THE ST. LOUIS COUNTY BAR ASSOCIATION PRESENTS:
ETHICS, IMPLICIT BIAS AND LITIGATION CLE
Thursday, March 24, 2022, 1:00 – 4:00 p.m., via Zoom
3.0 Total CLE Credit Hours – 2.0 Ethics Credit Hours - 1.0 Elimination of Bias Credit Hours

Moderator: *Lauren Surdyke*
St. Louis County Bar Association, CLE Chair and Executive Committee member,
of Greensfelder, Hemker and Gale, P.C.

1) 1:00 – 1:50 **WHEN THE OCDC SPEAKS, LAWYERS LISTEN: What issues were important to the Office of Chief Disciplinary Counsel in 2021**
Presenter: Paul Petruska of Greensfelder, Hemker and Gale, P.C.

1:50 – 2:00 Break

2) 2:00 – 2:50 **How Labels & Stereotypes Impact Perception**
Presenter: The Honorable Heather Cunningham

2:50 – 3:00 Break

Moderator: *Eric Michael Tuncil,*
St. Louis County Bar Association, President,
of Law Offices of Mary Ann Weems

3) 3:00 – 3:50 **What Makes a Great Litigator** - includes an opportunity for questions and answers
Presenters: The Honorable Heather Cunningham, The Honorable Lorne Baker and The Honorable Jeffery Medler

FORMAT: All participants will be muted, excluding speakers during their designated topic. Please submit questions through the Chat feature.

MATERIALS: Any written materials will be available on March 24, 2022 on the St. Louis County Bar website.

ATTENDANCE CERTIFICATE AND EVALUATION: Will be emailed to you on March 25, 2022.

Followed by a Happy Hour at Café Napoli in Clayton,
with drinks served compliments of our generous sponsor

GREENSFELDER
ATTORNEYS AT LAW

PAUL E. PETRUSKA

COUNSEL
12 Wolf Creek Drive
Suite 100
Belleville, IL 62226
p 618.239.3607
f 618.257.7353
ppetruska@greensfelder.com

Practice Areas

- Litigation
  - Insurance Coverage
  - Product Liability
  - Toxic Tort
  - Transportation & Logistics

Industries

- Construction

Admissions

- Illinois
- Missouri
- U.S. Eastern District of Missouri
- U.S. Western District of Missouri
- U.S. Southern District of Illinois
- U.S. Central District of Illinois
- U.S. Northen District of Illinois

"Working with clients to help them fully understand and evaluate their risks is an important part of my role. I focus on zealously representing their interests not only to resolve disputes but to help prevent future issues."

Paul Petruska is an experienced trial attorney, estate planner and small business advisor who focuses on solving each client's unique problems. Paul's focus on client needs has helped him create a practice that provides a wide spectrum of services. For clients concerned with litigation defense, Paul has disposed of cases through motion practice, obtained defense verdicts in jury tried cases, and successfully handled appeals. For those needing proactive advice to avoid litigation, Paul has served as outside general counsel to draft safety, employment and document retention policies, while also addressing human resource matters. For clients worried about the future, Paul has drafted everything from a simple will to complex trust agreements to address that concern.

Paul's focus on defending each client's unique interests helps him serve as a vital team member for companies in numerous industries. His litigation experience includes matters related to transportation, product liability, employment litigation, construction, personal injury, commercial catastrophic property damage, and toxic torts.

PAUL E. PETRUSKA

8th Circuit Court of Appeals

Education

J.D., St. Louis University School of Law, 1995, *cum laude*

B.A., St. Louis University, 1992, *magna cum laude*

Paul also has a diverse work history. He began as an associate for a medium-size insurance defense firm, became a partner in a boutique litigation firm, and was the chief trial attorney for a large commercial insurer's major case unit. Paul works closely with clients to help them understand, evaluate and address areas of risk to avoid potential litigation. He is well-versed in liability analysis, data analysis and strategic planning, helping him to accurately assess the best course of action in a given dispute.

As new needs have arisen, Paul has looked to address them. During the pandemic, he has drafted policies specific to COVID-19 and advised clients seeking economic relief through COVID-19 programs such as the Paycheck Protection Program, the Economic Injury Disaster Loan, the Shuttered Venue Operator Grant Program and the Restaurant Revitalization Fund.

COMMUNITY/CIVIC ACTIVITIES

- Chaminade College Preparatory School, Mock Trial Team Program, Volunteer

REPRESENTATIVE MATTERS

Transportation Cases

- Pre-Suit Investigation and Defense – For dozens of clients, went to accident scene within hours of a trucking or railroad accident to ensure paper documents, electronic evidence, and employee testimony was preserved for defense in case lawsuits filed. Nearly 50% of the aforementioned pre-suit investigations revealed documents and/or evidence that helped avoid a lawsuit. One example of litigation avoidance was when a receipt was found in the passenger seat of the potential plaintiff's car, indicating he stopped at a restaurant an hour before the accident to get dinner and had three shots of alcohol.
- Lawsuit Defense – Substantial experience in Missouri state, Illinois state and federal courts defending wrongful death lawsuits in trucking and railroad accidents.

PAUL E. PETRUSKA

- Jury Trials – Four railroad Federal Employers' Liability Act (FELA) cases tried to jury verdict.

Catastrophic Property Loss Cases

- Manufacturing facility extensively damaged when a massive pressurized tank exploded (released pressure). Hired a team of experts is six different specialties, ensuring client was prepared to address all damages claims.
- Multi-story building had valve fail causing a flood of six floors, all with multiple tenants. Helped the property owner document the exact cause and quickly put wrong-doers on notice.
- Obtained five defense verdicts from a jury in Ozark County Missouri after a jury trial of tractor damage from contaminated diesel fuel.

Manufacturing Cases

- Rule 12 Motion to Dismiss was granted in one of the earliest internet defamation cases. Plaintiff, the owner of nutritional supplement company, filed claims against multiple other nutritional supplement companies alleging they were defaming him personally on an internet message board that was vital to their business. My client was dismissed, partially because of my citation to the MTV show Beavis and Butt-head.
- Motion for Summary Judgment was granted in a heavy equipment product liability cases based on the Illinois strict product liability statute of repose.
- Successfully defended automotive manufacturer in alleged airbag defect case.
- Successfully defended tire manufacturer in lawsuit alleging tire ruptured while SUV was traveling on the highway, causing serious personal injury to the driver.

Automotive Dealership Cases

- Kenneth Bell v. Baldwin Chevrolet, 561 S.W.3d 469 (Mo. Ct. App. 2018) – won a Motion for Summary Judgment at trial on all claims relating to an allegedly defective Corvette. Subsequently won the appeal.
- Motion to Dismiss for lack of subject matter jurisdiction was granted by Eastern District of Missouri. Plaintiff alleged she was injured when her car, without warning, moved in her driveway and struck her. Plaintiff brought the claim in federal court alleging diversity jurisdiction and that she was a resident of a state other than Missouri. The Motion to Dismiss was granted because there was uncontradicted evidence that Plaintiff was a resident of Missouri.

PAUL E. PETRUSKA

Employment Cases

- Discrimination Claim Defense – Tried a race discrimination claim in front of jury in the Western District of Missouri federal court. The Judge allowed the submission of multiple years of economic loss, emotional distress and punitive damages. We kept the verdict to $60,000 including attorneys' fees.
- Pre-Suit Investigation – Upon complaint by employee, we performed the investigation to documents the legitimacy of the complaint, or lack thereof.
- Administrative Defense – Successfully defended discrimination claims in the U.S. Equal Employment Opportunity Commission (EEOC), Missouri Commission on Human Rights and the Illinois Department of Human Rights.

Small Business Consultation

- Assisted multiple small businesses in applying and obtaining forgiveness for the first Paycheck Protection Program loans in May 2020.
- Assisted multiple shuttered venue operators obtain grants under the Shutter Venue Operator Grant Program, including one client who obtained a grant over $1.5 million.
- Drafted COVID-19 safety policy for multiple small business clients during the early stages of the Pandemic.

NEWS

Paul Petruska joins Leadership Belleville program
August 18, 2021

Interview with Paul Petruska, "Supreme Court upholds ACA for third time, but new threats loom"
Part B News, June 28, 2021

SEMINARS & SPEAKING ENGAGEMENTS

"The Need to Be More Productive With Less Budget – Can Technology Help?" webinar
Association of Corporate Counsel, St. Louis Chapter, October 21, 2021

"Defense Attorneys' Perspective on Proportionality in Written Discovery and the New Provisions of Federal Rule 30" virtual seminar
Federal Bar Association, July 28, 2021

PAUL E. PETRUSKA

"The Shuttered Venue Operator and Restaurant Revitalization Fund Grant Programs: How to Help Your Clients Access the Billions Available" webinar
Federal Bar Association and MyLawCLE, March 31, 2021

"COVID-19 Business Relief Opportunities" webinar
Greater Belleville Chamber of Commerce, January 28, 2021

Speaker, “Liability Insurance: What Do You Actually Have and What Should You Really Have in Place to Protect Your Railroad”
American Short Line & Regional Railroad Association’s 2012 Convention

Speaker, “Asbestos: Past, Present and Future”
National Business Institute seminar, Asbestos: Current Issues and Effective Litigation Tac-tics

Speaker, “Corporate Electronic Information Policies: Why You Need One and What You Can Learn From Other’s Mistakes"
American Short Line & Regional Railroad Association’s 2010 Annual Convention

Speaker, “Pathology of Asbestos-Related Disease”
National Business Institute seminar, Asbestos: Current Issues and Effective Litigation Tac-tics

Speaker, “Beware of ERISA Lien Rights Or Your Settlement May Fail"
Winter Meeting of the National Association of Railroad Trial Counsel

Speaker, “Ethics: In Re Silica Product Liability Litigation MDL 1553"
National Business Institute seminar, Asbestos: Current Issues and Effective Litigation Tac-tics

Speaker, “Highlights of Missouri’s Tort Reform Law"
The Bar Association of Metropolitan St. Louis’ Bench and Bar Conference

Speaker, “An Overview of the Different Social Media Platforms"
Associated General Contractors of St. Louis Seminar, February 19, 2011

Panelist, “Intellectual Property, Ethics and Privacy Online"
St. Louis Bloggers Guild’s 2nd Annual Interactive Festival

Speaker, “Beware of ERISA Lien and Medicare Lien Issues That May Arise During Settlement"
CLE Presentation for Client

Speaker, “The Computer Sits Second Chair, How Supportive is Litigation Support Software"
Winter Meeting of the National Association of Railroad Trial Counsel

PAUL E. PETRUSKA

Speaker, “Courtroom Presentation Strategies: Communicating Your Story to the Jury"
The Missouri Bar

Speaker, “The Use and Misuse of Computerized Exhibits"
Special Litigation Conference, National Association of Railroad Trial Counsel

PUBLICATIONS

Articles & Books

The Manufacturer's Preview of the American Jobs Plan
The Illinois Manufacturer, July 2021

What restaurant owners should know about the second round of PPP funding
Feast Magazine, January 8, 2021

Asbestos Take-Home Cases: Liability Depends on State Law
American Bar Association Journal, Mass Torts

Newsletters

The American Rescue Plan: Restaurants Finally Get Their Relief Fund
March 12, 2021

What Landlords Should Know About the December 2020 COVID-19 Rent Relief Act
February 5, 2021

What Small Businesses Should Know About Round 2 PPP Funding
December 23, 2020

JUDGE HEATHER R. CUNNINGHAM BIOGRAPHY

Heather R. Cunningham was appointed Associate Circuit Judge on March 6, 2020 and Circuit Judge on January 28, 2022 by Governor Parson. Prior to her appointment, Judge Cunningham previously served as a Family Court Commissioner-Juvenile Division.

