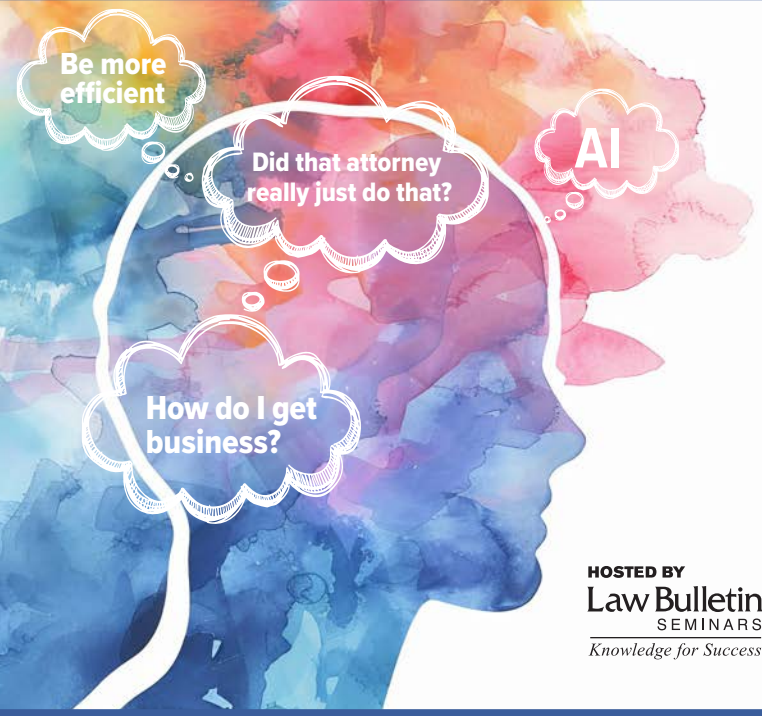


HOSTED BY
Law Bulletin SEMINARS
Knowledge for Success

EARN UP TO 6 PMCLE

ETHICS 2026

LIVESTREAM AND ON-DEMAND

WED. MAY 13

PM Program: 1:30PM - 5:00PM (3 hours)

AARON W. BROOKS
Chief Information Security Officer, *Illinois ARDC*

RICHARD C. GLEASON
Litigation Group Manager, *Illinois ARDC*

HON. JEFFREY A. GOFFINET
Associate Judge, *1st Judicial Circuit Court*

KATHRYNE "KATIE" R. HAYES
Partner, *Collins Bargione & Vuckovich*

DANIEL F. KONICEK
Partner, *Konicek & Dillon, P.C.*

JULIA ROUNDTREE LIVINGSTON
Diversity, Equity & Inclusion Manager, *Illinois Supreme Court Commission on Professionalism*

MATTHEW J. O'HARA
Partner, *Smith Gambrell Russell LLP*

THANK YOU

2Civility Illinois Supreme Court Commission on Professionalism
ARDC Attorney Registration & Disciplinary Commission
BUILDEN A DECADE OF LAW FIRM MARKETING
Burke, Warren, MacKay & Serritella, P.C.
Collins Bargione & Vuckovich
Konicek & Dillon
Lawyerport
Lawyers' Assistance Program
Smith Gambrell Russell

Lawyerport

KNOWLEDGE YOU NEED. ADVANTAGES YOU WANT.

Lawyerport integrates the flagship products of Law Bulletin Media into a single, trusted solution.

STAY INFORMED

Browse today's top news, search extensive archives and link to thousands of profiles for a deeper understanding

Chicago Daily Law Bulletin
CHICAGO LAWYER

GAIN AN ADVANTAGE FOR YOUR CLIENT

Leverage unique search tools and proprietary data to evaluate, research, build and win your case

JVR JURY VERDICT REPORTER

KNOW YOUR LEGAL COMMUNITY

Access the most comprehensive directory of the Illinois legal community

SULLIVAN'S LAW DIRECTORY

SULLIVAN'S JUDICIAL PROFILES

FIND CRITICAL COURT INFORMATION

See your upcoming court calls, review the entire Cook County court docket and expand your due diligence for tracking when parties have been involved in litigation

Court Calls
Court Docket

Lawyerport Will Evolve Your Practice. See How.

CALL 312.644.3744 or **EMAIL** LPsales@lawyerport.com

Law Bulletin
SEMINARS
Knowledge for Success

Welcome to the Law Bulletin Seminars Ethics 2026 Conference. The morning program provides 3 Illinois PMCLE credits, including the required wellness credit, and a separate afternoon program also provides 3 Illinois PMCLE credits, including diversity. We are honored that you have chosen our conference to meet your professionalism requirements.

Our afternoon program will explore two trending AI topics and the negative impacts of bullying in the legal profession. The afternoon sessions will begin with an engaging session on bullying and how to prevent it. The next two panels will examine our obligations to our clients and the courts when we use AI tools in our practice to produce our work. Our speakers include ARDC leaders and professional responsibility experts who will provide practical guidance to use in your practice while avoiding ethical pitfalls.

We wish to extend a special thanks to the Illinois ARDC, the Illinois Supreme Court Commission on Professionalism, the Lawyers' Assistance Program and our exceptional faculty. We also are thankful for the support of Burke, Warren, MacKay & Serritella, P.C., Collins Bargione & Vuckovich, Konicek & Dillon PC, Smith Gambrell Russell LLP, and Builden Partners.

We hope you enjoy this event and encourage you to attend some of our other Law Bulletin Seminars events throughout the year. Visit our website LawBulletinSeminars.com to learn how you can earn your MCLE credits in a dynamic and professional environment.

If you should have any questions, comments or suggestions, please contact us. Law Bulletin Media has been serving the Chicago legal community for over 170 years, and your comments have helped improve our products and services over the years. We will continue to solicit and act on your advice.

Thank you again for attending,

Peter Mierzwa
President
Law Bulletin Media

TABLE OF CONTENTS

PM PROGRAM - Topics

PAGE

5 **PANEL 4 — 1:30 - 2:30pm**

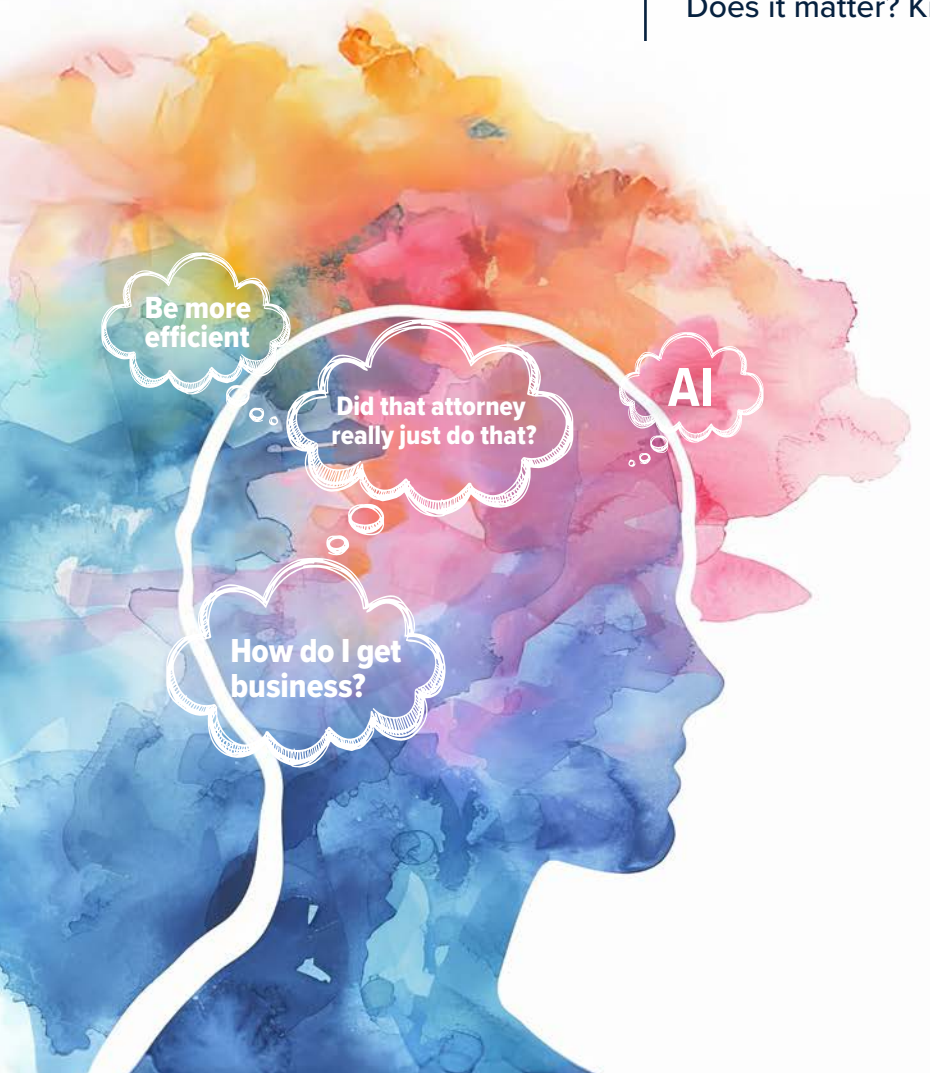
Preventing bullying in the legal profession: An ethical case for courage and change (DEI)

29 **PANEL 5 — 2:40 - 3:40pm**

You, your client and AI usage: When and what type of client notice and consent is needed?

134 **PANEL 6 — 3:55 - 4:55pm**

Whose work is it when you use AI or other tech? Does it matter? Know your duties under the rules



PANEL 4 — 1:30 - 2:30pm

Preventing bullying in the legal profession: An ethical case for courage and change (DEI)

Panelists: **Julia Roundtree Livingston,** Diversity, Equity & Inclusion Manager, *Illinois Supreme Court Commission on Professionalism*

Julia Roundtree Livingston, Diversity, Equity & Inclusion Manager,
Illinois Supreme Court Commission on Professionalism

Julia is the Diversity, Equity, and Inclusion (DEI) Manager at the Illinois Supreme Court Commission on Professionalism where she leads the Commission's education and advocacy initiatives aimed at promoting DEI in Illinois' legal and justice systems. She joined the Commission in 2023.

Prior to joining the Commission, Julia was Executive Director of Macon County Court Appointed Special Advocates (CASA), which provides court-appointed volunteers to advocate for abused, neglected, and/or dependent children who are involved in the Macon County juvenile court system. She was appointed to this role in 2018 after serving as CASA's Director of Development.

At CASA, Julia led a sustainable nonprofit organization with multiple streams of funding while educating the community on the need for CASA's services. This included working with local lawyers and judges to organize trainings for CASA volunteers, regularly communicating with legal and judicial professionals about CASA's capabilities, and presentations to the Decatur Bar Association on CASA's work.

