuring that the provider has enforceable obligations to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information; (2) investigating the online data storage provider’s security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances; (3) employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and (4) investigating the storage provider’s ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.” In addition, the lawyer should stay informed of both technological advances that could affect confidentiality and changes in the law that could affect any privilege protecting the information.

### **North Carolina**

North Carolina State Bar Ethics Committee

N.C. Formal Ethics Op. 2011-6 (2012)

“This opinion does not set forth specific security requirements because mandatory security measures would create a false sense of security in an environment where the risks are continually changing. Instead, due diligence and frequent and regular education are required.” The opinion, however, recommends some security measures.

- Inclusion in the SaaS vendor’s Terms of Service or Service Level Agreement, or in a separate agreement between the SaaS vendor and the lawyer or law firm, of an agreement on how the vendor will handle confidential client information in keeping with the lawyer’s professional responsibilities.
- If the lawyer terminates the use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm will have a method for retrieving the data, the data will be available in a non-proprietary format that the law firm can access, or the firm will have access to the vendor’s software or source code. The SaaS vendor is contractually required to return or destroy the hosted data promptly at the request of the law firm.
- Careful review of the terms of the law firm’s user or license agreement with the SaaS vendor including the security policy.
- Evaluation of the SaaS vendor’s (or any third party data hosting company’s) measures for safeguarding the security and confidentiality of stored data including, but not limited to, firewalls, encryption techniques, socket security features, and intrusion-detection systems.
- Evaluation of the extent to which the SaaS vendor backs up hosted data.

The opinion also encourages law firms to consult periodically with professionals competent in the area of online security because of the rapidity with which computer technology changes.

## **Ohio**

Ohio State Bar Association Professionalism Committee

Ohio State Bar Association Informal Advisory Op. 2013-03

“[A] lawyer’s duty to preserve the confidentiality of cloud-stored client data is to exercise competence (1) in selecting an appropriate vendor, (2) in staying abreast of technology issues that have an impact on client data storage and (3) in considering whether any special circumstances call for extra protection for particularly sensitive client information or for refraining from using the cloud to store such particularly sensitive information.” When selecting a vendor, it is necessary for the lawyer to know the qualifications, reputation, and longevity of the vendor, and to read and understand the agreement entered into with the vendor. The opinion lists the following “commonly-occurring issues”:

- What safeguards does the vendor have to prevent confidentiality breaches?
- Does the agreement create a legally enforceable obligation on the vendor’s part to safeguard the confidentiality of the data?
- Do the terms of the agreement purport to give “ownership” of the data to the vendor, or is the data merely subject to the vendor’s license?
- How may the vendor respond to government or judicial attempts to obtain disclosure of your client data?
- What is the vendor’s policy regarding returning your client data at termination of its relationship with your firm? What plans and procedures does the vendor have in case of natural disaster, electric power interruption or other catastrophic events?
- Where is the server located (particularly if the vendor itself does not actually host the data, and uses a data center located elsewhere)? Is the relationship subject to international law?

Consistent with other ethics opinions, such as those from Pennsylvania and New Hampshire, the opinion concludes that storing client data in the cloud does not always require prior consultation because it interprets the language “reasonably consult” as indicating that the lawyer must use judgment in order to determine if the circumstances call for consultation.

## **Oregon**

Oregon State Bar Legal Ethics Committee

Or. Ethics Op. 2011-88

A lawyer “may store client materials on a third-party server as long as the lawyer complies with the duties of competence and confidentiality to reasonably keep the client’s information secure within a given situation.” Reasonable steps to ensure that the vendor will reliably secure client data and keep information confidential “may include, among other things, ensuring the service agreement requires the vendor to preserve confidentiality and security of the materials. It may also require that vendor notify the lawyer of any nonauthorized third-party access to the materials.” Moreover, the lawyer “may be required to reevaluate the protective measures used by the third-party vendor to safeguard the client materials” because as “technology advances, the third-party vendor’s protective measures may become less secure or obsolete over time.”

## **Pennsylvania**

Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility

Pa. Ethics Op. 2011-200

A lawyer “may ethically allow client confidential material to be stored in ‘the cloud’ provided the lawyer takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.” The opinion advises that “[l]awyers may need to consider that at least some data may be too important to risk inclusion in cloud services.” The opinion contains a list of over 30 precautions that reasonable care may require.

## **Vermont**

Vermont Bar Association

Vt. Advisory Ethics Op. 2010-6 (2011)

Lawyers may use cloud computing in connection with client information as long as they take reasonable precautions to protect the confidentiality of and to ensure access to the information. “Complying with the required level of due diligence will often involve a reasonable understanding of: (a) the vendor’s security system; (b) what practical and foreseeable limits, if any, may exist to the lawyer’s ability to ensure access to, protection of, and retrieval of the data; (c) the material terms of the user agreement; (d) the vendor’s commitment to protecting the confidentiality of the data; (e) the nature and sensitivity of the stored information; (f) notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and (g) other regulatory, compliance and document retention obligations that may apply based upon the nature of the stored data and the lawyer’s practice. In addition, the lawyer should consider: (a) giving notice to the client about the proposed method for storing client data; (b) having the vendor’s security and access systems reviewed by competent technical personnel; (c) establishing a system for periodic review of the vendor’s system to be sure the system remains current with evolving technology and legal requirements; and (d) taking reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present.”