Judge Cunningham graduated from Bradley University with a degree in political science and a minor in history. She received her law degree from St. Louis University.

Before her appointment to the bench, Judge Cunningham worked for Cordell& Cordell P.C., and served as Attorney for the Juvenile Officer in the 20th Circuit and the 21st Circuit. She was an Adjunct Professor at St. Louis Community College-Meramec.

Judge Cunningham serves as Co-Chair of the Court's Diversity and Inclusion Committee, member of the Commissioners and Administrators Review and Application Committee. She was recently appointed a member of the Commission on Racial and Ethnic Fairness and appointed a member of the Juvenile Justice System Subcommittee.

Judge Cunningham is a member of the Missouri Bar, St. Louis County Bar, Women Lawyer's Association of St. Louis, and Bar Association of Metropolitan St. Louis.

Judge Cunningham lives with her husband and children in St. Louis County.

ASSOCIATE CIRCUIT JUDGE JEFFREY MEDLER BIOGRAPHY

Appointed associate circuit court judge in October 2020. A St. Louisan residing his entire life in St. Louis County. He graduated from St. Louis University Law School. Founding partner of his law firm in 1998.

Practiced in many areas of law over his 20+ years in private practice. In 2004, named Outstanding Young Lawyer of the Year by the St. Louis County Bar Association. Sat on several charity boards before joining the bench.

ASSOCIATE CIRCUIT JUDGE LORNE J. BAKER BIOGRAPHY

Lorne J. Baker was appointed associate circuit judge by Governor Michael L. Parson in 2018. Prior to his appointment, he most recently served as an administrative law judge for the Missouri Division of Workers' Compensation, to which he was appointed by Governor Jeremiah "Jay" Nixon in 2016.

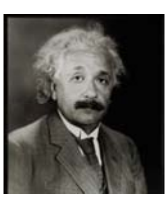
Judge Baker received his Bachelor of Arts from the University of Michigan in Ann Arbor, Michigan in 1990 and his law degree from the University of Missouri-Columbia in 1993.

Prior to his judicial appointments, Judge Baker practiced law in the private and public sectors for more than 20 years.

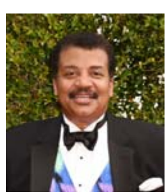
WHEN THE OCDC SPEAKS – LAWYERS SHOULD LISTEN

Paul E. Petruska
Greensfelder, Hemker & Gale, P.C.
March 24, 2022

Why Me?



AM I?



AM I?

AM I?

Why Me?

- I am a regular attorney
- My career has raised interesting ethics issues
- I think I put together interesting presentations
- No bigger challenge that creating an interesting ethics presentation

No Ethics Rules

Unnamed Attorney –

"Paul, there is no such thing as ethical rules for attorneys, there are just the rules of professional conduct"

GREENSFELDER

No Business For Paul

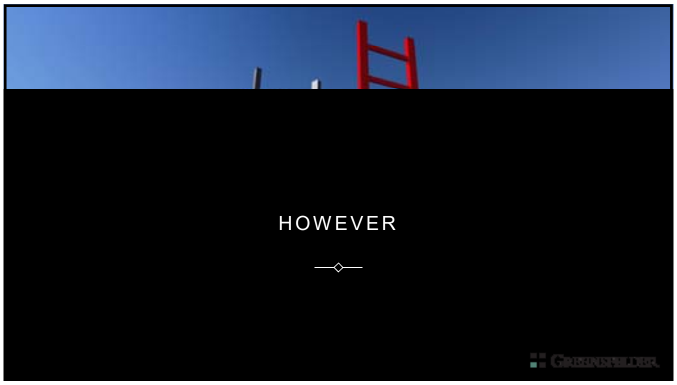
- 2004 – I was a very busy railroad defense lawyer, with 10% other cases to keep things interesting
- 2008 – No more railroad cases
- Why – 2005 venue law change
- 2005 Bench and Bar panel

GREENSFELDER

AVP Chief Trial Attorney

My last job with an insurance company had a great title

GREENSFELDER


HOWEVER


CEO

My Last Job – AVP Chief Trail Attorney

- Paid by Insurance Company
- I represent Insureds
- What Duty Do I Owe and To Who

Every Day Raised Interesting Issues

- Understanding adjusters
- Non-understanding adjusters
- It was my job to protect the real client (the insured), yet make my employer happy
- Some days were easier than others

Ethical Issues

- What about the person who said there are no ethical rules?
- Re-read the Preamble
- Lawyers can be an advisor, advocate, negotiator…
- Lawyers play a vital role in the preservation of society…

Ethical Issues
Venue Change

Rule 4-6.4 – Law Reform Activities affecting client interest

Conflicts Rules?
4-1.7, 4-1.8, 4-1.9, 4-1.10

Ethical Issues
My Insurance Job

Almost all rules are implicated

Preamble paragraph 9

Pictures and Copyright

- Pictures on the internet are often protected by copyright
- I can't just download them, use them and claim ignorance
- Rule 4-8.4
- I bought a license for these photos

2021 Articles from the Office of Chief Disciplinary Counsel

Office of Chief Disciplinary Counsel > For Lawyers Print

OCDC Article Archive

Here is a list of articles published by the Office of Chief Disciplinary Counsel beginning in 2003 until present:

2021

- **Why You Should Not Represent Criminal Codefendants**
- **Self Audit - 2021 FINAL(from MOBAR JOURNAL)**
- **Ethical Considerations Amid a Pandemic-MOBAR**
- **Moving Between Private Practice and Government Service-MOBAR**

LAWYER TRUST ACCOUNTS: SELF AUDIT

AN OCDC CHECKLIST TO HELP LAWYERS REDUCE RISKS, MEET FIDUCIARY OBLIGATIONS, AND ASSURE COMPLIANCE WITH THE SUPREME COURT OF MISSOURI'S RULES OF PROFESSIONAL CONDUCT.

JULY 2021

1 SETTING UP IOLTA ACCOUNTS

- ☐ I have an IOLTA Trust Account at a financial institution deemed **eligible** by the Missouri Lawyer Trust Account Foundation and **approved** by the Missouri Supreme Court Advisory Committee. *Rule 4-1.145(a)(5); Rule 4-1.145(a)(2).*
- ☐ I have reported and updated my bank and account number on my **Annual Enrollment Statement** with the Supreme Court of Missouri. *Rule 4-1.15(h).*
- ☐ I don't have a trust account, but I am **exempt** because of a specific provision of Rule 1.15 (h); and, I have checked the appropriate box on my Annual Enrollment statement. *Rule 4-1.15(h).*
- ☐ My trust account is in a financial institution located in the **same state** as my law office. *Rule 4-1.15(h)(4).*

2

RECEIPTS & DEPOSITS

- ☐ **Receipts are deposited daily and intact** into my trust account. I make no "split deposits." *Rule 4-1.15(a)(4) and Comment 4.*
- ☐ I immediately **notify my clients** (or third parties) when I receive funds on their behalf. *Rule 4-1.15(d).*
- ☐ For every receipt into my trust account, **my simultaneous records** include:
  - Payor identity
  - Reason for payment and reason for holding funds
  - Receipt date
  - Receipt to payor
  - Deposit receipt (bank record)
  - Client identity
  - Copy of check

  Rule 4-1.15(a)(4) and Rule 4-1.15(d).
- ☐ **As soon as I receive** any of these funds, I deposit them into my trust account:
  - Court costs and client expenses
  - Settlement proceeds
  - Client or third-party funds
  - Advance fees and flat fees in excess of $2,000.

GREENSPOONMARDER

2

RECEIPTS & DEPOSITS, CONTINUED

- ☐ I do not withdraw fees until earned. *Rule 4-1.15(c) and Rule 4-1.15 Comments 5 & 6.*
- ☐ I withdraw fees as soon as they are earned, in accord with a regular and reasonable billing cycle, and in most circumstances, within one month. *Rule 4-1.15(a).*
- ☐ I may deposit limited funds in my trust account for the sole purpose of paying known bank service charges. I maintain accurate up-to-date records of the amounts held and expended for bank fees. But, I do not deposit or hold additional funds in my trust account as a protection buffer against overdrafts or for any other reason. *Rule 4-1.15(b) & Rule 4-1.15, Comment 6.*

GREENSPOONMARDER

3

DISBURSEMENTS

- ☐ For every **payment** from my trust account, my **simultaneous records** include:
  - Client identity
  - Payor identity
  - Payment date
  - Reason for payment - with client reference
  - Copy of check
  - Entries in account journal and account ledger
  - Related records
    - Settlement sheet
    - Correspondence to client regarding payment
    - Correspondence to payee regarding payment
- ☐ **I never take cash withdrawals** or allow checks for "Cash" or "Bearer." *Rule 4-1.15(a)(5).*
- ☐ **Before any disbursements** are made from my trust account, I confirm that:
  - I have reasonable cause to believe the funds deposited are both "collected" and **"good funds."** *Rule 4-1.15(a)(6) and Rule 1.15 Comment 5.*
  - I have allowed a **"reasonable time"** to pass for the deposited funds to be actually collected and "g funds." *Rule 4-1.15(a)(6). (Rule 4-1.15 Comment 5* indicates that **10 days** is normally reasonable.)
  - I have verified the balance in the trust account.
- ☐ I have a written agreement with my bank that **no charges** will be assessed against my trust account credit card transactions. *Rule 4-1.15.*

GREENSPOONMARDER

4 RECORDS

☐ **At any time, I have the following trust account records completed and up-to-date:**
- A **general journal** showing all deposits and withdrawals, identifying the date, source, and description of each item deposited as well as the date, payee, and purpose of each disbursement;
- A **ledger for each separate client** or beneficiary showing the source of all funds deposited, the names of all persons for whom the funds are or were held, the amount of such funds, the descriptions and amounts of charges or withdrawals, and the names of all payees;
- **Fee agreements,** engagement letters, retainer agreements;

GREENSFELDER

4 RECORDS, CONTINUED

- **Accountings** to clients or third persons showing the disbursement of funds to them or on their behalves;
- **Invoices** for legal fees and expenses rendered to clients;
- **Disbursement** records;
- The physical or electronic equivalents of all **checkbook registers, bank statements, records of deposit, pre-numbered canceled checks,** and **substitute checks** provided by a financial institution;
- Records of all **electronic transfers** to and from client trust accounts, including the name of the person authorizing transfer, the date of transfer, the name of the recipient, and confirmation from the financial institution of the trust account number from which money was withdrawn and the date and the time the transfer was completed;
- **Reconciliations** of the client trust accounts;
- **Portions of client files** that are reasonably related to client trust account transactions;
- **Credit card transaction records** with clients to the extent permitted by law and the payment card industry data security standard; and
- **Receipts** for cash received. *Rule 4-1.15(f) and Comments 11 & 19.*

☐ I maintain all trust accounting records described above (in paper or electronic form) for the latter of **six years** from the end of the representation or when the last related transaction occurs, **despite any agreement** I reach with my client to return or destroy the client file before six years. *Rule 4-1.15(f). Rule 1.22(d).*

☐ All **partners** in my firm understand that each may be **held responsible** for ensuring the availability and accuracy of these records. *Rule 4-1.15 Comment 12.*

GREENSFELDER

5 ROUTINE PRACTICES, CONTINUED

☐ I recognize that only a lawyer admitted to practice law in Missouri or a person under the direc supervision of the lawyer shall be an **authorized signatory** or authorize transfers from a clien account. *Rule 1.15(a)(3).*

☐ **I regularly review each client ledger** in my trust account to determine that no client's balan negative.