Julia grew the organization's impact by increasing the number of community volunteers who became advocates as well as the number of children that CASA serves. In 2021, Julia led Macon County CASA in expanding its services into a second county, DeWitt County.

Julia was also a member of the Illinois CASA Equity Task Force, the Illinois CASA/Children Advocacy Centers Task Force, and the CWEC (Child Welfare Advisory Committee) on Racial Equity led by the Illinois Department of Children & Family Services.

Before joining CASA, Julia was the Director of Development at Baby TALK, an educational non-profit in Decatur, Illinois, and an English professor at Southern Illinois University Carbondale, the University of Illinois Urbana-Champaign, Florida State University, and Richland Community College.

Livingston continued

Julia received an ABD (all but dissertation) in African American Literature and U.S. Literature Since 1865 from Florida State University and a master's and bachelor's degree from Southern Illinois University Carbondale, where she was a 4-year letter winner in cross country and indoor/outdoor track.

She is a member of the Diversity & Education Leadership Team at the Maroa-Forsyth School District and founder of Discourse on Racial Difference: A Macon County Book Club, which has 600 members statewide.

In December 2023, Julia was named chair of the Untold Stories Committee, a Macon County community engagement program led by the Heart of Illinois Community Foundation which is charged with promoting a fuller understanding of history as a contribution to conversations about racial equity and social justice

Julia lives with her husband and three children in Forsyth, Illinois. As a family, they enjoy board games, watching sports, playing basketball and soccer, and traveling.

2Civility
Illinois Supreme Court Commission on Professionalism

Bullying in the Legal Profession: Confronting a Culture of Intimidation

Learning Objectives

1) Describe the prevalence of bullying in the legal profession.
2) Understand the impact of bullying on lawyers' health and careers.
3) Identify specific strategies that lawyers and legal organizations can employ to address and prevent bullying in the legal profession.

Key Resources

- Stephanie A. Scharf & Roberta D. Liebenberg, Bullying in the Legal Profession: A Study of Illinois Lawyers' Experiences and Recommendations for Change, Illinois Supreme Court Commission on Professionalism (2024)
  - ☐ Executive Summary
- Illinois Supreme Court Commission on Professionalism Releases Multifaceted Study on Bullying in the Illinois Legal Profession and Recommendations for Prevention (Press Release, Oct. 1, 2024)
- Illinois Supreme Court Commission on Professionalism Launches Bullying Prevention Challenge for Lawyers and Bar Associations (Press Release, June 10, 2025)

Outline

1) **Overview of Commission's Study on Bullying in the Legal Profession**

   a. ***Qualitative and Quantitative Components***
      - Statewide survey of lawyers actively practicing law in Illinois; 6,010 lawyers completed the survey
      - 10 focus groups with a range of participants as defined by race and ethnicity, gender identity, sexual orientation, age and experience, disability, type of employment, and location of employment
      - Due to survey's large sample size and Illinois' geographic and demographic diversity, the Report's findings are instructive for lawyers and legal organizations nationally

   b. ***Definition of bullying***: Survey defined bullying as "inappropriate behavior intended to intimidate, humiliate, or control the actions of another person, including verbal, nonverbal, or physical acts

2) **Study's Key Findings**

   a. 1 in 4 Illinois lawyers experienced some form of bullying during the one-year period encompassed by the survey
   b. ***Disproportionate impact of bullying on certain groups of lawyers***

- Gender: 38% of female lawyers were bullied at work in the past year, compared to 15% of male lawyers

- Disability: 38% of lawyers with a disability were bullied in the past year, compared to 23% of lawyers without a disability

- Race and ethnicity: In the past year …
  - 36% of Middle Eastern/North African lawyers were bullied
  - 35% of Black/African American lawyers were bullied
  - 34% of Hispanic lawyers were bullied
  - 32% of multiracial lawyers were bullied
  - 28% of Asian American lawyers were bullied
  - 23% of white lawyers were bullied

- Age
  - 39% of lawyers aged 25 to 35 were bullied in the past year; lawyers in this age group were more likely than others to report that they had been bullied
  - The likelihood of being bullied decreases for each increasingly older group of lawyers
  - 12% of lawyers aged 66 to 75 were bullied in the past year

- Sexual orientation
  - 29% of gay or lesbian lawyers were bullied in the past year as compared to 25% of heterosexual lawyers
  - 29% of lawyers who are gay, lesbian, or bisexual were the target of verbal bullying related to their sexual orientation, while 3% of heterosexual lawyers were verbally bullied related to their sexual orientation

c. ***Most reported types of bullying behavior:***

- Verbal intimidation, such as insults, name-calling, or shouting
- Harsh, belittling, or excessive criticism of work
- Demeaning nonverbal behaviors
- Imposing unrealistic work demands
- Behind-the-back malicious rumors
- Improperly taking credit for work
- Not receiving important work information

  ❖ *Lawyers also reported being asked to do something unethical or improper, cyberbullying, physical intimidation (throwing objects,*

invading space, and stalking), and physical contact (inappropriate touching, pushing, or shoving).

d. ***Who perpetrated the bullying in the most recent event reported***
- A lawyer who worked in a different firm/company (e.g., opposing counsel) (33%); a lawyer in the same firm/company in a more senior or very high-level position (31%); a judge (14%); a client (7%)

e. ***Impact on lawyers' mental health, productivity, careers***
- 54% of those bullied experienced a negative change in emotional well-being (such as anxiety, loss of self-confidence, and other negative feelings and reactions)
- 39% of those bullied felt less productive at work
- 20% of those bullied experienced a decline in physical health
- 18% of lawyers said they had left a job practicing law because of bullying

- "At my current job, the partner that I report to appears incapable of acknowledging his role in creating the toxic workplace problems that exist. On a daily basis, this leads to increased staff stress, anxiety, and uncertainty... Staff is ignored, badgered, lied to regularly, and blamed for mistakes caused by the partner."
- **"Bullying compounds itself**. After being bullied, you begin to worry. Then, you have trouble sleeping. You come to work but you aren't working at your full capacity."
- **"Bullying is a great silencer**."
- "I am on anti-anxiety medication and manage a tremendous amount of stress that is tied most directly to the negativity that seems so much more personal in litigation."
- "The worst part is that it made me second guess myself."
- "Bullying affects job performance because it can make you question your judgment."

f. ***Lawyers' Responses to Being Bullied***
- Almost half of lawyers who were bullied (47%) ignored the bullying and many others walked away (16%). Direct responses by those who were bullied included verbally defending themselves (43%), attempting to defuse the situation (31%), getting upset or angry (19%), and/or telling the bully to stop (12%). A small number (1%) responded by bullying in return, with a handful physically defending themselves (less than 1%).

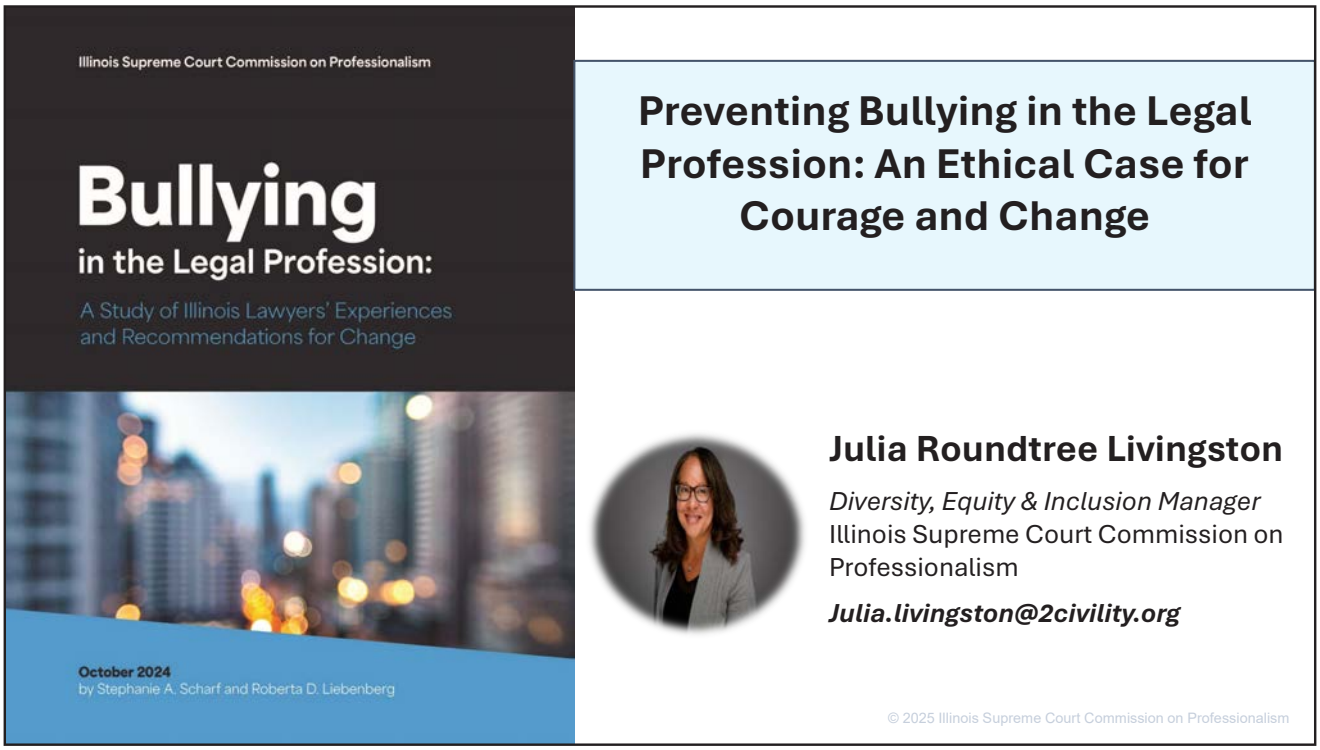
g. ***Reporting of Bullying***
- Only 20% of lawyers who were bullied in their workplace reported it to a supervisor, upper-level attorney, or human resources manager.

- Bullying is underreported in legal organizations due to not wanting to be perceived as weak or a "complainer" (34%), fear of the bully's status (27%), the belief that the employer would not do anything (27%), and concerns regarding loss of work or job (16%).

3) **Report's Key Recommendations**
   a. Legal workplaces should develop, implement, and enforce anti-bullying policies.
   b. Legal workplaces should conduct training specific to their organization's anti-bullying policies and procedures to equip lawyers with tools to respond, whether they are being targeted by bullying or witnessing it.
   c. Courts should enforce anti-bullying standards in courtrooms and litigation activities.
   d. Bar associations should use their resources and reach to advance programs that educate members on the prevalence and impact of bullying in the legal profession.
   e. Lawyers being bullied should respond in the way they feel best safeguards their rights, well-being, and career.