## **Virginia**

Virginia Bar Association Standing Committee on Legal Ethics

Va. Legal Ethics Op. 1872 (2013)

“When a lawyer is using cloud computing or any other technology that involves the use of a third party for the storage or transmission of data, the lawyer must follow Rule 1.6(b)(6) and exercise care in the selection of the vendor, have a reasonable expectation that the vendor will keep the data confidential and inaccessible by others, and instruct the vendor to preserve the confidentiality of the information. The lawyer will have to examine the third party provider’s use of technology and terms of service in order to know whether it adequately safeguards client information, and if the lawyer is not able to make this assessment on her own, she will have to consult with someone qualified to make that determination.” Virginia’s Rule 1.6(b)(6) provides that to the extent a lawyer reasonably believes necessary, the lawyer may reveal “information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.”



**Washington**

Washington State Bar Association Rules of Professional Conduct Committee

Wa. Ethics Op. 2215 (2012)

This opinion suggests that the best practices for lawyers “without advanced technological knowledge” would include: “(1) Familiarization with the potential risks of online data storage and review of available general audience literature and literature directed at the legal profession about cloud computing industry standards and features. (2) Evaluation of the provider’s practices, reputation, and history. (3) Comparison of provisions in the service provider agreements to the extent that the service provider recognizes the lawyer’s duty of confidentiality and agrees to handle the information accordingly. (4) Comparison of provisions in service provider agreements to the extent that the agreement gives the lawyer methods for retrieving the data if the agreement is terminated or the service provider goes out of business. (5) Confirming provisions in the agreement that will give the lawyer prompt notice of any nonauthorized access to the lawyer’s stored data. (6) Ensure secure and tightly controlled access to the storage system maintained by the service provider. (7) Ensure reasonable measures for secure backup of the data that is maintained by the service provider.”

## Appendix

### A Checklist: Using Reasonable Efforts

This checklist is divided into two sections: “Law Office Policies and Procedures” and “Choosing a Provider.”

The “Law Office Policies and Procedures” section provides guidance for using reasonable efforts to ensure that the law firm has office policies and procedures in place that are designed to protect both the lawyer’s access to and the confidentiality of client information when using cloud-based services.

The “Choosing a Provider” section provides guidance for using reasonable efforts in choosing a service provider for cloud-based services.

#### I. Law Office Policies and Procedures

##### *Lawyers’ Policies and Procedures regarding Computer Security*

- ☐ Do you use a firewall to prevent unauthorized access?
- ☐ Do you use virus and spyware programs to guard against malware?
- ☐ Are your operating systems up to date with the latest security protections?
- ☐ Do you use strong passwords to protect desktop computers, laptop computers, tablets, and smart phones from unauthorized access?
- ☐ Do you have procedures in place requiring that all employees of the firm who use cloud-based services receive training on and must abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords?
- ☐ Do you have procedures in place requiring all employees of the firm to verify the identity of individuals to whom information protected by the duty of confidentiality is disclosed?
- ☐ Do you have electronic audit trail procedures to monitor who is accessing the data?
- ☐ Do you have procedures in place to avoid inadvertent disclosure of information, such as the disclosure of information in metadata?

- ☐ Do you have procedures in place to address security breaches, including the identification of persons to be notified about any known or suspected breach involving information protected by the duty of confidentiality?<sup>1</sup>

*Lawyers' Policies and Procedures regarding Reasonable Access to Client Information*

- ☐ Do you regularly back up data in case it has been lost, corrupted, or accidentally deleted?
- ☐ Do you protect the ability to represent the client by storing a copy of the data onsite?
- ☐ Do you have an alternate way to connect to the internet since cloud services are accessed through the internet?

*Lawyers' Policies and Procedures regarding Encryption*

- ☐ Do you have procedures in place to determine when electronic records containing client information should be encrypted?
- ☐ Do you have procedures in place to determine if the client wants the electronic records encrypted?

---

<sup>1</sup> Wis. Stat. § 134.98 requires notice of the unauthorized acquisition of personal information. It provides in part:

**(a)** If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.

**(b)** If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident of this state who is the subject of the personal information.

**(bm)** If a person, other than an individual, that stores personal information pertaining to a resident of this state, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the personal information shall notify the person that owns or licenses the personal information of the acquisition as soon as practicable.

### *Lawyers' Policies and Procedures regarding Informing the Client*

- ☐ Do you provide information about the use of cloud computing in your engagement agreements?
- ☐ Do you obtain the client's informed consent to use cloud computing when the information is sensitive?

### *Provider's History of Performance and Reliability*

- ☐ Does the provider disclose its history of performance and reliability? Have you examined the provider's available service history including reports of known security breaches?

### *Provider's Information Security Management System*

- ☐ Does the provider offer robust security measures that are based on internationally accepted standards?
- ☐ Does the provider have an enforceable obligation to preserve security?
- ☐ Does the provider have the technology built to withstand a reasonably foreseeable attempt to infiltrate data? Does the provider perform penetration testing?
- ☐ Have you investigated the provider's security of data centers and whether the storage is in multiple centers?
- ☐ Does the provider clearly explain in its service agreement its practices and procedures for handling client information? Does the provider agree to follow those practices and procedures?
- ☐ Have you investigated the provider's existing security practices including data encryption, password protection, and system backups?