☐ **Upon request** by any payee, I promptly provide **a full accounting.** *Rule 4-1.15(d).*

☐ **If a dispute arises** as to rights to any funds I hold, **I promptly separate the disputed funds.** *Rule 4-1.15(e); Comment 7.*

☐ As to funds received or held that are related to disputed funds, I **promptly distribute undisp portions** to appropriate payees. *Rule 4-1.15(e). Comment 7.*

GREENSFELDER

5 ROUTINE PRACTICES, CONTINUED

- ☐ I recognize that only a lawyer admitted to practice law in Missouri or a person under the direct supervision of the lawyer shall be an **authorized signatory** or authorize transfers from a client trust account. *Rule 1.15(a)(3).*
- ☐ **I regularly review each client ledger** in my trust account to determine that no client's balance is negative.
- ☐ **Upon request** by any payee, I promptly provide **a full accounting.** *Rule 4-1.15(d).*
- ☐ **If a dispute arises** as to rights to any funds I hold, **I promptly separate the disputed funds.** *Rule 4-1.15(e); Comment 7.*
- ☐ As to funds received or held that are related to disputed funds, I **promptly distribute undisputed portions** to appropriate payees. *Rule 4-1.15(e). Comment 7.*

GREENSFELDER

6 PROHIBITED PRACTICES

- ☐ **I never use my client trust account to pay personal or professional expenses. I understand that such use of my trust account places my clients' funds at risk of seizure by my creditors.** *Rule 4-1.15.*
- ☐ Even if my client trust account goes unused for an extended period, I refrain from using it for any purpose other than for client or third-party funds as permitted in Rule 4-1.15. I understand that such use of my trust account could place my future clients' funds at risk of seizure by my creditors. *Rule 4-1.15.*
- ☐ I do not hold funds to coerce clients into any position. *Rule 4-1.15, Comment 7.*

GREENSFELDER

7 UNDERSTANDING RULES ABOUT FEES

- ☐ I understand that **I may not contract with clients to accept non-refundable fees** or declare certain fees to be earned upon receipt, because all fees are subject to review for reasonableness and all advance fees in excess of $2,000 must be held in a trust account until earned. *Formal Opinion 128, as amended.*
- ☐ I understand that even though an advance flat fee that will be promptly paid and which does not exceed $2,000 may be placed directly into the office operating account, **I will have to refund any unearned portion** if the attorney-client relationship is terminated. *Rule 4-1.15 Comment 20*

GREENSFELDER

8 SECURITY

- ☐ My trust account is **titled as a CLIENT TRUST ACCOUNT** or similar words. And, that denomination appears on my checks and deposit slips. *Rule 4-1.15(a).*
- ☐ To prevent mistakes, I keep my trust account checks, deposit slips, and records **physically and electronically secure and separate** from all other accounts and financial materials. *Rule 4-1.15(a).*

175

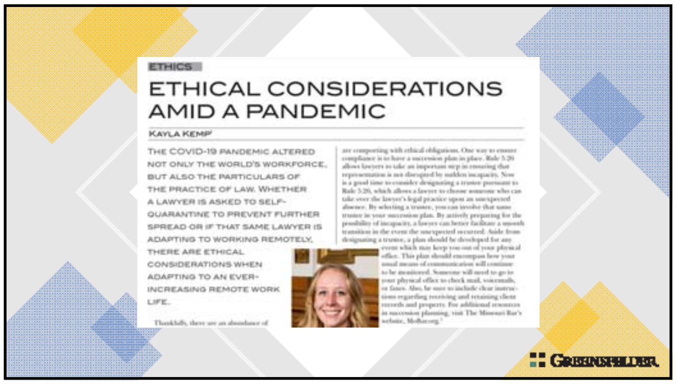
8 SECURITY, CONTINUED

- ☐ I maintain **written policies and procedures** for handling funds and maintain records for my trust and operating accounts. And, I have confirmed that my policies comply with the requirements of the most current versions of Rules 4-1.145, 4-1.15, and 4-1.155. *Rule 4-1.15, Comment 2. In re Farris, 472 S.W.3d 549 (Mo. banc 2015).*
- ☐ **I have trained my staff,** and retrained them this year, on firm policies and procedures for handling funds and maintaining financial records. *Rule 4-1.15, Comment 2 and Rule 4-5.3.*

- ☐ We annually contract with an external accounting professional to analyze my trust and operating account procedures and actual practices. *(Recommended to reduce the possibility or severity of mistakes and misuse by authorized and unauthorized actors.) Rule 4-1.15, Comment 2.*
- ☐ **I require dual control** before each trust account transaction may be completed.
- ☐ I use a different color for trust accounting checks and checkbook covers than for other accounts. *Recommended to prevent mistakes and reduce risk of internal fraud.*
- ☐ **We are extremely cautious and suspicious if unknown parties** (prospective clients) ask us to receive or briefly hold funds, especially when sent by cashier's check. We talk to our banker and risk manager before accepting any such arrangements.
- ☐ In recognition of my personal and professional accountability for protecting client and third-party funds, and regardless of whether I delegate certain tasks, **I undertake careful analysis of account history upon noticing any of the following warning signs in my operating or trust account:**

Why Highlight IOLTA – a bank account?

- 115 IOLTA cases in 2020
- 139 IOLTA cases in 2019
- 124 IOLTA cases in 2018
- 145 IOLTA cases in 2017
- 144 IOLTA cases in 2016



ETHICS

ETHICAL CONSIDERATIONS AMID A PANDEMIC

KAYLA KEMP[1]

THE COVID-19 PANDEMIC ALTERED NOT ONLY THE WORLD'S WORKFORCE, BUT ALSO THE PARTICULARS OF THE PRACTICE OF LAW. WHETHER A LAWYER IS ASKED TO SELF-QUARANTINE TO PREVENT FURTHER SPREAD OR IF THAT SAME LAWYER IS ADAPTING TO WORKING REMOTELY, THERE ARE ETHICAL CONSIDERATIONS WHEN ADAPTING TO AN EVER-INCREASING REMOTE WORK LIFE.

Thankfully, there are an abundance of

are comporting with ethical obligations. One way to ensure compliance is to have a succession plan in place. Rule 5.26 allows lawyers to take an important step in ensuring that representation is not disrupted by sudden incapacity. Now is a good time to consider designating a trustee pursuant to Rule 5.26, which allows a lawyer to choose someone who can take over the lawyer's legal practice upon an unexpected absence. By selecting a trustee, you can involve that same trustee in your succession plan. By actively preparing for the possibility of incapacity, a lawyer can better facilitate a smooth transition in the event the unexpected occurred. Aside from designating a trustee, a plan should be developed for any event which may keep you out of your physical office. This plan should encompass how your usual means of communication will continue to be monitored. Someone will need to go to your physical office to check mail, voicemails, or faxes. Also, be sure to include clear instructions regarding receiving and retaining client records and property. For additional resources in succession planning, visit The Missouri Bar's website, MoBar.org.[2]

Some Key Topics

- PLAN FOR INCAPACITATION
- WATCH MENTAL HEALTH
- NOTARY OPTIONS

Cyber Security Issues

- Zoom has had security breaches (June 2019, January 2020)
- Rule 4-1.6(c) – duty to prevent unauthorized disclosure or access to client info
- ABA formal opinion 477R provides guidance to secure communications over the internet
- 5,183 data breaches in 2019 (all companies) with 7.9 billion records exposed

What About Third-Party Services

- If "devices" are managed by third-parties, perhaps contractually obligate third-party to maintain security
- For Remote access, consider NIST and ISO standards for securing remote access
- Rule 4-5.3 – Lawyers must make reasonable assurances non-lawyer working with them comply with ethics rules

GREENSFELDER

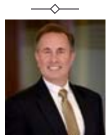
Paul Petruska
Of Counsel Attorney at Greensfelder, Hemker & Gale, P.C.

Questions?

https://www.linkedin.com/in/paulpetruska/

GREENSFELDER

How to Contact Us



Paul Petruska
618-239-3607
ppetruska@greensfelder.com

GREENSFELDER

THANK YOU

Legal Disclaimer: This document is not intended to give legal advice. It is comprised of general information. Readers facing specific issues should seek the assistance of an attorney.

GREENSFELDER

LAWYER TRUST ACCOUNTS: SELF AUDIT

AN OCDC CHECKLIST TO HELP LAWYERS REDUCE RISKS, MEET FIDUCIARY OBLIGATIONS, AND ASSURE COMPLIANCE WITH THE SUPREME COURT OF MISSOURI'S RULES OF PROFESSIONAL CONDUCT.

JULY 2021

1 SETTING UP IOLTA ACCOUNTS

☐ I have an IOLTA Trust Account at a financial institution deemed **eligible** by the Missouri Lawyer Trust Account Foundation and **approved** by the Missouri Supreme Court Advisory Committee. *Rule 4-1.145(a)(5); Rule 4-1.145(a)(2).*

☐ I have reported and updated my bank and account number on my **Annual Enrollment Statement** with the Supreme Court of Missouri. *Rule 4-1.15(h).*

☐ I don't have a trust account, but I am **exempt** because of a specific provision of Rule 1.15 (h); and, I have checked the appropriate box on my Annual Enrollment statement. *Rule 4-1.15(h).*

☐ My trust account is in a financial institution located in the **same state** as my law office. *Rule 4-1.15(h)(4).*

2 RECEIPTS & DEPOSITS

☐ **Receipts are deposited daily and intact** into my trust account. I make no "split deposits." *Rule 4-1.15(a)(4) and Comment 4.*

☐ I immediately **notify my clients** (or third parties) when I receive funds on their behalf. *Rule 4-1.15(d).*

☐ For every receipt into my trust account, **my simultaneous records** include:
•Payor identity
•Reason for payment and reason for holding funds
•Receipt date
•Receipt to payor
•Deposit receipt (bank record)
•Client identity
•Copy of check *Rule 4-1.15(a)(4) and Rule 4-1.15(d).*

☐ **As soon as I receive** any of these funds, I deposit them into my trust account:
•Court costs and client expenses
•Settlement proceeds
•Client or third-party funds
•Advance fees and flat fees in excess of $2,000.