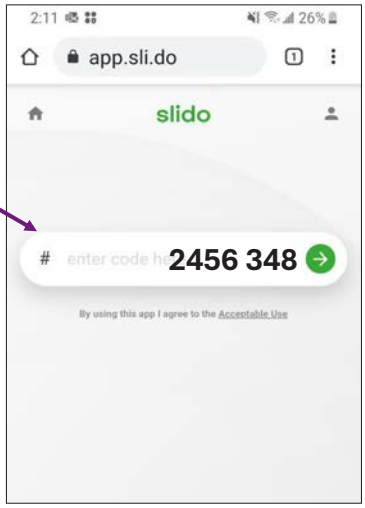
4) **Additional tips for navigating bullying**
(*see* Suskind, Dorothy, How to Deal With Adult Bullies: Strategies for Navigating Workplace Abuse, Psychology Today (May 6, 2022))

- ❖ Document
- ❖ Set boundaries
- ❖ Report to ARDC if Rules of Professional Conduct have been violated (Rule 3.5(d), Rule 4.4(a), Rule 8.4(d), (j))
- ❖ Follow any applicable organizational bullying policy
- ❖ Report if you feel safe doing so
- ❖ Attempt to create distance
- ❖ Rely upon friends/mentors (including co-workers and those outside of work) as shields and sources of support
- ❖ Build a bench of people to bolster your reputation and career
- ❖ Rehearse rebuttals and responses


Illinois Supreme Court Commission on Professionalism
Bullying
in the Legal Profession:
A Study of Illinois Lawyers' Experiences and Recommendations for Change
October 2024
by Stephanie A. Scharf and Roberta D. Liebenberg
Preventing Bullying in the Legal Profession: An Ethical Case for Courage and Change
Julia Roundtree Livingston
Diversity, Equity & Inclusion Manager
Illinois Supreme Court Commission on Professionalism
Julia.livingston@2civility.org
© 2025 Illinois Supreme Court Commission on Professionalism

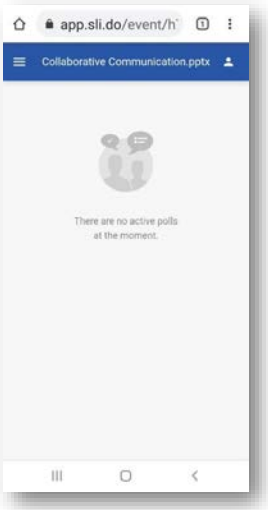

On your phone or tablet, go to www.slido.com or scan the QR code with your phone camera.
Slido.com
www.slido.com
© 2025 Illinois Supreme Court Commission on Professionalism

On the Slido website, enter **2456 348** in the participant box at the top.

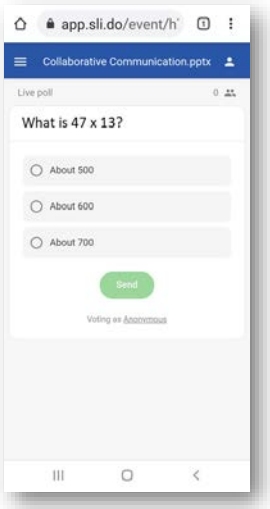


Then, tap the green arrow.

Home Page



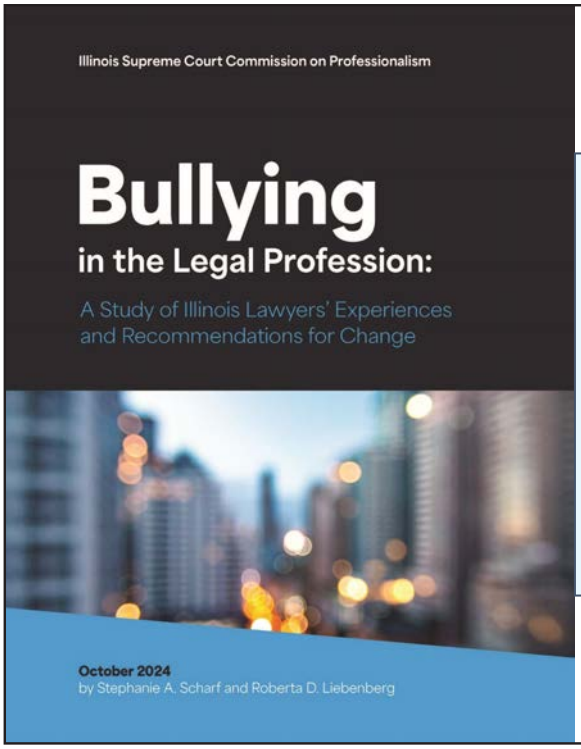
Poll Screen



Do not edit
How to change the design

Was the partner bullying the junior associate?

ⓘ The Slido app must be installed on every computer you're presenting from slido



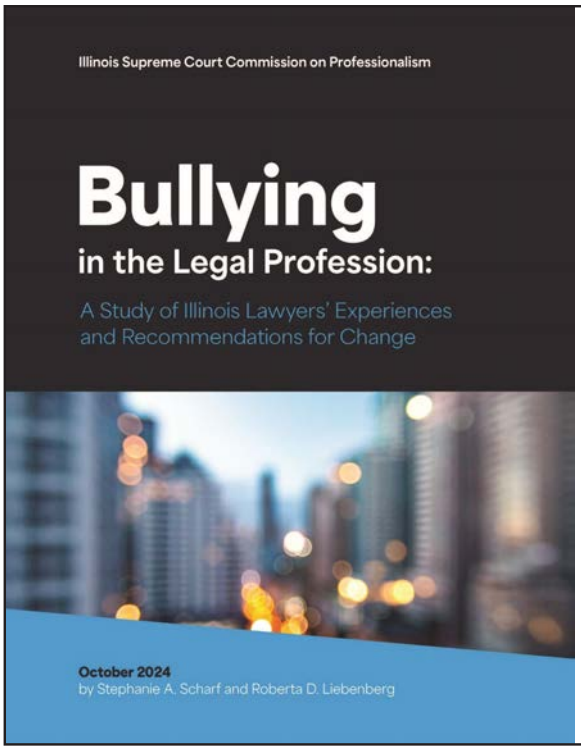
- The "Why" for the Study
- The Data from the Study
- The Recommendations for Change

Illinois Supreme Court Commission on Professionalism

Commission created by the Illinois Supreme Court.

Promote integrity, ethics, inclusion, well-being, and civility among Illinois lawyers and judges.

Achieve our mission through robust communications platforms, CLEs, surveys/reports, media, and collaboration with justice stakeholders.



- Released by the Illinois Supreme Court Commission on Professionalism in October 2024
- Believed to be one of the first wide-scale research projects in the U.S. on the topic
- Studied more than **6,000 Illinois lawyers**
- Survey **defined bullying** as "inappropriate behavior intended to intimidate, humiliate, or control the actions of another person, including verbal, nonverbal, or physical acts“
- Focused on bullying as opposed to harassment

Incivility vs. Bullying = Intent, Targeting, Frequency

- ***Bullying*** - inappropriate behavior (that is often repeated over time) intended to intimidate, humiliate, or control the actions of another person, including verbal, nonverbal, or physical acts

- ***Incivility*** - rude or disrespectful behavior that, while inappropriate, may not always be targeted at a particular person and may not always be intended to intimidate, humiliate, or control a particular person

Bullying vs Harassment = Protected Characteristic

- ***Harassment*** - bullying that is targeted at someone due to a protected characteristic. Bullying that cannot be proven to be motivated by such a characteristic is usually not illegal and may not be encompassed by many organizations' anti-harassment policies.

Unchecked incivility can foster the corrosive conditions that lead to bullying and harassment.

Workplace & Work Logistics of Surveyed Lawyers

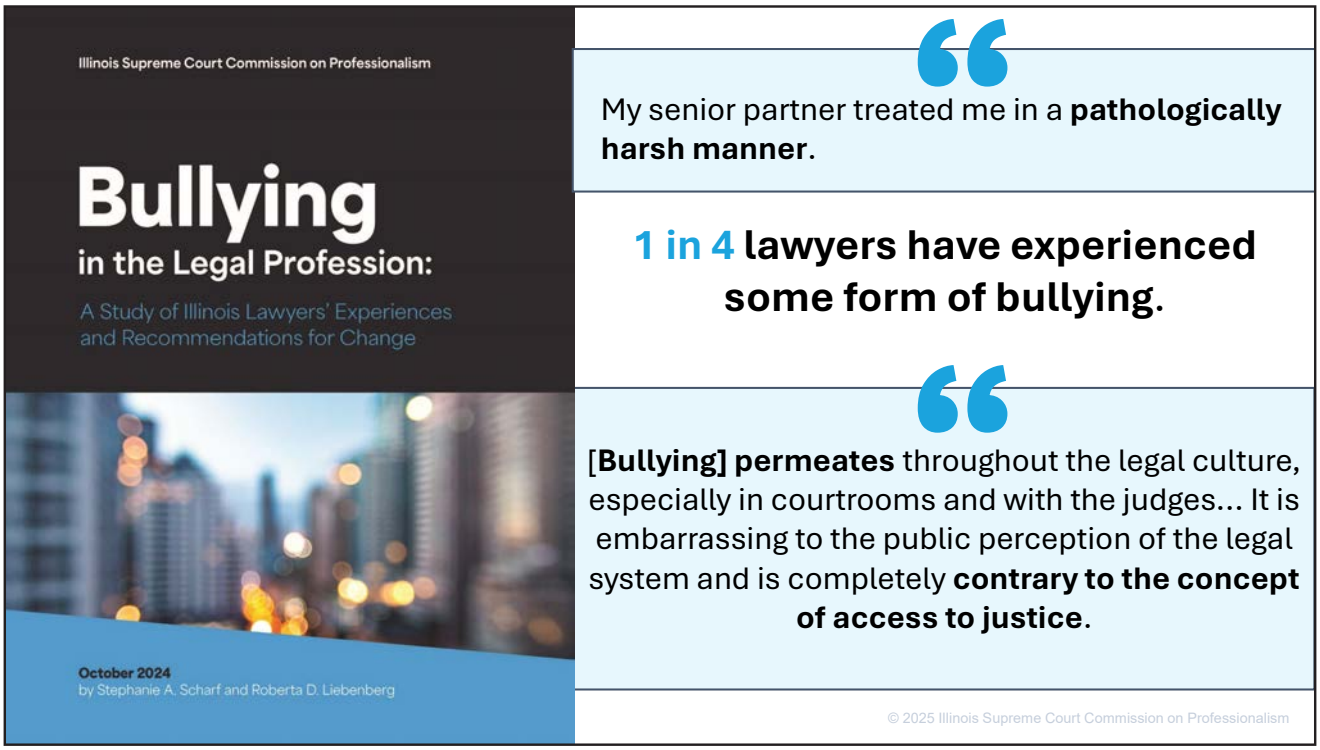
Where lawyers work	% of respondents
Law firm	42%
Solos	25%
Government	16%
Corporate law department	10%
Other	3%
Legal aid	2%
Nonprofit	2%
Judiciary	1%
Law school/Academia	1%