2 RECEIPTS & DEPOSITS, CONTINUED

☐ I do not withdraw fees until earned. *Rule 4-1.15(c) and Rule 4-1.15 Comments 5 & 6.*

☐ I withdraw fees as soon as they are earned, in accord with a regular and reasonable billing cycle, and in most circumstances, within one month. *Rule 4-1.15(a).*

☐ I may deposit limited funds in my trust account for the sole purpose of paying known bank service charges. I maintain accurate up-to-date records of the amounts held and expended for bank fees. But, I do not deposit or hold additional funds in my trust account as a protection buffer against overdrafts or for any other reason. *Rule 4-1.15(b) & Rule 4-1.15, Comment 6.*

3 DISBURSEMENTS

☐ For every **payment** from my trust account, my **simultaneous records** include:
•Client identity
•Payor identity
•Payment date
•Reason for payment - with client reference
•Copy of check
•Entries in account journal and account ledger
•Related records
- Settlement sheet
- Correspondence to client regarding payment
- Correspondence to payee regarding payment

☐ **I never take cash withdrawals** or allow checks for "Cash" or "Bearer." *Rule 4-1.15(a)(5).*

☐ **Before any disbursements** are made from my trust account, I confirm that:
•I have reasonable cause to believe the funds deposited are both "collected" and **"good funds."** *Rule 4-1.15(a)(6) and Rule 1.15 Comment 5.*
•I have allowed a **"reasonable time"** to pass for the deposited funds to be actually collected and "good funds." *Rule 4-1.15(a)(6). (Rule 4-1.15 Comment 5* indicates that **10 days** is normally reasonable.)
•I have verified the balance in the trust account.

☐ I have a written agreement with my bank that **no charges** will be assessed against my trust account for credit card transactions. *Rule 4-1.15.*

4 RECORDS

☐ **At any time, I have the following trust account records completed and up-to-date:**
•A **general journal** showing all deposits and withdrawals, identifying the date, source, and description of each item deposited as well as the date, payee, and purpose of each disbursements;
•A **ledger for each separate client** or beneficiary showing the source of all funds deposited, the names of all persons for whom the funds are or were held, the amount of such funds, the descriptions and amounts of charges or withdrawals, and the names of all payees;
•**Fee agreements,** engagement letters, retainer agreements;

4 RECORDS, CONTINUED

•**Accountings** to clients or third persons showing the disbursement of funds to them or on their behalves;
•**Invoices** for legal fees and expenses rendered to clients;
•**Disbursement** records;
•The physical or electronic equivalents of all **checkbook registers, bank statements, records of deposit, pre-numbered canceled checks,** and **substitute checks** provided by a financial institution;
•Records of all **electronic transfers** to and from client trust accounts, including the name of the person authorizing transfer, the date of transfer, the name of the recipient, and confirmation from the financial institution of the trust account number from which money was withdrawn and the date and the time the transfer was completed;
•**Reconciliations** of the client trust accounts;
•**Portions of client files** that are reasonably related to client trust account transactions;
•**Credit card transaction records** with clients to the extent permitted by law and the payment card industry data security standard; and
•**Receipts** for cash received. *Rule 4-1.15(f) and Comments 11 & 19.*

☐ I maintain all trust accounting records described above (in paper or electronic form) for the latter of **six years** from the end of the representation or when the last related transaction occurs, **despite any agreement** I reach with my client to return or destroy the client file before six years. *Rule 4-1.15(f). Rule 1.22(d).*

☐ All **partners** in my firm understand that each may be **held responsible** for ensuring the availability and accuracy of these records. *Rule 4-1.15 Comment 12.*

5 ROUTINE PRACTICES

☐ **I regularly reconcile** my trust account by carefully comparing these records:
•Bank statements;
•Related checks and deposit slips;
•All transactions in my account journal;
•Transactions in each client's ledger; and
•Explanations of transactions noted in correspondence, settlement sheets, etc.
Rule 4-1.15(a)(7); Comment 18.

☐ In managing my trust account, I know that I may delegate tasks, but I recognize that **I cannot delegate responsibility.**

☐ If I delegate tasks, I've consulted with a risk manager or a CPA to learn steps to establish protections and dual controls. *Rule 4-1.15(a) (3) and Comment 2.*

☐ **I personally conduct frequent and regular reconciliations,** being the first person in my office to open bank statements.

☐ I understand that **I am deemed to know what accurate accountings** of my trust account would reflect. *In re Farris, 472 S.W.3d 549 (Mo. banc 2015).*

5 ROUTINE PRACTICES, CONTINUED

- ☐ I recognize that only a lawyer admitted to practice law in Missouri or a person under the direct supervision of the lawyer shall be an **authorized signatory** or authorize transfers from a client trust account. *Rule 1.15(a)(3).*
- ☐ **I regularly review each client ledger** in my trust account to determine that no client's balance is negative.
- ☐ **Upon request** by any payee, I promptly provide **a full accounting.** *Rule 4-1.15(d).*
- ☐ **If a dispute arises** as to rights to any funds I hold, **I promptly separate the disputed funds.** *Rule 4-1.15(e); Comment 7.*
- ☐ As to funds received or held that are related to disputed funds, I **promptly distribute undisputed portions** to appropriate payees. *Rule 4-1.15(e). Comment 7.*

6 PROHIBITED PRACTICES

- ☐ **I never use my client trust account to pay personal or professional expenses. I understand that such use of my trust account places my clients' funds at risk of seizure by my creditors.** *Rule 4-1.15.*
- ☐ Even if my client trust account goes unused for an extended period, I refrain from using it for any purpose other than for client or third-party funds as permitted in Rule 4-1.15. I understand that such use of my trust account could place my future clients' funds at risk of seizure by my creditors. *Rule 4-1.15.*
- ☐ I do not hold funds to coerce clients into any position. *Rule 4-1.15. Comment 7.*

7 UNDERSTANDING RULES ABOUT FEES

- ☐ I understand that **I may not contract with clients to accept non-refundable fees** or declare certain fees to be earned upon receipt, because all fees are subject to review for reasonableness and all advance fees in excess of $2,000 must be held in a trust account until earned. *Formal Opinion 128, as amended.*
- ☐ I understand that even though an advance flat fee that will be promptly paid and which does not exceed $2,000 may be placed directly into the office operating account, **I will have to refund any unearned portion** if the attorney-client relationship is terminated. *Rule 4-1.15 Comment 20*

8 SECURITY

- ☐ My trust account is **titled as a CLIENT TRUST ACCOUNT** or similar words. And, that denomination appears on my checks and deposit slips. *Rule 4-1.15(a).*
- ☐ To prevent mistakes, I keep my trust account checks, deposit slips, and records **physically and electronically secure and separate** from all other accounts and financial materials. *Rule 4-1.15(a).*

SECURITY, CONTINUED

- ☐ I maintain **written policies and procedures** for handling funds and maintain records for my trust and operating accounts. And, I have confirmed that my policies comply with the requirements of the most current versions of Rules 4-1.145, 4-1.15, and 4-1.155. *Rule 4-1.15, Comment 2. In re Farris, 472 S.W.3d 549 (Mo. banc 2015).*

- ☐ **I have trained my staff,** and retrained them this year, on firm policies and procedures for handling funds and maintaining financial records. *Rule 4-1.15, Comment 2 and Rule 4-5.3.*

- ☐ We annually contract with an external accounting professional to analyze my trust and operating account procedures and actual practices. *(Recommended to reduce the possibility or severity of mistakes and misuse by authorized and unauthorized actors.) Rule 4-1.15, Comment 2.*

- ☐ **I require dual control** before each trust account transaction may be completed.

- ☐ I use a different color for trust accounting checks and checkbook covers than for other accounts. *Recommended to prevent mistakes and reduce risk of internal fraud.*

- ☐ **We are extremely cautious and suspicious if unknown parties** (prospective clients) ask us to receive or briefly hold funds, especially when sent by cashier's check. We talk to our banker and risk manager before accepting any such arrangements.

- ☐ In recognition of my personal and professional accountability for protecting client and third-party funds, and regardless of whether I delegate certain tasks, **I undertake careful analysis of account history upon noticing any of the following warning signs in my operating or trust account:**

- Lack of monthly reconciliations of bank accounts;
- Unopened bank statements or unopened bills;
- Frequent trips to the bank;
- Complaints from vendors or third parties that they are not being timely paid or that they did not receive a check that had been issued;
- Past due law office bills such as phone or other utility bills;
- Operating account or personal account checks written to the trust account;
- Monthly checks for the same amount (such as a car or mortgage payment);
- Unusual urgency about resolving a case (settlement, closing, etc.);
- Signs of a lifestyle beyond the means of the lawyer or employee;
- Signs of depression or alcohol or drug abuse;
- Blank or incomplete check stubs or deposit slips;
- Missing checks;
- Accounts that do not balance;
- Checks returned for insufficient funds;
- Unidentified counter withdrawals or electronic transfers;
- Round-numbered checks:
- Checks clearing significantly out of sequence;
- Excessive voided checks;
- Checks made payable to an unfamiliar vendor;
- Excessive checks to a particular vendor;
- Possessiveness, secretiveness, or defensiveness of the lawyer or employee responsible for bookkeeping

(The list in this paragraph was provided by The Office of Disciplinary Counsel to the Supreme Court of South Carolina and The Professional Responsibility Committee of the South Carolina Bar.)
Rule 4-1.15, Comment 2. In re Farris, 472 S.W.3d 549 (Mo. banc 2015).

9

FIRM ACKNOWLEDGEMENTS

- ☐ **I recently read Rules 4-1.145, 4-1.15, and 4-1.155.** If I had questions or concerns about my ethical obligations under those rules, I sought advice from the Legal Ethics Counsel, *mo-legal-ethics.org,* 573-638-2263. If I had questions or concerns about establishing an account or working with a financial institution, I sought advice from the Administrator of the Missouri Lawyer Trust Account Foundation, *moiolta.org.*

- ☐ **I recently reviewed Rule 4-1.155** to help me **determine whether particular deposits should be held in an IOLTA account,** or instead, be placed in a dedicated trust account for the benefit of a client (because, e.g., the amount of funds deposited is large and/or will be held for an extended period).

- ☐ I understand that my license to practice law in Missouri establishes my **irrefutable consent for my bank to report any overdrafts** in my trust account to the Office of Chief Disciplinary Counsel. *Rule 4-1.15(a)(2). Rule 4-1.15-Advisory Committee Regulation.*

- ☐ I understand that the **OCDC will investigate any trust account overdraft** and **I will be expected to produce records** required by Rule 4-1.15. *Rule 4-8.1.*

- ☐ I have recently reviewed the regulations related to FDIC coverage of funds held in trust accounts. *fdic.gov.*

- ☐ I recognize that I may not hold client funds to coerce clients into any position. *Rule 4-1.15: Comment 7.*

- ☐ I reviewed *Rule 4-1.15 and Comment 8* for guidance when my client and a third-party dispute disposition of funds held by me.