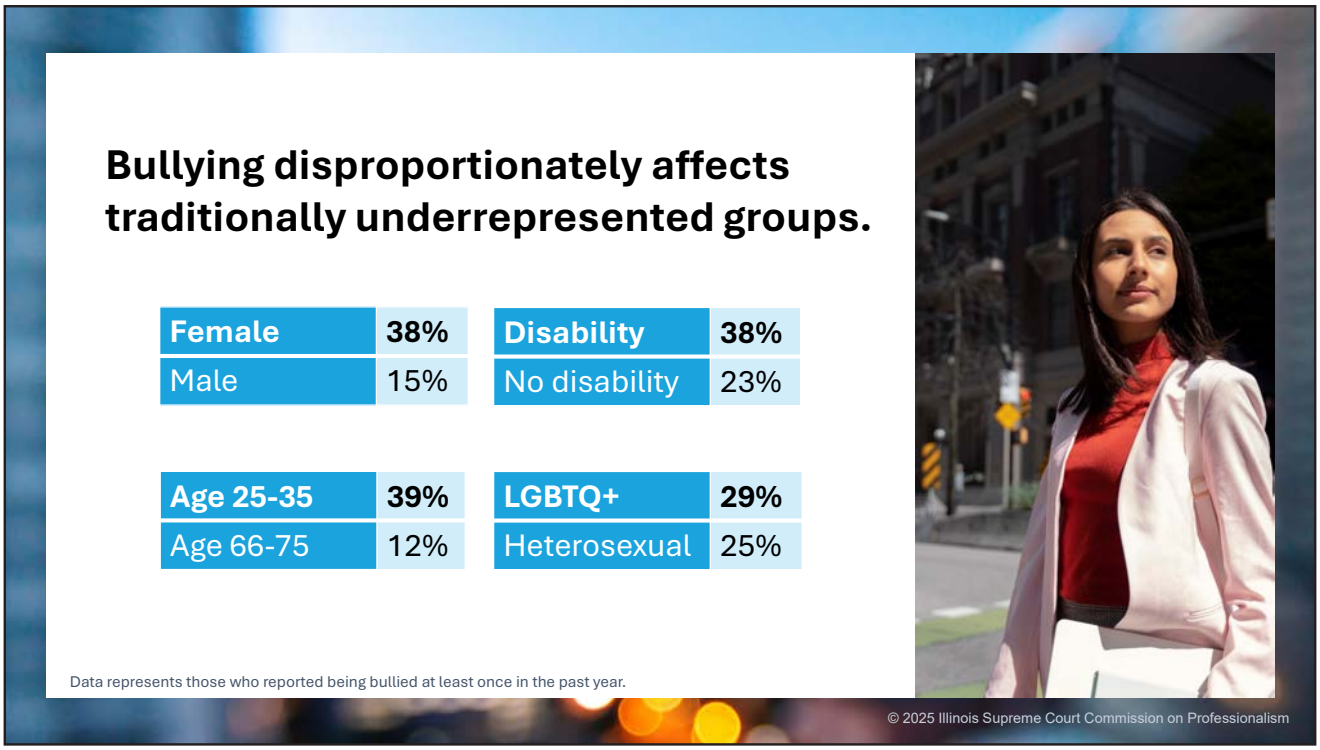
Number of attorneys in firm	% of respondents
Solo	38%
2-5	26%
6-10	9%
11-50	12%
51-249	5%
250+	10%

Illinois locations of employment of surveyed lawyers

Locations of employment	% of respondents
Chicago/Cook County	63%
Northern Illinois	22%
Central Illinois	10%
Southern Illinois	5%

What does bullying look like in the legal workplace?


Illinois Supreme Court Commission on Professionalism
Bullying
in the Legal Profession:
A Study of Illinois Lawyers' Experiences and Recommendations for Change
October 2024
by Stephanie A. Scharf and Roberta D. Liebenberg
My senior partner treated me in a pathologically harsh manner.
1 in 4 lawyers have experienced some form of bullying.
[Bullying] permeates throughout the legal culture, especially in courtrooms and with the judges... It is embarrassing to the public perception of the legal system and is completely contrary to the concept of access to justice.
© 2025 Illinois Supreme Court Commission on Professionalism


Bullying disproportionately affects traditionally underrepresented groups.
Female 38%
Male 15%
Disability 38%
No disability 23%
Age 25-35 39%
Age 66-75 12%
LGBTQ+ 29%
Heterosexual 25%
Data represents those who reported being bullied at least once in the past year.
© 2025 Illinois Supreme Court Commission on Professionalism

> I left the last two Legal Aid agencies because of bullying and lack of ADA accommodations.

> Aggressive, mostly older lawyers intimidate younger/newer ones and use it as a legal tactic.

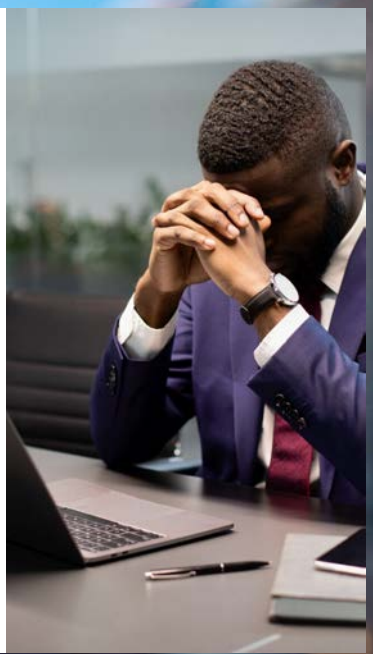
> The Chief Executive Officer regularly threatened, intimidated, and belittled me generally, in private and in person. He also did the same specifically based on my sexual orientation but did that only in private.

> Female lawyers reported being subjected to shouting, insults, and being called demeaning names such as “Sweetheart,” “Honey,” and “Cutie,” to more extreme name-calling such as “f***ing c**t.”

Lawyers of color were bullied more often than white lawyers.

Middle Eastern/North African	36%
Black	35%
Hispanic	34%
Multiracial	32%
Asian American	28%
White	23%

Data represents those who reported being bullied at least once in the past year.

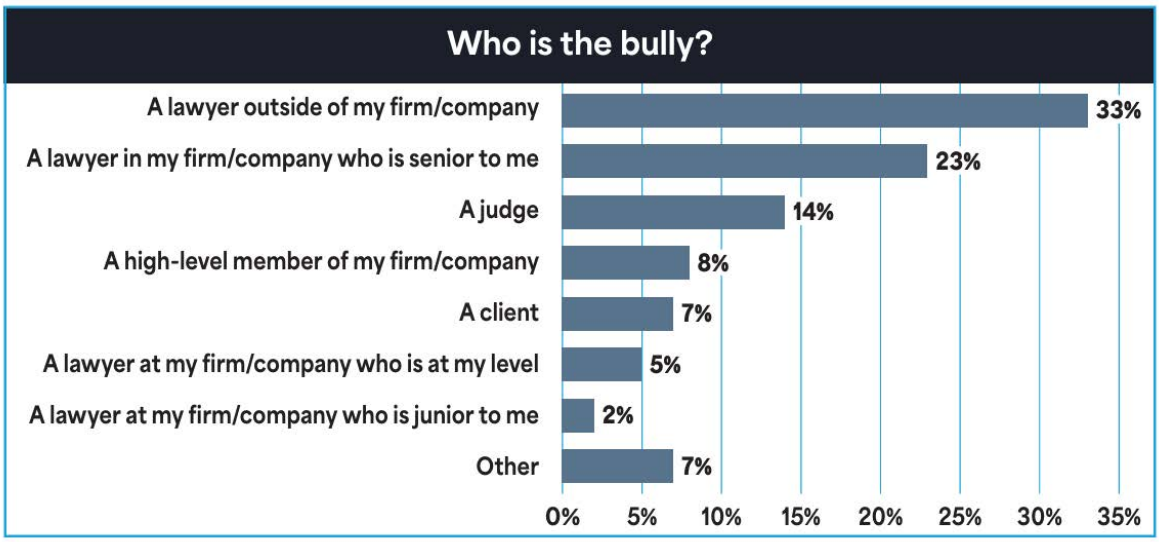


> In an employment evaluation, I was described as an 'angry Black man' who 'didn't get along with colleagues or clients.'

> On multiple occasions, I've been told, 'You're very articulate. You have no accent.'

> I've worked in several legal environments that are toxic. The people are manipulative and very competitive. Biases and stereotypes are prevalent and racial cliques are dominant. Minorities struggle to advance and find mentorship that can help them.

Who could be a bully in the legal profession?



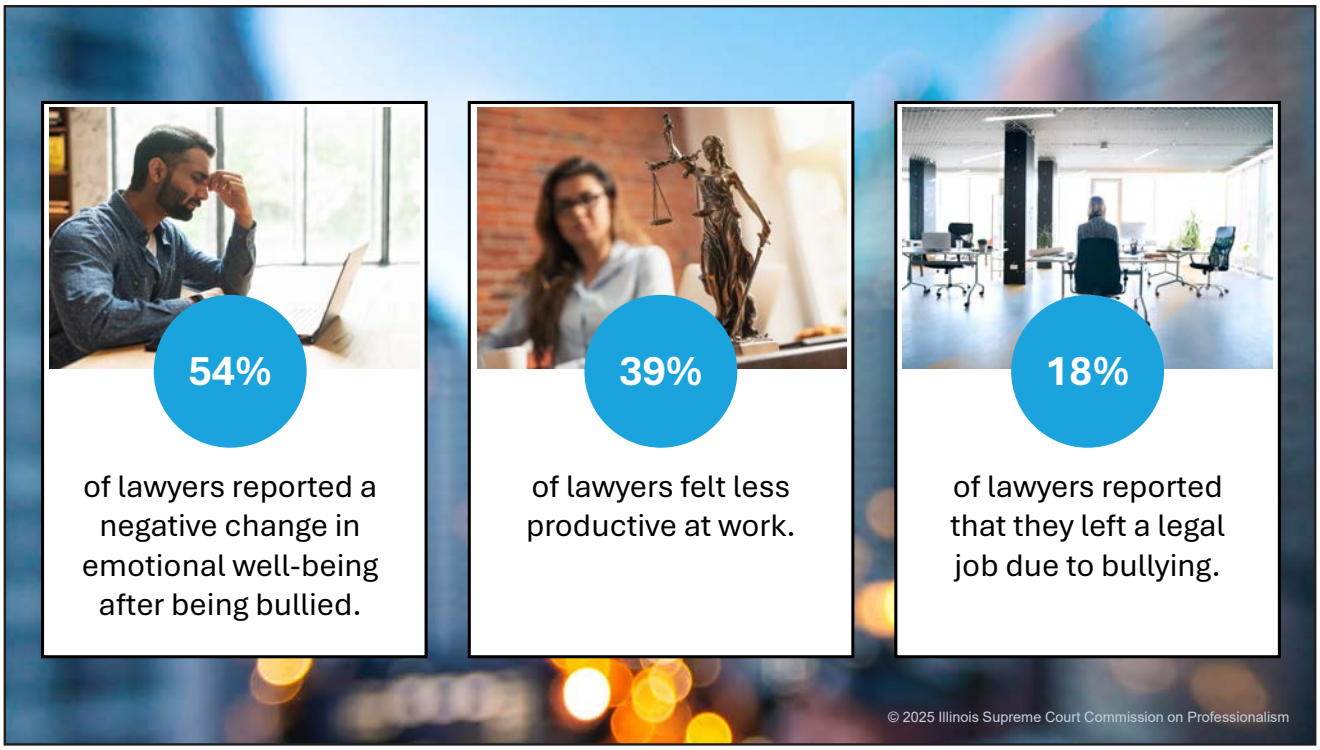
Most commonly experienced types of bullying in the past year

1. Verbal intimidation, such as disrespectful speech, insults, name-calling, shouting
2. Harsh, belittling, or excessive criticism of you or your work
3. Demeaning nonverbal behaviors, such as eye-rolling, finger-pointing, staring
4. Routinely being subject to unrealistic deadlines or other unreasonable work demands
5. Behind-the-back false accusations, malicious rumors
6. Someone improperly taking credit for your work
7. Not receiving work-related information, not being invited to important work meetings

Do not edit
How to change the design

What examples of bullying did you see?

ⓘ The Slido app must be installed on every computer you're presenting from slido



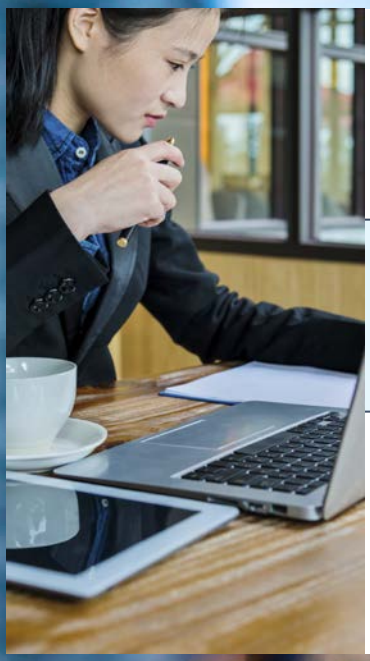
Negative effects reported by those bullied	% of bullied lawyers who reported this response
Experienced a negative change in emotional well-being (such as anxiety, loss of self-confidence, and other negative feelings and reactions)	54%
Felt less productive at work	39%
Experienced a decline in physical health	20%
Had reduced opportunities to work on matters	12%
Changed jobs	6%
Changed practice areas or departments	4%
Lost a promotion opportunity	3%
Lost their job and stopped working as a lawyer	2%

Note: Multiple responses can be reported.

> At my current job, the partner that I report to appears incapable of acknowledging his role in creating the **toxic workplace problems** that exist. On a daily basis, this leads to increased staff **stress, anxiety, and uncertainty**... Staff is ignored, badgered, lied to regularly, and blamed for mistakes caused by the partner

> **Bullying compounds itself**. After being bullied, you begin to worry. Then, you have trouble sleeping. You come to work but you aren't working at your full capacity.

> **Bullying is a great silencer**.

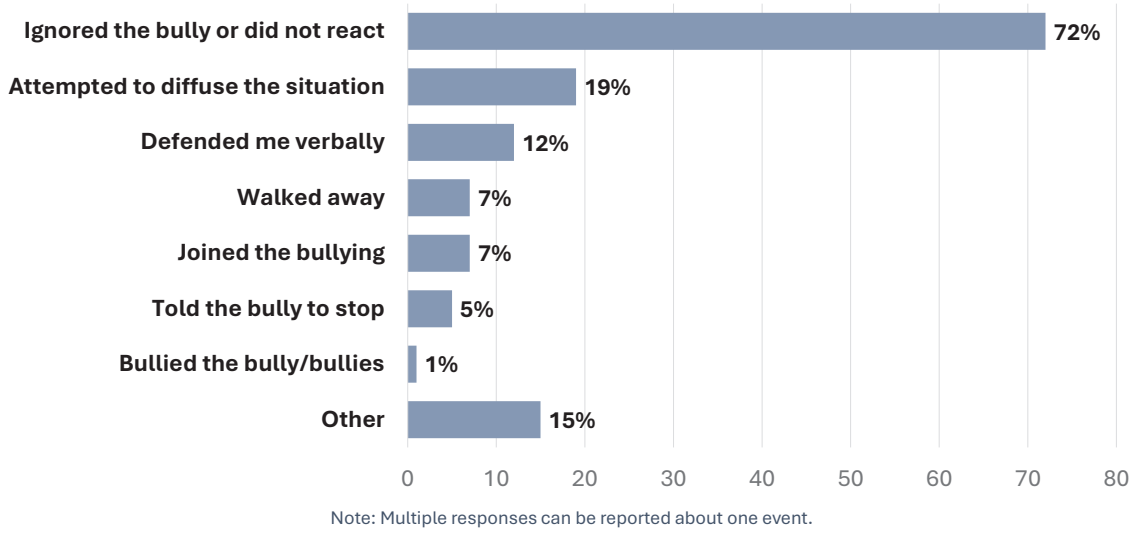


Only 20% of bullying cases are reported to supervisors, firm leaders, or HR.

> If I said something, I might have lost my job.
> **I feared possible repercussions.**

More than half of those who did report rated their employer's response as not sufficient or totally unsatisfactory.

Reactions of witnesses to bullying



Note: Multiple responses can be reported about one event.

Recommendations for Legal Organizations

1. Implement anti-bullying policies in all workplaces where lawyers practice.
2. Institute regular and customized workplace training against bullying.
3. Bar associations should continue to educate and offer anti-bullying support.

29

Recommendation

Enforce anti-bullying standards in courtrooms and litigation activities.

- ☑ **Circuit-wide standing orders**
- ☑ **Judicial trainings**

> A judge that makes it very clear from the first impression that something's about to happen, that they are not going to tolerate [bullying] in their courtroom, makes a huge difference.

Recommendation

Law schools should offer educational programs and training to law students on bullying prevention.

> Competitiveness is baked into the legal profession from the time the LSATs are taken through the type of firm one works in. It's extremely hierarchical and perfectionistic, which lends itself to bullying behaviors.

Recommendation

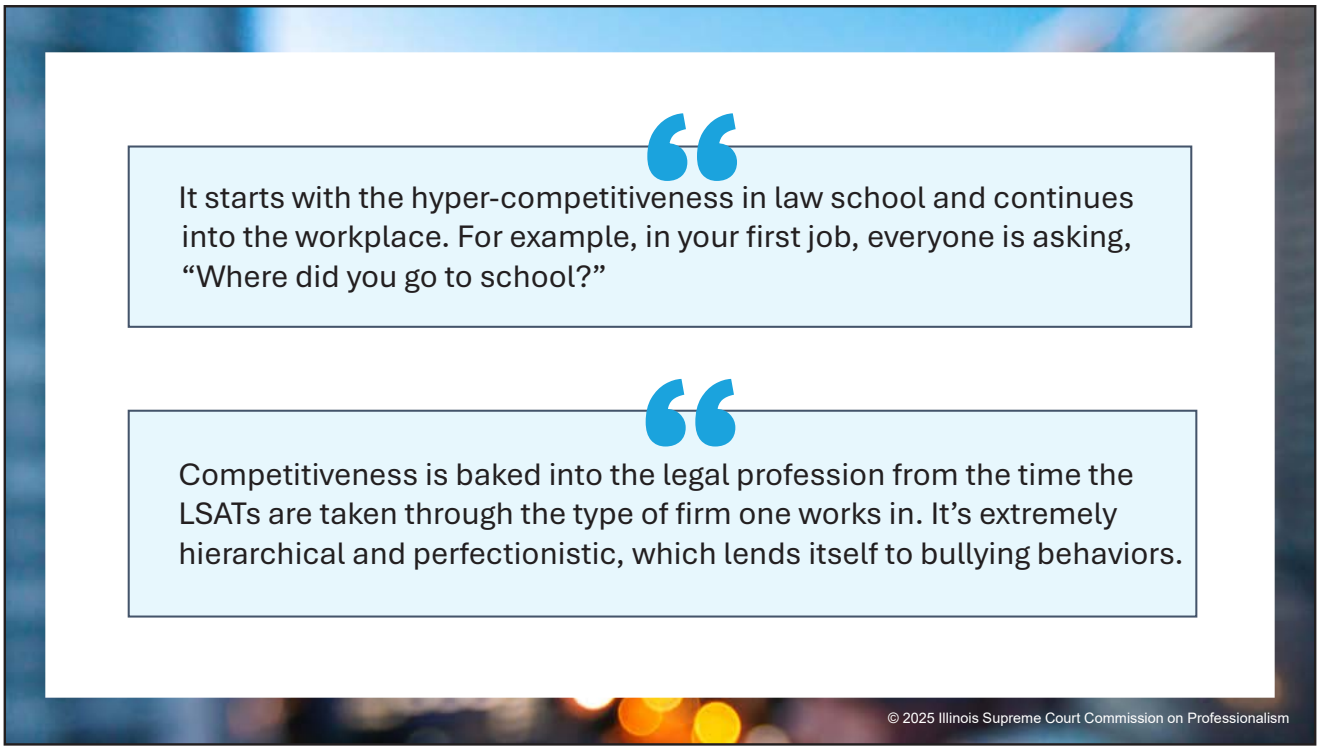
Individuals who are targeted should take the steps they feel best protect their rights, well-being, and careers.