- ☐ I understand that money held for clients and third parties, including fees paid in advance, belongs to them and not me.

ETHICAL CONSIDERATIONS AMID A PANDEMIC

Kayla Kemp[1]

The COVID-19 pandemic altered not only the world's workforce, but also the particulars of the practice of law. Whether a lawyer is asked to self-quarantine to prevent further spread or if that same lawyer is adapting to working remotely, there are ethical considerations when adapting to an ever-increasing remote work life.

Thankfully, there are an abundance of resources and technological solutions which can be utilized to facilitate practicing during a pandemic. As lawyers, we must be mindful to ensure that as we adapt, we must continue to meet our ethical duties under the Missouri Rules of Professional Conduct ("Rules").

Kayla Kemp

Planning for Incapacitation During a Pandemic

Lawyers should be prepared to adapt to a rapidly changing environment, whether that be a natural disaster, pandemic, or some other act of God. Not only do we need to be prepared for abrupt changes to the ways in which we meet with clients or appear before courts, but we also need to be prepared for incapacity, more so now than ever before. Like the general population, our profession's population is increasingly aging. According to the 2020 American Bar Association Profile of the Legal Profession, the median age of lawyers as of 2019 was 47.5 years old[2]. Nearly one in six lawyers are 65 or older.[3] This is notable because the Center for Disease Control (CDC) warns the risk for severe illness with COVID-19 increases with age. Those who are 50-64 years of age are four times more likely to be hospitalized than the comparison group, which consisted of those 18-29 years old. The risk of death was 30 times higher for those 50-64 years old compared to the comparison group.[4] Those figures increase with each following age group. Nonetheless, every lawyer must consider the possibility of becoming incapacitated with little to no notice.

Lawyers should ensure that, in the event of incapacity, they are comporting with ethical obligations. One way to ensure compliance is to have a succession plan in place. Rule 5.26 allows lawyers to take an important step in ensuring that representation is not disrupted by sudden incapacity. Now is a good time to consider designating a trustee pursuant to Rule 5.26, which allows a lawyer to choose someone who can take over the lawyer's legal practice upon an unexpected absence. By selecting a trustee, you can involve that same trustee in your succession plan. By actively preparing for the possibility of incapacity, a lawyer can better facilitate a smooth transition in the event the unexpected occurred. Aside from designating a trustee, a plan should be developed for any event which may keep you out of your physical office. This plan should encompass how your usual means of communication will continue to be monitored. Someone will need to go to your physical office to check mail, voicemails, or faxes. Also, be sure to include clear instructions regarding receiving and retaining client records and property. For additional resources in succession planning, visit The Missouri Bar's website, MoBar.org.[5]

Mental Health Concerns

The physical threat COVID-19 presents is not the only health risk. On Feb. 19, 2020, the American Lawyer released the results of its year-long "Mental Health and Substance Abuse Survey," which found that 31.2% of the more than 3,800 respondents surveyed reported they were depressed. Additionally, 64% reported anxiety, 10.1% reported an alcohol problem, and 2.8% reported a drug problem.[6] These findings predate the onset of the pandemic in the United States.

The CDC released findings noting that in June of 2020 the rates of depression and anxiety amongst adults in the United States were three to four times higher than the corresponding point in 2019.[7] Approximately 40% of those surveyed reported struggling with mental health or substance abuse. According to the same study, rates of suicidal ideation, substance abuse, and alcohol consumption are steadily rising. Lawyers should familiarize themselves with the mental health and substance use resources available through The Missouri Bar[8]. Depression and anxiety can result in lawyers neglecting their responsibilities and, therefore, harming their clients. Just as lawyers ought to be proactive in planning for physical incapacitation, lawyers should also be proactive in caring for their mental well-being. A lawyer who is grappling with these serious health issues needs to make every effort to seek help, such as through the Missouri Lawyers' Assistance Program (MOLAP).[9] Through MOLAP, all Missouri Bar members can speak with a licensed clinical social worker by calling 800-688-7859. The program is free and confidential.

Competence Amidst Chaos

The first obligation set forth in the Rules is that of competence. Rule 4-1.1 – Competence – Comment [6] dictates "[t]o 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. . . ."

Keeping abreast of changes to the practice of law necessities brings an awareness of the risks associated with working remotely. Despite the challenges presented during the current pandemic, lawyers have the duty to remain competent. Comment [3] to Rule 4-1.1 provides guidance on a lawyer's ethical obligation during such a situation as a global pandemic:

> In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances, for ill-considered action under emergency conditions can jeopardize the client's interest.

In the event of an emergency, a lawyer may give advice in a matter the lawyer does not possess the skill ordinarily needed to provide such advice. Of course, advising without the necessary skill is only acceptable where referral or consultation with another lawyer is impractical.

Lawyers must continue to educate themselves on technological innovations which can be utilized to virtually serve their clients. Also, lawyers need to stay current on any legal changes that allow them to continue to meet clients' needs to enter into contracts, update wills, or create personal health care directives.

Remote Notarization

On April 6, 2020, Gov. Mike Parson issued Executive Order 20-08 suspending a statutory requirement that a notary public must conduct such notarization of official documents while the signer personally appears. Executive Order 20-08 was set to expire June 15, 2020; then, Executive Order 20-12 extended remote notarization to Aug. 28, 2020. Subsequently, Executive Order 20-14 and Executive Order 20-19 extended remote notarizations until March 31, 2021.

The practice of remote notarization provides a secure and safe method to execute legal documents. Notarization can occur while utilizing audio-video technology, provided certain conditions are met:

(1) If the signatory is not personally or otherwise known to the notary, the signatory must display a valid photo ID to the notary during the video conference;

(2) The signatory must affirmatively represent that they are physically situated in the State of Missouri, and the notary must be physically located in the State of Missouri and say in which county they are physically located for the jurisdiction on the notarial certificate;

(3) The video conference must be a live and interactive audio-visual communication between the signatory, notary, and any other necessary persons to allow for direct interaction at the time of signing;

(4)The notary must record in their journal the exact time and software used to perform the notarial act, along with all other required information; and

(5) The document must contain a notarial certificate, a jurat, or acknowledgement, which states that the signatory appeared remotely pursuant to Executive Order 20-14.

Electronic Notarization

While Missouri already permits electronic notarization, which is the use of electronic signatures and seals, Executive Order 20-14 allows for remote and electronic notarization to occur together when:

(1) The notary public is registered as an electronic notary public with the Missouri Secretary of State;

(2) The document must be electronically signed with a software approved by the Missouri Secretary of State; and

(3) The notary must affix the electronic notary seal to the electronic document.

Lawyers should do their due diligence and check with the Missouri Secretary of State to confirm they are using a registered remote notary[10] and the software used to electronically sign the document[11] is approved.

Cyber Security

While there are many benefits to utilizing technology to facilitate legal services, there are also risks. For example, Zoom – a platform used to facilitate virtual audio and visual meetings – has had security breaches. In July 2019, a vulnerability in Zoom's Macintosh desktop client was found which let malicious websites turn on a Macintosh user's webcam without that user's knowledge.[12] Then, in January 2020, another vulnerability was discovered. Unauthorized users could enter Zoom meetings that were not password protected and did not have Zoom's Waiting Room feature – which allows for manual admission into Zoom meetings – enabled. Security flaws such as these are not unique to Zoom. Consequently, when utilizing third-party platforms, lawyers ought to take precautions such as using updated software and taking reasonable security measures.

Rule 4-1.6(c) specifies "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information of the client." Comment [15] details the factors to be considered in determining whether a lawyer acted completely by undertaking reasonable efforts to prevent inadvertent or unauthorized disclosure of information related to client representation. The ABA's Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R, "Securing Communication of Protected Client Information," which provides guidance as to security measures that should be employed given the ever-increasing cybersecurity threats that exist when transmitting information over the internet: [13]

> However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications.[14]

While cyber security was a matter of grave concern in 2017, the threat of harm has only increased.[15] In 2019, there were more than 5,000 data breaches reported.[16] These breaches amounted to approximately 8 billion exposed records. Educating yourself on the various types of cyberattacks which can leave your client-confidential information vulnerable is the first step.[17]

Third-party Service Providers

For those lawyers whose devices are managed by a third party, include explicit terms in your contracts detailing which security practices are to be followed. These security features can include audits that report security status and the health of your devices. The National Institute for Standards and Technology and the Institute for Standards Organization provide best practices for guidance on how to strengthen your network's defenses. Lawyers should consider including clauses in their contracts which detail how third parties will secure remote access. Methods to help secure remote access to your network include VPNs, multi-factor authentication, and rotating strong passwords. After all, Comment [1] to Rule 4-5.3 – Responsibilities Regarding Nonlawyer Assistants requires lawyers with managerial authority make reasonable assurances that the nonlawyers in the firm and those who work outside the firm act in a way compatible with the ethical obligations of the lawyer.

As technology evolves, so does our obligation to act reasonably under the Rules of Professional Conduct. And as we adapt, we must consider what further efforts we can take to meet our ethical duties. The current global pandemic has shifted our way of life, both at work and at home. It is important for every lawyer to understand the resources available to help alleviate the burden they may feel.

Endnotes

1 Kayla Kemp is staff counsel at the Office of Chief Disciplinary Counsel. Special thanks to Melinda J. Bentley, legal ethics counsel, whose presentation, "Ethical Considerations for Missouri Lawyers Practicing During the COVID-19 Pandemic: A Conversation with the Chief Disciplinary Counsel & Ethics Counsel," was invaluable.

2 Am. Bar Ass'n, 2020 American Bar Association Profile of the Legal Profession (2020), https://www.americanbar.org/news/reporter_resources/profile-of-profession/.

3 Am. Bar Ass'n, 2020 American Bar Association Profile of the Legal Profession (2020), https://www.americanbar.org/news/reporter_resources/profile-of-profession/.

4 Centers for Disease Control and Prevention, COVID-19: Older Adults (2020), https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/older-adults.html.

5 The Missouri Bar, Planning Ahead: A Guide to Protect Your Clients' and You Survivors' Interests in the Event of Your Disability of Death (2005).

6 Lizzy McLellan, *Lawyers Reveal True Depth of Mental Health Struggles*, Law.com (Feb. 19, 2020, 11:00 AM), https://www.law.com/2020/02/19/lawyers-reveal-true-depth-of-the-mental-health-struggles/.

7 Czeisler MÉ et al., *Mental Health, Substance Use, and Suicidal Ideation During the COVID-19 Pandemic – United States, June 24–30, 2020,* MMWR Morb. Mortal Wkly. Rep. 2020;69:1049-1057 (2020).

8 Coronavirus Resource Center for Lawyers, https://mobar.org/site/content/Lawyer-Resources/Coronavirus_Resource_Center_for_Lawyers.aspx?WebsiteKey=dd54fe1d-87c8-4d7e-9547-e59fcd729541 (last visited Jan. 11, 2021).