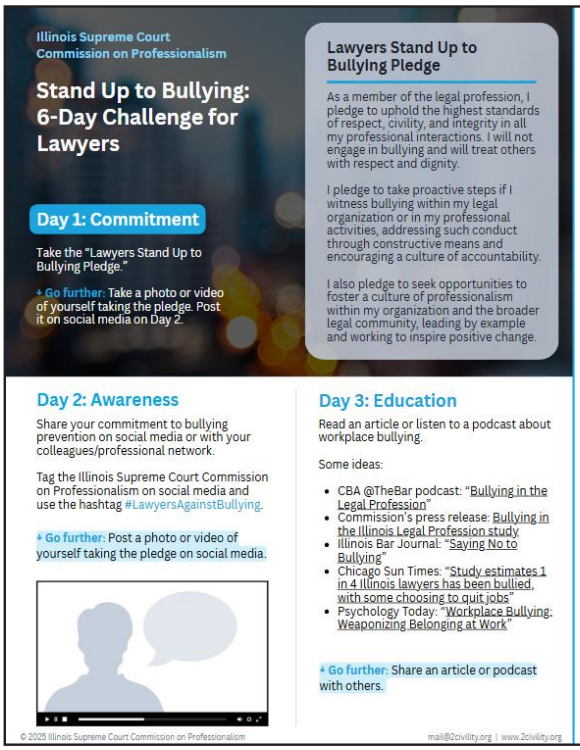
- **Document**
- **Follow organization's policy**
- **Talk to mentors/allies inside and outside of the organization**
- **Set boundaries with the bully**
- **Stand up for yourself and your work**
- **Seek to avoid working with the bully, if feasible**

Do not edit
How to change the design

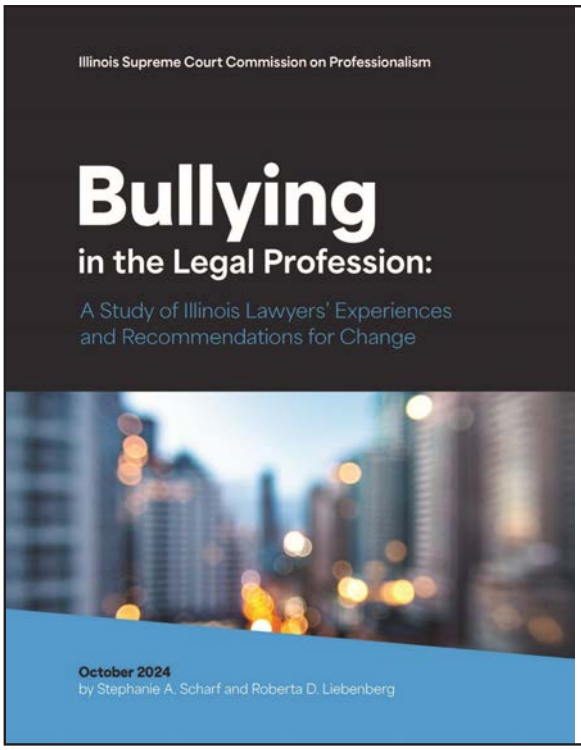
What would you do if you were in Jason's position?

ⓘ The Slido app must be installed on every computer you're presenting from slido

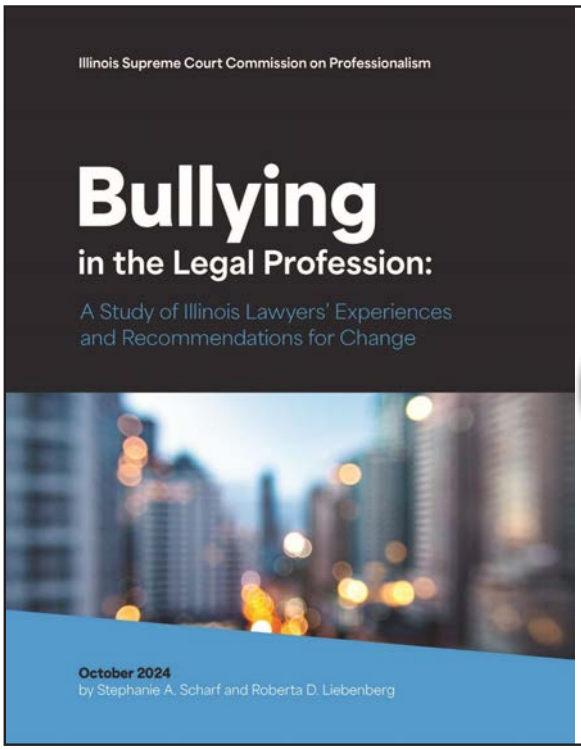




Read the full challenge by scanning the QR code or by visiting https://www.2civility.org/stand-up-to-bullying-6-day-challenge-for-lawyers/



Read the full report by scanning the QR code or by visiting www.2Civility.org/bullying-in-the-legal-profession



Questions?

Julia Roundtree Livingston
Diversity, Equity & Inclusion Manager
Illinois Supreme Court
Commission on Professionalism

Julia.livingston@2civility.org

Connect with the Commission

Julia Roundtree Livingston,
Diversity, Equity & Inclusion Manager

- Julia.Livingston@2civility.org
- (2) Julia Roundtree Livingston | LinkedIn

1. **Visit our website.**
   2civility.org
2. **Follow us on social media.**
3. **Subscribe to our email newsletters.**

Scan to receive legal profession news, CLEs, and Commission updates.

PANEL 5 — 2:40 - 3:40pm

You, your client and AI usage: When and what type of client notice and consent is needed?

Panelists:

Aaron W. Brooks, Chief Information Security Officer, *Illinois ARDC*

Hon. Jeffrey A. Goffinet, Associate Judge, *1st Judicial Circuit Court*

Matthew J. O'Hara, Partner, *Smith Gambrell Russell LLP*

Aaron W. Brooks, Chief Information Security Officer, *Illinois ARDC*

Aaron contracts with the Illinois Attorney Registration and Disciplinary Commission, serving as its Chief Information Security Officer and its primary legal and technical advisor on artificial intelligence. His role with the ARDC is just part of his primary practice that focuses on privacy, information security, and technology transactions. He has more than twenty-five years of experience representing hospitals, governmental organizations, software developers, and other entities that work with highly sensitive information and complex technology systems.

He is an active member of the Illinois State Bar Association and currently serves as Chair of the ISBA Steering Committee on Artificial Intelligence. He is also the past Chair of both the ISBA Intellectual Property Section Council and the ISBA Privacy and Information Security Section Council. Through these roles, Aaron has spent nearly two decades educating Illinois lawyers about their ethical obligations related to emerging technologies.

Aaron also is an Adjunct Professor at the University of Illinois, where he teaches blockchain law and technology. He received his law degree from the University of Illinois and holds a Master of Science in Cybersecurity Management from the University of Illinois as well.

Hon. Jeffrey A. Goffinet, Associate Judge, *1st Judicial Circuit Court*

Judge Goffinet practiced law in southern Illinois for 31 years as civil litigator with the firm of Brandon, Schmidt & Goffinet, in Carbondale. As an Associate Judge, Judge Goffinet currently presides over the Law docket in Williamson County. Judge Goffinet has served as the vice-chair of the Illinois Supreme Court Trial Court Administrators Education committee and was co-chair of the Illinois Supreme Court Task Force on artificial intelligence.

Judge Goffinet also served as adjunct faculty at the Southern Illinois University School of Law for more than a decade teaching classes on pretrial and trial advocacy. He has taught multiple courses at EdCon, the Illinois judges education conference, on digital evidence and civil trials. Most recently, he has presented courses on generative artificial intelligence and its impact on the judicial system to the State of Illinois Circuit Clerks, Conference of the Chief Judges of the Northernmost Circuits (Illinois); the ISBA Allerton Conference, Inns of Court, Jackson County Bar Joint CLE and multiple others. Judge Goffinet is a longtime volunteer doing service work and construction from Appalachia to Anchorage, Alaska.

Matthew J. O'Hara, Partner, *Smith Gambrell Russell LLP*

Matt is a Partner in the Litigation Practice of Smith, Gambrell & Russell, LLP and previously a member of the Firm's Executive Committee. He also was previously a Partner with Freeborn & Peters, which combined with SGR in 2023.

Matt is a business trial lawyer who concentrates his practice in the litigation and trial of complex commercial matters in federal and state courts and matters involving the law of lawyering. He has tried cases involving the federal securities laws, antitrust laws, breach of fiduciary duty, trade secrets, trademark infringement, breach of contract, legal malpractice, contract reformation, unjust enrichment, license agreements, executive employment, the Uniform Commercial Code, fraud, and criminal defense. He also litigates private shareholder and partnership disputes, fraudulent transfers, defamation, and other commercial matters. Matt has represented clients in investigations by the Securities and Exchange Commission, the Federal Trade Commission, and the Illinois Attorney Registration and Disciplinary Commission. He is also experienced in briefing and arguing state and federal appeals. In the legal industry, Matt represents law firms and lawyers in litigation, counseling, and disciplinary defense, and serves as an expert witness in cases involving legal ethics and professional liability.

Matt is very active in providing pro bono legal services. In 2008, he was one of the recipients of the Constitutional Rights Foundation Chicago's "Bill of Rights in Action" Award. He has been quoted concerning his pro bono representations in a variety of publications and on a number of news programs, including the New York Times, the

O'Hara continued

Washington Post, the Chicago Tribune, the Los Angeles Times, the Miami Herald, The Wall Street Journal, El País (Spain), ABC (Spain), El Mundo (Spain), Radio Free Europe, the BBC, Radio Nacional Argentina, the American Lawyer, the Chicago Daily Law Bulletin, and the CBA Record.

Before joining the Firm, Matt was a Partner at Hinshaw & Culbertson LLP, where he served on the Executive Committee and as co-chair of the Lawyers Professional Liability practice group. Matt began his legal career in 1996 at Sachnoff & Weaver, Ltd., which merged with Reed Smith LLP in 2007. He served as a deputy general counsel to Reed Smith, advising the firm on ethics and risk management.

PANEL 5

You, your client and AI usage: When and what type of client notice and consent is needed?

Aaron W. Brooks, Chief Information Security Officer, *Illinois ARDC*

Hon. Jeffrey A. Goffinet, Associate Judge, *1st Judicial Circuit Court*

Matthew J. O'Hara, Partner, *Smith Gambrell Russell LLP*

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE

EFFECTIVE JANUARY 1, 2025

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

The Illinois Supreme Court Policy on Artificial Intelligence

- GAI Use is Authorized
- Attorney Accountability
- Duty of Competence
- Privacy and Security

Key Points

- Can be used by counsel/litigants without disclosure.
- Must comply with current Illinois court rules and be well-grounded in facts and law.
- You sign it. You own it.

Key Focus
AI Confidentiality and Security

The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.

AI applications tend to hallucinate because they are built to generate the next statistically significant _____.