9 Missouri Lawyers' Assistance Program, https://mobar.org/molap/ (last visited Jan. 11, 2021).

10 Registered Electronic Notaries, https://www.sos.mo.gov/RegisteredElectronicNotary (last visited Jan. 11, 2021).

11 Approved Notary Software Vendors, https://s1.sos.mo.gov/Business/Notary/softwarevendors (last visited Jan. 11, 2021).

12 Jonathan Leitschuh, *Zoom Zero Day: 4+ Million Webcams & Maybe an RCE? Just Get Them to Your Website!*, Medium.com (July 8, 2019), https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5.

13 ABA Committee on Ethics & Pro. Resp., Formal Op. 477R (2017).

14 *Id.* at pg. 5.

15 Microsoft Digital Defense Report, September 2020, https://www.microsoft.com/en-us/security/business/security-intelligence-report (last visited Jan. 11, 2021).

16 Rae Hodge, *2019 Data Breach Hall of Shame,* cnet.com (Dec. 27, 2019, 4:00 AM), https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/.

17 *See* Melinda J. Bentley, *Ethics: The Ethical Implications of Technology in Your Law Practice: Understanding the Rules of Professional Conduct Can Prevent Potential Problems,* 76 J.MoBar (2020).

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477 **May 11, 2017**

Securing Communication of Protected Client Information

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for e-mail communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."[1]

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.[2]

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.[3]

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c)

---

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).

2. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

3. *See* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

and a new Comment to Rule 1.6, addressing a lawyer's obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when," and not "if."[4] Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.[5]

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the "technology amendments" made to the Model Rules in 2012, identify some of the technology risks lawyers' face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[6] The scope of this requirement was clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[7]

---

4. "Cybersecurity" is defined as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack." CYBERSECURITY, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/cybersecurity (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

5. Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI's Cyber Division, indicated that "[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm's computer system is a really optimal way to obtain economic and personal security information." Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.

6. A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

7. *Id.* at 43.

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] specifies that, to remain competent, lawyers need to "keep abreast of changes in the law and its practice." The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document. [8]

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[9] The 2012 modification added a new duty in paragraph (c) 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."[10]

Amended Comment [18] explains:

> 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.

---

8. ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

9. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

10. *Id.* at (c).

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.[11]

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

> . . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.[12]

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- 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).[13]

11. The 20/20 Commission's report emphasized that lawyers are not the guarantors of data safety. It wrote: "[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances."

12. ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2013). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures.[14] Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. <u>Understand the Nature of the Threat</u>.

Understanding the nature of the threat includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.[15] "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

---

14. See item 3 below.

15. *See, e.g.*, Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries*, TREND-MICRO (Jan. 25, 2016), http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As comment [18] makes clear, what is deemed to be "reasonable" may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions.

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, "delete" usually does not mean information is permanently deleted, and "deleted" data may be subject to recovery. Therefore, a lawyer should consider whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it,[16] and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client's lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party.[17] If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived, and the lawyer must determine whether it is prudent to warn a client of the dangers associated with such a method of communication.[18]

---

16. *See* Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

17. *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) (discussing the duty to protect the confidentiality of e-mail communications with one's client); Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer's email server).

18. some state bar ethics opinions have explored the circumstances under which e-mail communications should be afforded special security protections, *See, e.g.*, Tex. Prof'l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer…;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as "privileged and confidential" in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or "disclaimer" to client emails, where such a disclaimer is accurate and appropriate for the communication.[19]

Model Rule 4.4(b) obligates a lawyer who "knows or reasonably should know" that he has received an inadvertently sent "document or electronically stored information relating to the representation of the lawyer's client" to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer's duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Model Rule 5.1 provides that a partner in a law firm, 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 all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being

---

- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

19. *See* Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read "this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed" with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make "reasonable efforts to ensure that" the nonlawyer's "conduct is compatible with the professional obligations of the lawyer."

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer's obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer's due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor's security policies and protocols;
- vendor's hiring practices;
- the use of confidentiality agreements;
- vendor's conflicts check system to screen for adversity; and
- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.[20]

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including "using an Internet-based service to store client information." Comment [3] provides that the "reasonable efforts" required by Model Rule 5.3 to ensure that the nonlawyer's services are provided in a manner that is compatible with the lawyer's professional obligations "will depend upon the circumstances." Comment [3] contains suggested factors that might be taken into account:

- 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.

20. MODEL RULES OF PROF'L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

> Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers 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."[21] If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.[22]
>
> Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer's actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.[23] The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [18] to Model Rule 1.6, "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."

---

21. The ABA's catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

22. By contrast, where a 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." MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [4] (2017). The concept of monitoring recognizes that although it may not be possible to "directly supervise" a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf.

23. MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) & (4) (2016).

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

THE ETHICAL IMPLICATIONS OF TECHNOLOGY IN YOUR LAW PRACTICE:

UNDERSTANDING THE RULES OF PROFESSIONAL CONDUCT CAN PREVENT POTENTIAL PROBLEMS

MELINDA BENTLEY[1]

IMPLEMENTING AND USING TECHNOLOGY DEVICES AND SYSTEMS IN YOUR LAW PRACTICE CAN BE BOTH EXCITING AND DAUNTING. HOW DO YOU SELECT A DEVICE SUCH AS A PHONE, LAPTOP, COMPUTER, OR OTHER HARDWARE? HOW DO YOU SELECT A PIECE OF SOFTWARE, CASE MANAGEMENT SYSTEM, DOCUMENT MANAGEMENT SYSTEM, BACKUP SYSTEM, OR ACCOUNTING SYSTEM?

Melinda Bentley

How do you become competent in making those selections and using those technologies? What if there is a loss of a device or data? How do you train your staff? While the Rules of Professional Conduct (Rules) cannot tell you what to buy, fortunately, they do give you clear standards, and further guidance is provided through the Comments to the Rules to assist you with implementing and using technology devices and systems in your practice.[2] Further, by having a keen understanding of the Rules and Comments, you, as a lawyer, can be proactive in both preventing potential problems and being able to respond efficiently and ethically if a difficulty, large or small, occurs.

Key Ethics Rules: Building A Framework of Understanding

Three key ethics obligations are at the forefront of establishing a lawyer's understanding in order to prevent potential technology problems: competence, confidentiality, and responsibilities regarding nonlawyer assistants.

Rule 4-1.1 – Competence

The first key ethics obligation underlying a lawyer's use of technology is found in Rule 4-1.1, which states that "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Further, Comment [6] provides that "[t]o 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.)*

Rule 4-1.6 – Confidentiality of Information

The second key ethics obligation underlying a lawyer's use of technology is found in Rule 4-1.6(a), which generally prohibits a lawyer from revealing information relating to the representation of a client unless an exception is met. In 2017, the Supreme Court of Missouri adopted an additional requirement for lawyers in Rule 4-1.6(c) 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 the client." Such disclosure or access to confidential client information not only applies to physical information, such as paper documents in a client file, but also to electronically stored information. Think of the large amount of confidential client information lawyers have electronically. That electronic confidential client information makes lawyers' duty of technology competence under Rule 4-1.1 that much more critical.

Reasonable Efforts on Unauthorized Access and Inadvertent or Unauthorized Disclosure. What constitutes reasonable efforts by a lawyer to safeguard confidential client information to prevent inadvertent or unauthorized disclosure, or unauthorized access? Comment [15] provides guidance to Rule 4-1.6(c) that lawyers are required to act competently regarding safeguarding this information. First, Comment [15] specifically creates three categories of safeguarding information from: (1) unauthorized access by third parties; (2) inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client; (3) and/or inadvertent or unauthorized disclosure by those who are subject to the lawyer's supervision. When describing these categories, Comment [15] references Rules 4-1.1 (Competence), 4-5.1 (Responsibilities of Partners, Managers, and Supervisory Lawyers), and 4-5.3 (Responsibilities Regarding Nonlawyer Assistants).

Second, Comment [15] provides factors to consider in determining the reasonableness of the lawyer's efforts, including but 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).

Comment [15] notes that there is no violation of Rule 4-1.6(c) "if the lawyer has made reasonable efforts to prevent the access or disclosure."[3]

Additionally, Comment [15] provides guidance that the client may require the lawyer to implement special security measures that are not required by Rule 4-1.6, but it also notes that a client may give informed consent to forgo otherwise required security measures under Rule 4-1.6. "Informed consent," as defined in Rule 4-1.0(e), requires communication of "adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct." Per Rule 4-1.0(e), guided by Comment [6], informed consent in this context means discussing the material advantages and disadvantages of forgoing security measures, discussing available options and alternatives, and possibly advising the client to seek other counsel on this decision. Factors as to reasonableness will depend on the experience of the client or if the client is independently represented by counsel.[4]

Further, Comment [15] references that it is beyond the scope of the Rules to determine if state or federal data privacy laws require additional safeguards over client confidential information, or notification in the event of a loss of electronic information or unauthorized access to such information.

Finally, Comment [15] advises lawyers to consult Rule 4-5.3 (Responsibilities Regarding Nonlawyer Assistants) and its Comments [3] and [4] regarding supervision of nonlawyer assistants outside the firm.

Reasonable Precautions in Transmission. Comment [16] to Rule 4-1.6 notes that a "lawyer must take reasonable precautions to prevent ... information [relating to the representation of a client] from coming into the hands of unintended recipients." In offering guidance on this responsibility, Comment [16] provides two factors to consider when determining if the lawyer can have a reasonable expectation of confidentiality: first, the "sensitivity of the information," and second, "the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."

Comment [16] provides that no special security measures are required "if the method of communication affords a reasonable expectation of privacy."[5] Just as with the considerations previously discussed in Comment [15], Comment [16] provides guidance that the client may require the lawyer to implement special security measures that are not required by Rule 4-1.6, but it also notes that a client may give informed consent to forgo otherwise required security measures under Rule 4-1.6. Further, a lawyer may be required to take additional steps to comply with other law, but that is an issue beyond the scope of the Rules.

Rule 4-5.3 – Responsibilities Regarding Nonlawyer Assistants

The third key ethics obligation underling a lawyer's use of technology is found in Rule 4-5.3, which applies to a lawyer's responsibilities for the conduct of nonlawyers who are "retained by or associated with a lawyer." Rule 4-5.3(a) sets the requirements for firm-wide measures to ensure that partners or lawyers with comparable managerial authority make reasonable efforts to make sure the firm has measures in place to give reasonable assurance that the nonlawyer assistant's conduct is compatible with the professional obligations of the lawyer. Similarly, Rule 4-5.3(b) requires a lawyer with direct supervisory responsibility to make reasonable efforts to make sure the nonlawyer assistant's conduct is compatible with the professional obligations of the lawyer. Per Rule 4-5.3(c), lawyers are responsible for the conduct of nonlawyer assistants who they employ, retain, or associate with if the conduct of the nonlawyer assistant would be a violation of the Rules of Professional Conduct if engaged in by the lawyer and if one of two scenarios is present:

> (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.

Comment [2] to Rule 4-5.3 provides guidance on supervising the conduct of nonlawyer assistants employed by a lawyer, including but not limited to administrative assistants, investigators, law student interns, and paralegals. It describes making sure such assistants receive "appropriate instruction and supervision concerning the ethical aspects of their employment," particularly on preserving confidentiality.[6] Ways to ensure appropriate instruction include written policies and protocols, as well as regular instruction on the Rules of Professional Conduct and relevant substantive areas of law in which the nonlawyer is providing assistance. Further, specific protocols should be implemented within the law firm to ensure appropriate supervision of the work product of the nonlawyer.

Comment [3] to Rule 4-5.3 provides guidance on using nonlawyer assistants outside the firm who assist the lawyer in rendering legal services to a client, including but not limited to retaining investigative or paraprofessional services, hiring a document management company, sending client documents to a third party for printing or scanning, and using a service based on the internet to store client information. Lawyers using these services still must make reasonable efforts to ensure that the services are provided in a manner compatible with the lawyer's professional obligations, and the extent of those efforts will depend on the circumstances.[7]

Applying the Rules to Potential Technology Issues

The Growing Need for Technology Competence

As provided for in Rule 4-1.1 and its Comment [6], lawyers do have an ethical obligation to be competent in technology, including its risks and its benefits, in a lawyer's practice. For example, a lawyer in Oklahoma was publicly censured in 2016 based on a reciprocal discipline from the United States Bankruptcy Court for the Western District of Oklahoma where the lawyer was suspended for failure to file documents in a manner that was compatible with applicable rules.[8] The lawyer failed to report his discipline in the Bankruptcy Court to the Oklahoma Bar Association and also failed to timely notify his clients of his suspension.[9] During the hearing before the trial panel of the Oklahoma Bar Association's Professional Responsibility Tribunal, the lawyer "acknowledged his problems with the bankruptcy court were caused by his lack of expertise in computer skills and his frustration trying to meet the federal court's expectations with electronic pleading requirements." The trial panel reported that the lawyer's problems were not with his knowledge of substantive bankruptcy law, but instead "technological proficiency."[10] The Supreme Court of Oklahoma, in issuing its public censure of the lawyer, encouraged him to "continue to improve his computer skills, or better, to hire an adept administrative assistant to do his pleadings."[11]

While hiring adept support staff is helpful in some circumstances when properly supervised per Rule 4-5.3, it is not a substitute for a lawyer's own technology competency as required by Rule 4-1.1. What are some ways to gain technology competency skills? The answers will be different for each lawyer depending on the lawyer's practice setting and level of technological savvy. One of the best ways to gain the requisite skill and knowledge about the risks and benefits of relevant technology for a law practice is by taking continuing legal education programs related to technology.[12] While Missouri does not require that lawyers receive specific minimum continuing legal education (MCLE) credits related to technology competence, it does offer MCLE accreditation of a number of technology programs that help lawyers gain and maintain professional competence as it relates to the practice of law, professional responsibility, or law office management.[13]

There are several resources readily available to help lawyers build their technology competence, including articles, publications, blogs, podcasts, and more. When it comes to these resources, lawyers should be sure to check that they are receiving information from reputable sources that are appropriate for their practice settings.[14] Malpractice insurance providers may also have resources or standards for insureds.

Additionally, lawyers should read the terms and conditions of service carefully for each new hardware or software item they consider incorporating into their practices to ensure the item has appropriate safeguards for maintaining client confidential information.[15] Further, lawyers should consider consulting an information technology (IT) professional for assistance.[16]

Email and Other Electronic Communications

If lawyers are using email to communicate with clients, they must take reasonable precautions to prevent the unintended interception of confidential client information and should only use email upon proper consideration of Rule 4-1.6 and Comments [15]-[16].[17] While email may be appropriate in some circumstances, other circumstances where the lawyer is transmitting highly sensitive information may require special security measures to comply with Rule 4-1.6.[18] Special security measures may include using email encryption software, placing password protection on attachments, or using "a well vetted and secure third-party cloud based file storage system to exchange documents."[19] Remember that Rule 4-1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." In looking to the factors discussed in Comment [15] to Rule 4-1.6 as to reasonable efforts to prevent access or disclosure, consider having a conversation with the client at the outset of the representation to determine if email is an appropriate means of communication. Some points to consider are:

- How do the lawyer and the client want to use email to communicate?
- What information will the lawyer and client be exchanging by email?
- What are the terms and conditions of the platforms that host both the lawyer's email and the client's email? Are the platforms ensuring privacy or are they mining emails for personal information?
- How is the client going to be accessing the email?[20] On a personal or work phone or computer? Who else has access to that device or the email account?

Consider these points, as well as the sensitivity of the information being transmitted, to determine if additional security measures are necessary or if email should even be used.[21] By asking some of these questions, it should help the lawyer determine if he or she is acting reasonably in using email as a form of communication.

Other forms of electronic communication may include online client portals that have communication features or by texting. Similar questions about confidentiality and appropriateness of the medium should be asked for each of these other potential forms of electronic communication.

Also, lawyers should be mindful that if they are using one of these forms of electronic communication with clients, the correspondence needs to be retained for the client files in accordance with Rule 4-1.22 (Retaining Client Files) and Advisory Committee of the Supreme Court of Missouri Formal Opinions 115 (no withholding of property belonging to the client to enforce payment of fees or expenses) and 127 (scanning client files).[22]

Data Backups, Case and Document Management Systems, and Electronic File Retention

When considering how to backup data, a lawyer should consider the nature of the information to be backed up. Most of it will likely be confidential client information, but it may include items such as trust account records, business records, and much more. Whether a lawyer is considering online (i.e., cloud) and/or on-site backups, those backups pertaining to confidential client information are governed by Rule 4-1.6 and guided by Comments [15] and [16].[23]

Guidance is provided to lawyers regarding cloud backups in Missouri Informal Advisory Opinion 2018-09. It describes how lawyers need to maintain competence in using relevant technology per Rule 4-1.1, safeguard confidential client information per Rule 4-1.6(c), and supervise per Rule 4-5.3.[24] It also cautions lawyers to read the terms and conditions of service carefully to determine ownership and security of client information and the level of access the attorney and provider will have to that client information. It goes on to describe what constitutes reasonable efforts to safeguard confidential client information while using cloud computing, including but not limited to:

- Security measures protecting confidentiality of client information during transmission and storage;
- Prompt notification of attorney in the event of a security breach or provider's receipt of a subpoena for client information;
- Ownership of data solely by attorney or attorney's firm;
- No access rights by the provider to client information, except as required by law;
- Regular data backup by the provider;
- Handling of client information in the event attorney's relationship with the provider is terminated;
- Compliance with applicable law regarding data storage and transmission;
- Reliable access to data by attorney;
- No access to data by third parties, including advertisers, except as required by law; and
- Domestic storage of data or, alternatively, storage in a jurisdiction subject to United States data protection laws or equivalent.[25]

It also provides guidance that lawyers should review the provider policies and practices periodically, as these can change.[26]

For on-site backups, lawyers should consider such things as the physical security of the equipment storing the confidential information, level of encryption, and redundancy (the same data being stored in multiple ways in case one system fails). Lawyers should consult with an IT professional to assist in properly setting up and maintaining this system.

Many case or document management systems are now provided by vendors as cloud-based services, though some are still provided for on-site network usage. When selecting a case or document management system, lawyers should consider similar factors as just discussed for cloud or on-site back-ups.

When backing up client information, lawyers should be mindful that they are required to securely store client files for six or 10 years after the completion or termination of the representation absent having an agreement with the client based on informed consent confirmed in writing.[27] The six-year client file retention applies to client files where the representation was completed or terminated on or after July 1, 2016, and the 10-year requirement applies where the representation was completed or terminated prior to July 1, 2016.[28] "Client files, except for items of intrinsic value, may be maintained by electronic, photographic, or other media provided that printed copies can be produced. These records shall be readily accessible to the lawyer."[29] Advisory Committee of the Supreme Court of Missouri Formal Opinion 127 permits the destruction of paper files (except for items of intrinsic value) prior to the expiration of the required retention period if the files are maintained electronically for the required period in accordance with the Rules of Professional Conduct.[30]

Keeping Client Confidential Information Secure on Phones, Laptops, Tablets, Etc.

Just as lawyers have an obligation to secure physical files of clients from unauthorized access, the same is true of electronic files lawyers maintain on portable electronic devices such as phones, laptops, tablets, and other similar devices.[31] Whether the devices are those of the firm, or lawyers and employees are permitted to bring their own devices and use them for firm business, reasonable measures may include some of the following suggestions:

- Take reasonable steps to ensure confidentiality by, at a minimum, having strong passwords to access these devices.[32]
- Passwords should be changed periodically.[33]

CONTINUED ON PAGE 47

- Consider additional safeguards such as encrypting the data on these devices, using multifactor-factor authentication to access firm systems.[34]
- Avoid public Wi-Fi and only choose secure Wi-Fi, as well as consider using a virtual private network (VPN).[35]
- For lost or stolen devices, have a way to remotely disable the devices and destroy the data contained on those devices.[36]
- Implement firewalls, keep updated anti-malware, anti-spyware, and anti-virus protections on all devices where confidential client information is stored or transmitted.[37]
- Apply all security patches and updates for software and devices.[38]

These suggestions are some starting points for what constitutes reasonable measures to secure client confidential information and are not intended to be an exclusive list. As previously suggested, lawyers should be sure to consider the type of client confidential information and applicable state and federal laws. The prudent lawyer will consider consulting with an IT professional, the lawyer's malpractice insurance carrier, and other appropriate resources for additional guidance.

Metadata

Another source of client confidential information lawyers should be mindful of securing is metadata, meaning electronically embedded data.[39] Informal Advisory Opinion 2014-02 asks in the litigation context if a lawyer "has an ethical obligation to make good faith efforts to prevent the inadvertent electronic transmission of embedded metadata to opposing party or counsel?" Citing Rule 4-1.6, guidance is provided that the lawyer must use reasonable care to ensure that no confidential client information related to the representation is revealed without the client's consent, including confidential information that is contained in embedded metadata.[40] It provides that this may require scrubbing documents of metadata before transmitting them.[41] However, the Informal Advisory Opinion goes on to note:

> Efforts to protect confidential information must be exercised in light of Attorney's obligation pursuant to Rule 4-3.4(a) not to unlawfully obstruct another party's access to evidence or unlawfully alter, destroy, or conceal evidence. Removing metadata with evidentiary value before transmitting certain documents may constitute a violation of laws governing discovery and therefore violate Rule 4-3.4(a). This informal opinion does not render an opinion about the existence of discoverable evidence in particular metadata or about the effect on substantive legal privileges of the pre-transmission removal or lack of removal of metadata.[42]

Responding to a Loss of Client Confidential Information Due to a Lost Device or File, Data Breach, or Cyberattack

Lawyers are custodians of highly sensitive information and can be prime targets for hackers.[43] Missouri Informal Advisory Opinion 2017-02 discusses a lawyer's ethical duties when a nonlawyer assistant has disclosed client confidential information to third parties, but the ethics analysis as it relates to disclosing this breach to the client will be similar in the event of a lost device or file, data breach, or cyberattack. It advises that lawyers have an obligation under Rule 4-1.4 (Communication) to disclose the confidentiality breach to the affected client and explain the matter to the extent necessary for the client to make an informed decision about the representation. That disclosure also needs to occur in the event of a lost device or file where client confidential information is disclosed, whether lost by the lawyer or a nonlawyer assistant employed or retained either inside or outside the law firm, as the lawyer is responsible for that conduct under Rule 4-5.3. A similar communication is also necessary in the event of a data breach or cyberattack where confidential client information is disclosed.[44]

Rule 4-1.6(c), requiring reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation, also notes in Comments [15] and [16] that state and federal data privacy laws may govern or impose notification requirements upon a loss of electronic information or unauthorized access, so lawyers should be mindful of these laws both in how they choose to safeguard confidential client information and handle a loss of such information.