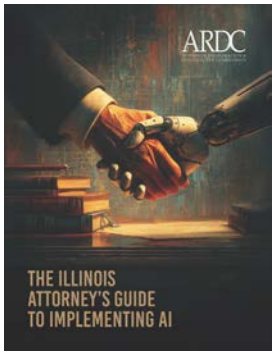
Attention Mechanism

Token (98%)
Response (1%)
Output (1%)

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

5

ARDC Core Framework

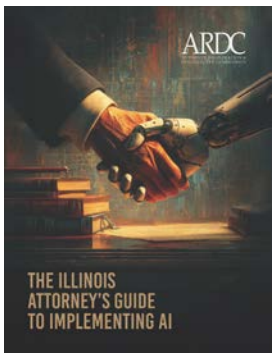


- Step One: Classify the Information to be Processed
- Step Two: Classify the GAI Tool to be Used
- Step Three: Apply the 8 Key Risk Factors
- Step Four: Decision Matrix and Client Communication Strategy

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

6

Data Classification



- **General:** not subject to any confidentiality protections
- **De-Identified**: relates a client but without identifiable information
- **Confidential**: Information that is protected by Rule 1.6
- **Sensitive/Personal**: Highly sensitive beyond Confidential Information

Data Classification	Public	Consumer	Business	Enterprise
General Information Non-confidential information entirely unrelated to any client matter	Unrestricted	Unrestricted	Unrestricted	Unrestricted
De-Identified Information No reasonable likelihood of identifying the client or matter	Consent	Opt-Out	Opt-Out	Unrestricted
Confidential Information Information protected by Rule 1.6, but without Sensitive Personal Information	Prohibited	Consent	Opt-Out	Opt-Out
Sensitive Personal Information Highly sensitive data including PII, PHI, or other regulated personal data	Prohibited	Prohibited	Consent	Opt-Out
System-Wide Processing GAI systems used in firm-wide administrative, security, or operational functions	Prohibited	Prohibited	Prohibited	Notice Only

Table 3: Relationship between data classification, GAI tool classification, and client communication strategy

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Data Classification	Public	Consumer	Business	Enterprise
General Information Non-confidential information entirely unrelated to any client matter	Unrestricted	Unrestricted	Unrestricted	Unrestricted
De-Identified Information No reasonable likelihood of identifying the client or matter	Consent	Opt-Out	Opt-Out	Unrestricted
Confidential Information Information protected by Rule 1.6, but without Sensitive Personal Information	Prohibited	Consent	Opt-Out	Opt-Out
Sensitive Personal Information Highly sensitive data including PII, PHI, or other regulated personal data	Prohibited	Prohibited	Consent	Opt-Out
System-Wide Processing GAI systems used in firm-wide administrative, security, or operational functions	Prohibited	Prohibited	Prohibited	Notice Only

Table 3: Relationship between data classification, GAI tool classification, and client communication strategy

Data Classification	Public	Consumer	Business	Enterprise
General Information Non-confidential information entirely unrelated to any client matter	Unrestricted	Unrestricted	Unrestricted	Unrestricted
De-Identified Information No reasonable likelihood of identifying the client or matter	Consent	Opt-Out	Opt-Out	Unrestricted
Confidential Information Information protected by Rule 1.6, but without Sensitive Personal Information	Prohibited	Consent	Opt-Out	Opt-Out
Sensitive Personal Information Highly sensitive data including PII, PHI, or other regulated personal data	Prohibited	Prohibited	Consent	Opt-Out
System-Wide Processing GAI systems used in firm-wide administrative, security, or operational functions	Prohibited	Prohibited	Prohibited	Notice Only

Table 3: Relationship between data classification, GAI tool classification, and client communication strategy

Data Classification	Public	Consumer	Business	Enterprise
General Information Non-confidential information entirely unrelated to any client matter	Unrestricted	Unrestricted	Unrestricted	Unrestricted
De-Identified Information No reasonable likelihood of identifying the client or matter	Consent	Opt-Out	Opt-Out	Unrestricted
Confidential Information Information protected by Rule 1.6, but without Sensitive Personal Information	Prohibited	Consent	Opt-Out	Opt-Out
Sensitive Personal Information Highly sensitive data including PII, PHI, or other regulated personal data	Prohibited	Prohibited	Consent	Opt-Out
System-Wide Processing GAI systems used in firm-wide administrative, security, or operational functions	Prohibited	Prohibited	Prohibited	Notice Only

Table 3: Relationship between data classification, GAI tool classification, and client communication strategy

Supporting Resources and Materials

Appendix 1: Illinois Supreme Court Policy on Artificial Intelligence, together with Judicial Reference Sheet on AI

Appendix 2: GAI Terms of Use Checklist

Appendix 3: Sample Notice of Artificial Intelligence Practices

Appendix 4: Sample Use of GAI Tools Policy

Appendix 5: Sample Informed Client Consent Form

AI Practice Resource Kit

Appendix 6: Cybersecurity Information Sheet ("CIS"): Deploying AI Systems Securely – Best Practices for Deployment

Hypothetical 1

- Emily has a new case in Arizona. She'd like to use a free AI tool embedded in her web browser to learn what the elements of a claim for tortious interference with contract are in that state.
- She types in a query and some follow-up queries into the browser, and does not include any information that identifies the parties in her case or any of the key facts.
- Must Emily get informed consent for her client to do this?

Hypothetical 2

- Emily is preparing an engagement letter for this new case for her new client.
- Should the engagement letter say anything about the use of AI tools in providing legal services?
- What topics should it cover?

Hypothetical 3

- Emily takes what she learns from her general research queries in an open system and uses AI tools available in Westlaw or Lexis to refine her research.
- The AI tool generates a memo summarizing the law and recommending legal arguments to make in a motion to dismiss.
- Emily intends to review the cases and other authorities referenced in the memo and to use the memo as a starting point for her motion, and edit the memo to tweak it to the facts of her case.

- **Is the client's informed consent required?**

Hypothetical 3 continued

Does the answer change at all in any of the following scenarios?

(1) Emily intends to use the AI-generated memo in a memo to the client about recommended defense strategies?

(2) Emily intends to use the AI-generated memo to write a letter to opposing counsel urging them to dismiss the case?

(3) Emily intends to use the AI-generated memo to write letters to third parties explaining why her client has third-party claims against them related to the dispute and urging them to contact her to discuss how litigation can be avoided?

Hypothetical 4

Emily's new case includes documents that reveal personal identifying information (PII), personal health information (PHI), and financial account information.

- Can Emily use AI tools in her document review platform to summarize these documents?
- Is Informed Client Consent required for AI tools to analyze such information?
- If so, how should Emily communicate the risks to the client so the client can provide Informed Client Consent?

Hypothetical 5

Paul is a lawyer at XYZ Law. XYZ Law has a business licenses to use both Zoom and Teams. Both platforms allow recording of video meetings through the use of AI voice recognition tools. While Paul has some concerns about using these tools, he can see that they can be useful.

- Paul wants to know if XYZ Law is required to address the use of AI recording tools in its engagement letters. Is it?
- If not, is it recommended?

Hypothetical 6

ABC Law's staff person responsible for the IT network recommends that the firm use a document review tool to analyze case documents in discovery. The vendor assures the staff person that client confidential information is not uploaded into a public tool, but rather stays within a closed system. Emily would like to use this tool to begin reviewing her client's documents about the case.

- Does this require informed consent?
- What should Emily learn about the tool to properly advise her client about where the client's information will be housed so that the client's consent is informed?

Ethics 2026
You, your client and AI usage:
When and what type of client notice and consent is needed?

Wednesday, May 13, 2026
Virtual Event | 2:40pm – 3:40pm

Panelists:
Aaron W. Brooks, Chief Information Security Officer, Illinois ARDC
Hon. Jeffrey A. Goffinet, Associate Judge, 1st Judicial Circuit Court
Matthew J. O'Hara, Partner, Smith Gambrell Russell LLP

Program Agenda

I. Moderator Introduction and Comments (*5 min*)
Peter Mierzwa, Law Bulletin Media President and Publisher

II. The Illinois Supreme Court Policy on Artificial Intelligence *(10 min)*.

Effective January 1, 2025, the Illinois Supreme Court announced a new Policy on Artificial Intelligence, together with a judicial reference sheet on AI. The Policy makes four key points:

- GAI Use is Authorized. The Policy authorizes the use of artificial intelligence by attorneys, subject to the requirements set forth in the Policy.

- Attorney Accountability. Attorneys who use artificial intelligence in their practice must thoroughly review and assume professional responsibility for any AI-generated information that is incorporated into their work product.

- Duty of Competence. The Policy requires attorneys who use artificial intelligence tools to understand those tools and ensure that they are secure and legally compliant. This aspect of the Policy echoes the long-standing rule set forth in Illinois Rule of Professional Conduct 1.1 that an attorney's duty of competence extends to the benefits and risks associated with technology.

- Privacy and Security. The Policy requires attorneys to confirm that GAI tools maintain the privacy and security of confidential and personally identifiable information.

III. The Illinois Attorney's Guide to Implementing AI *(15 min)*

Effective October 1, 2025, the Illinois Attorney Registration and Disciplinary Commission released the Illinois Attorney's Guide to Implementing AI, which is intended to supplement the privacy and security provisions in the Illinois Supreme Court Policy on Artificial Intelligence, which states:

"*The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust*."

This component of the Policy corresponds to a lawyer's duty to preserve client confidentiality, including the security of any client data in the lawyer's possession. Determining whether a GAI tool is appropriate for handling this type of information can be complex. For that reason, ARDC's guidance document includes policies, checklists, and practical examples to support attorneys in evaluating and implementing AI tools in a manner that protects sensitive data and complies with legal and ethical obligations.

The ARDC's guidance outlines a 4-step process that attorneys might use to help determine whether the AI tools they implement are appropriate for processing various types of information:

Step One: Classifying Data

Understanding the four levels of data sensitivity (General, De-Identified, Confidential, Sensitive Personal Information) and how these classifications determine whether and how AI tools may be used. Illustration of how ARDC maps internal data sets into this framework.

Step Two: Categorizing AI Tools

Explanation of public, consumer, business, and enterprise-grade AI systems, including the difference between native model platforms and integrated tools that rely on third-party APIs.

Step Three: The Eight Key Safeguards Required for Safe AI Use

How to apply the Guide's eight common risk factors, including model training restrictions, data retention limits, data isolation, supply-chain controls, and authentication requirements, across all AI systems.

Step Four: Define the Client Communication and Consent Approach

Some AI tools (such as "public" tools that have little-to-no privacy and security protections) may not be used to process client confidential information, even with client consent. As a general rule, AI tools that provide business-class privacy and security protections may be used to process confidential information if clients are provided with adequate notice and a right to opt out of AI processing.

IV. Applying the Policy and Guidance to Various Hypothetical Situations *(30 min)*

Hypothetical One: Emily has a new case in Arizona. She'd like to use a free AI tool embedded in her web browser to learn what the elements of a claim for tortious interference with contract are in that state. She types in a query and some follow-up queries into the browser, and does not include any information that identifies the parties in her case or any of the key facts.

Question: Must Emily get informed consent for her client to do this?

Hypothetical Two: Emily is preparing an engagement letter for this new case for her new client.