Working with IT Professionals and Vendors Outside the Law Firm

While lawyers may be aware of the obligations to train and supervise nonlawyer assistants within the firm, Rule 4-5.3, Comment [3] reminds lawyers that these same obligations apply regarding nonlawyer assistants employed or retained outside the firm. These include outside IT professionals lawyers may hire to help support their firms and vendors who provide services based on the internet to store client information such as data backup provides, case or document management programs, or other similarly based services used within the firm. Lawyers have the obligation to make reasonable efforts to ensure that the services are provided in a manner compatible with their professional obligations under the Rules.

Reasonable efforts will vary depending on 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."[45] Directions should be communicated to the nonlawyer in a manner appropriate under the circumstances so as to give reasonable assurance that the conduct of the nonlawyer is compatible with the professional obligations of the lawyer.[46] Missouri Informal Advisory Opinions 20070008 and 20050068 both suggest confidentiality agreements should be used when working with nonlawyer vendors and service providers outside the firm. Such agreements are also advisable when working with outside IT professionals, as well as direct training, as appropriate, on confidentiality and other applicable professional obligations of lawyers to ensure the IT professionals' conduct is compatible with the conduct of lawyers.

Be Aware of Scams

Lawyers are frequently the targets of potential scams, as lawyers may hold trust account funds for clients as well as sensitive confidential client information. These potential scams often start as emails from those purporting to be legitimate sources, such as potential clients, known clients, financial institutions, businesses, government entities, etc., but are actually phishing attempts to gain access to funds and/or personal information of lawyers or clients. Additionally, emails containing links or attachments from known or unknown senders may contain viruses, malware, spyware, ransomware, or other mechanisms to corrupt computer systems and/or gain access to sensitive information. Lawyers must be savvy to these potential scams and train themselves and their nonlawyer assistants to prevent these breaches.

Trust account scams are some of the most common attacks against lawyers. Lawyers who believe they may have clients who have provided fraudulent checks in an effort to obtain good funds from lawyers' trust accounts wonder how to ethically proceed. Guidance has been provided in Informal Advisory Opinion 2018-06, which addresses such a potential scam scenario in which a lawyer's purported prospective client sent the lawyer a bogus check for deposit into the trust account. That Informal Advisory Opinion discusses whether the lawyer may report this purported prospective client to law enforcement. Whether a lawyer-client relationship exists is a question of law and fact that is outside the scope of the Rules of Professional Conduct, but if the lawyer had a prospective client relationship under Rule 4-1.18, the lawyer would not be able to use or disclose information gained in the consultation except as would be permitted under Rule 4-1.9 as though this person were a former client.[47] If no lawyer-client relationship existed, and this person was not a prospective client, the lawyer would not have a duty of confidentiality and would be free to make a report to law enforcement authorities.[48]

Conclusion

As a lawyer, you should work to gain and maintain competence in technology, engage in reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of clients, and exercise appropriate professional responsibilities over the conduct of nonlawyer assistants both inside and outside the law firm. Focusing on these key ethics rules will assist you in selecting technology devices and systems in your firm, and help prevent breaches of client confidential information. If you have questions about the Rules of Professional Conduct regarding incorporating technology into your law practice, you are encouraged to contact the Legal Ethics Counsel office (www.MO-Legal-Ethics.org) to seek an informal advisory opinion about your prospective conduct.

Endnotes

1 Melinda J. Bentley is Legal Ethics Counsel for the Advisory Committee of the Supreme Court of Missouri.

2 *See* Rule 4, Scope [14].

3 Rule 4-1.0(h) defines "reasonable" or "reasonably" to be "conduct of a reasonably prudent and competent lawyer."

4 *See* Rule 4-1.0, Comment [6].

5 *See infra* discussion of email.

6 *See also* Mo. Informal Advisory Opinions 2018-04 and 2017-02 (interpreting Rule 4-5.3 as it applies to nonlawyer assistants within a law firm). Informal Advisory Opinions are published on The Missouri Bar's website at: http://www.mobar.org/ethics/informalopinions.htm.

7 See Mo. Informal Advisory Opinion 2018-09 (interpreting Rule 4-5.3 as it applies to use of a cloud computing vendor outside the firm).

8 *State of Oklahoma ex rel., Oklahoma Bar Ass'n v. Oliver*, 2016 OK 37, 369 P.3d 1074 (2016).

9 *Id.* at ¶15, 369 P.3d at 1077.

10 *Id.* at ¶5, 369 P.3d at 1075.

11 *Id.* ¶15, 369 P.3d at 1077.

12 *See* Mo. Informal Advisory Opinion 2018-09 (providing guidance on technology competence through continuing legal education courses).

13 *See* Rule 15.04(b): "A program or activity may be an accredited program or activity if it directly contributes to the professional competency of lawyers or judges and has significant intellectual or practical content related to the development or practice of law, professional responsibility, or law office management." *See also* Rules Related to The Fla. Bar, Ch. 6, R. 6-10.03(b) (requiring Florida lawyers to take at least three of 33 MCLE credit hours every three years in approved technology programs), and 27 N.C.A.C. Ch. 1D – § .1518(a)(2) (requiring North Carolina lawyers to take at least one hour annually of MCLE devoted to technology training.)

14 *See* Mo. Informal Advisory Opinion 2018-09.

15 *See Id.* and Rule 4-1.6, discussion *supra; see also* Legal Ethics Counsel Resource Page – Electronic Comunication Resources, http://molegalethics.org/electronic-communication-resources/.

16 See *Id.* and Rules 4-1.6 and 4-5.3, discussion *supra.*

17 *See* Mo. Informal Advisory Opinion 2012-01 (providing guidance on use of email).

18 *Id.*

19 ABA Comm'n on Ethics & Prof'l Responsibility, Formal Opinion 477R (revised May 22, 2017).

20 *See* Mo. Informal Advisory Opinion 990007 (providing guidance on use of email, including consideration of settings of sender and receiver).

21 *See* Rule 4-1.6, Comment [15].

22 Mo. Sup. Ct. Advisory Committee Formal Opinions are published on the website of the Supreme Court of Missouri at: http://www.courts.mo.gov/page.jsp?id=11696.

23 *See supra* discussion of Rule 4-1.6.

24 *See supra* discussions of Rules 4-1.1, 4-1.6, and 4-5.3.

25 Mo. Informal Advisory Opinion 2018-09.

26 *Id.*

27 *See* Rule 4-1.22.

28 *Id.*

29 *Id.*

30 *See also* Legal Ethics Counsel Resource Page, File Retention Resources, http://molegalethics.org/file-retention-resources/.

31 *See* Mo. Informal Advisory Opinion 980030 (providing guidance on preventing physical client file access in an office-sharing arrangement) and Rule 4-1.6(c).

32 ABA Comm'n on Ethics & Prof'l Responsibility, Formal Opinion 477R (2017) (revised May 22, 2017).

33 *Id.*

34 *Id.*

35 *Id. See also* Jill D. Rhodes & Robert S. Litt, The ABA Cybersecurity Handbook 35 (2d ed. 2018) ("Wireless communication creates opportunities for hackers to intercept sensitive data such as passwords for logging in to corporate networks and online banking sites. Public Wi-Fi locations such as airports, hotels, and coffee shops – convenient places to check email – often do not have security features necessary to protect confidential client data.").

36 ABA Formal Opinion 477R, *supra* note 32.

37 *Id.*

38 *Id. See also* Rhodes & Litt, *supra* note 35, 21-22 (2d ed. 2018), (describing cyber-attacks against law firms due to outdated software that had not been updated).

39 See Rule 4-4.4, Comment [2] (describing metadata as a form of electronically stored information).

40 Mo. Informal Advisory Opinion 2014-02.

41 *Id.*

42 *Id.*

43 *See* ABA Comm'n on Ethics & Prof'l Responsibility, Formal Opinion 483 (2018).

44 *Id.*

45 Rule 4-5.3, Comment [3].

46 *Id.*

47 Mo. Informal Advisory Opinion 2018-06.

48 *Id.*


The Missouri Bar
Jobs for Lawyers
★Free ★New Opportunities Weekly★
Full or part-time employment
Post a job opening
Contract opportunities
Office space/office sharing
FIND A JOB

Periodical


A TRADITION OF SUCCESS
Matthew E. Birch
Scott E. Nutter
Lynn R. Johnson
Victor A. Bergman
David R. Morantz
SHAMBERG
JOHNSON
AND BERGMAN
816-474-0004
www.sjblaw.com
2600 Grand Boulevard
Suite 550
Kansas City, MO 64108
S J & B
OUR EXPERIENCE PAYS
We have a long history of success inside and outside the courtroom. For over 40 years, we have maximized the value of cases referred to our firm and we will continue to do so into the future. If you have a client with a serious injury or death, we will welcome a referral or opportunity to form a co-counsel relationship.
The choice of a lawyer is an important decision and should not be based solely on advertisements.

JOURNAL OF THE

MISSOURI BAR

VOLUME 76
NUMBER 2

MARCH-APRIL
2020

THE VERDICT ON THE BUSINESS JUDGMENT RULE

PG. 64

THE NCAA AND ATHLETE PAY

PG.68

MoBar.org


Let’s
Talk
Litigation.
The Simon Law Firm, P.C.
Attorneys and Counselors at Law
Your trusted litigation partner.
(314) 241-2929 | www.simonlawpc.com
*The choice of a lawyer is an important decision and should not be based solely on advertisements.

The St. Louis County Bar Association
Requests the Honor of Your Presence

at its

Annual Dinner

Saturday, the Seventh of May, Two Thousand and Twenty-Two
Crystal Ballroom - Clayton Plaza Hotel
Clayton, Missouri

Eric Michael Tuncil
2022 President
and Master of Ceremonies

Brianna J. Baldwin
Roy F. Essen Outstanding Young Lawyer
Award Recipient

Thomas B. Weaver
Dudley C. Dunlop Distinguished Service
Award Recipient

Black Tie Optional
Cocktails 6:30 p.m.
Dinner 8:00 p.m.

$125 Per Person
$80 For Judges
Complimentary for Benefactors, Sustaining Members
and SLCBA Past Presidents
Includes Dinner and Open Bar Until 9:30 p.m.