Question: Should the engagement letter say anything about the use of AI tools in providing legal services? What topics should it cover?

Hypothetical Three: Emily takes what she learns from her general research queries in an open system and uses AI tools available in Westlaw or Lexis to refine her research. The AI tool generates a memo summarizing the law and recommending legal arguments to make in a motion to dismiss. Emily intends to review the cases and other authorities referenced in the memo and to use the memo as a starting point for her motion, and edit the memo to tweak it to the facts of her case.

Question: Is the client's informed consent required?

Question: Does the answer change at all in any of the following scenarios? (1) Emily intends to use the AI-generated memo in a memo to the client about recommended defense strategies; (2) Emily intends to use the AI-generated memo to write a letter to opposing counsel urging them to dismiss the case; (3) Emily intends to use the AI-generated memo to write letters to third parties explaining why her client has third-party claims against them related to the dispute and urging them to contact her to discuss how litigation can be avoided.

Hypothetical Four: Emily's new case includes documents that reveal personal identifying information (PII), personal health information (PHI), and financial account information.

Question: Can Emily use AI tools in her document review platform to summarize these documents? Is Informed Client Consent required for AI tools to analyze such information, and if so, how should Emily communicate the risks to the client so the client can provide Informed Client Consent?

Hypothetical Five: Paul is a lawyer at XYZ Law XYZ law has business licenses to use both Zoom and Teams. Both platforms allow recording of video meetings through the use of AI voice recognition tools. While Paul has some concerns about using these tools, he can see that they can be useful.

Question: Paul wants to know if XYZ Law is required to address the use of AI recording tools in its engagement letters. Is it? If not, is it recommended?

Bonus Hypotheticals (time permitting)

Hypothetical Six: ABC Law's staff person responsible for the IT network recommends that the firm use a document review tool to analyze case documents in discovery. The vendor assures the staff person that client confidential information is not uploaded into a public tool, but rather stays within a closed system. Emily would like to use this tool to begin reviewing her client's documents about the case.

Question: Does this require informed consent? What should Emily learn about the tool to properly advise her client about where the client's information will be housed so that the client's consent is informed?

Hypothetical Seven: XYZ Law decides it does not want to include mandatory provisions about the use of AI recording tools in its engagement letters, deciding that an ad hoc approach would be better. Paul has a new client, a company with its headquarters in Illinois and offices and employees in other states around the country. Paul is planning to interview over Zoom an executive based in Illinois about what she knows about the case. He'd like to use the AI recording tool to record and summarize the discussion.

Question: Is client consent required in this scenario?

Hypothetical Eight: Paul's client has employees in New York. Paul travels to New York, and while there, has a Teams meeting with his opposing counsel, whose office is in New York. He finds that his adversary is difficult and has misrepresented their prior conversations several times. Paul would like to use the AI recording feature in Teams to record their upcoming discussion about discovery disputes. Unlike Illinois, New York is a one-party consent state about recording of communications.

Question: Is Paul required to ask consent of his difficult adversary to record the conversation? If Paul decides he wants to record without asking for his adversary's consent, should Paul obtain the informed consent of his client to do this?

Hypothetical Nine: Paul is not comfortable with clients using AI tools to record his conversations with them where he gives legal advice and recommendations, because he believes it inhibits open dialog with this clients. He comes to believe his client's CEO is using AI recording features on Zoom to record their conversations, although the CEO does not tell him expressly he is doing that. While Paul would like to tell the CEO that he does not consent to recording, he is concerned that this will hurt his relationship with his client. He decides not to object before their next Zoom meeting.

Question: Should Paul state his preference that the CEO not record their discussion and inform his client of what he views as the downsides of recording attorney-client conversations before allowing himself to be recorded?

Hypothetical Ten: Paul assigns his associate to interview a number of the client's employees about the facts of their case.

Question: What directions should Paul give his associate about the use of AI recording tools to summarize the employee interviews?

Hypothetical Eleven: Emily is a lawyer at ABC Law. The firm has five lawyers and three support staff. There are varying levels of interest in using AI tools among the lawyers and staff. Some are keenly interested and have begun using AI tools in various ways in their work. ABC Law's staff person with responsibility for its IT system has begun to explore public AI tools and to also consider purchasing licenses to AI tools for the firm to use in its work.

Question: Is ABC Law required to have a written policy on usage of AI tools in client work? If it is not required, why would it be recommended for ABC Law to develop such a policy?

Appendix: Rule and Comments Relevant to AI and Client Consent

Rule 1.0 (e): "Informed consent" denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

RULE 1.1: COMPETENCE A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

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

RULE 1.4: COMMUNICATION (a) A lawyer shall: (1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules; (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished; (3) keep the client reasonably informed about the status of the matter; (4) promptly comply with reasonable requests for information; and (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law. (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

RULE 1.6: CONFIDENTIALITY OF INFORMATION
(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b) or required by paragraph (c).
***
(e) 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.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to

the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

Acting Competently to Preserve Confidentiality

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

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law

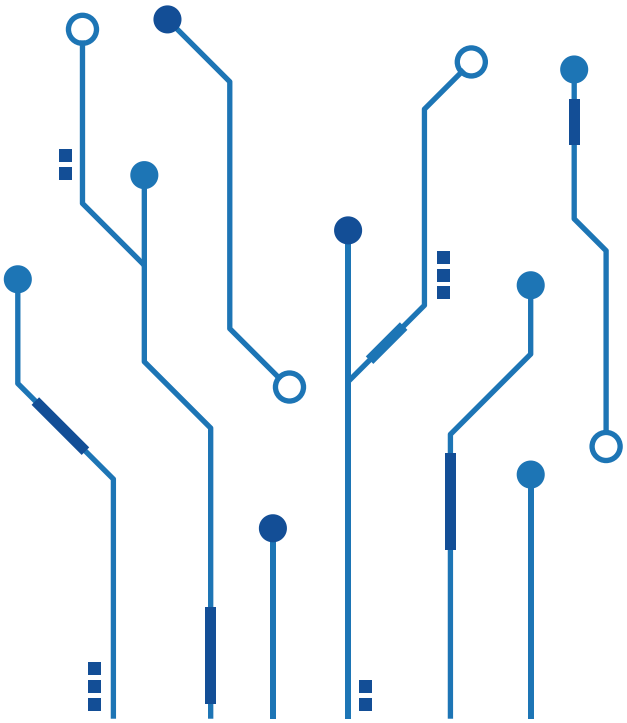
or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

RULE 3.3: CANDOR TOWARD THE TRIBUNAL
(a) A lawyer shall not knowingly:
(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
(2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or…

RULE 8.4: MISCONDUCT It is professional misconduct for a lawyer to:
***
(c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.
***

ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE

EFFECTIVE JANUARY 1, 2025



Embracing the advancements of artificial intelligence (AI), the Illinois Supreme Court remains steadfast in its commitment to upholding the highest ethical standards in the administration of justice. We acknowledge the rapid development of generative AI technologies capable of producing human-like text, images, video, audio, and other content. The integration of AI with the courts is increasingly pervasive, offering potential efficiencies and improved access to justice. However, it also raises critical concerns about authenticity, accuracy, bias, and the integrity of court filings, proceedings, evidence, and decisions. Understanding the capabilities and limitations of AI technology is essential for the Illinois Judicial Branch.

The Illinois Courts will be vigilant against AI technologies that jeopardize due process, equal protection, or access to justice. Unsubstantiated or deliberately misleading AI-generated content that perpetuates bias, prejudices litigants, or obscures truth-finding and decision-making will not be tolerated.

The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards. Disclosure of AI use should not be required in a pleading.

The Rules of Professional Conduct and the Code of Judicial Conduct apply fully to the use of AI technologies. Attorneys, judges, and self-represented litigants are accountable for their final work product. All users must thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations. Prior to employing any technology, including generative AI applications, users must understand both general AI capabilities and the specific tools being utilized.

The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.

This policy reflects the Illinois Supreme Court's commitment to upholding foundational principles while exploring the potential benefits of new AI technologies in a dynamic landscape. The Court will regularly reassess policies as these technologies evolve, prioritizing public trust and confidence in the judiciary and the administration of justice. **Judges remain ultimately responsible for their decisions, irrespective of technological advancements.**

The Court encourages the development of technologies that enhance service to all court users and promote equitable access to justice. To facilitate this, the judicial branch will support ongoing education on emerging technologies, including AI.

Illinois Supreme Court announces artificial intelligence policy

By Emma Oxnevad
Chicago Daily Law Bulletin
Posted December 18, 2024 3:00 PM CST

The Illinois Supreme Court announced its policy on artificial intelligence Wednesday, which stipulates that the Rules of Professional Conduct and the Code of Judicial Conduct "apply fully" to the use of AI.

The policy authorizes the use of AI by litigants, attorneys, judges, judicial clerks, research attorneys and court staff if compliant with legal and ethical standards. The use of AI is not required in a pleading, according to the policy.

But the policy prohibits the use of "unsubstantiated or deliberately misleading AI-generated content that perpetuates bias, prejudices litigants, or obscures truth-finding and decision-making." It notes that state courts will "be vigilant against AI technologies that jeopardize due process, equal protection, or access to justice."

It also requires that all users "thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations" and that "users must understand both general AI capabilities and the specific tools" before using any AI technology.

"Attorneys, judges, and self-represented litigants are accountable for their final work product," the policy states, in addition to providing that judges remain responsible for decisions regardless of advancements in technology.

Further, the policy provides that AI applications cannot compromise confidential communications, personal identifying information, protected health information, justice and public safety data, security-related information, or "information conflicting with judicial conduct standards or eroding public trust."

The high court will "regularly reassess policies as these technologies evolve, prioritizing public trust and confidence in the judiciary and the administration of justice," according to the policy.

"The Court encourages the development of technologies that enhance service to all court users and promote equitable access to justice," the policy states "To facilitate this, the judicial branch will support ongoing education on emerging technologies, including AI."

The policy was released following the approval of a report submitted by the Illinois Judicial Conference (IJC) Task Force on Artificial Intelligence, according to a news release.

The IJC Task Force, co-chaired by Williamson County Judge Jeffrey A. Goffinet and 17th Judicial Circuit Trial Court Administrator Thomas R. Jakeway, was created in early 2024. It was tasked with recommending the use and regulation of AI in Illinois courts.

It is comprised of judges, attorneys, court staff and other stakeholders. Three subcommittees were formed to examine AI's impact on policy, education and customer service. The task force also reviewed court rules to see if "amendments were warranted on account of the intersect of AI and the practice of law."

Bar association leaders reacted positively to the news Wednesday.

Illinois State Bar Association President Sonni Choi Williams Wednesday said in a statement to the Chicago Daily Law Bulletin that the policy was "a proactive step to encourage and facilitate the use of AI by members of the Illinois legal community."

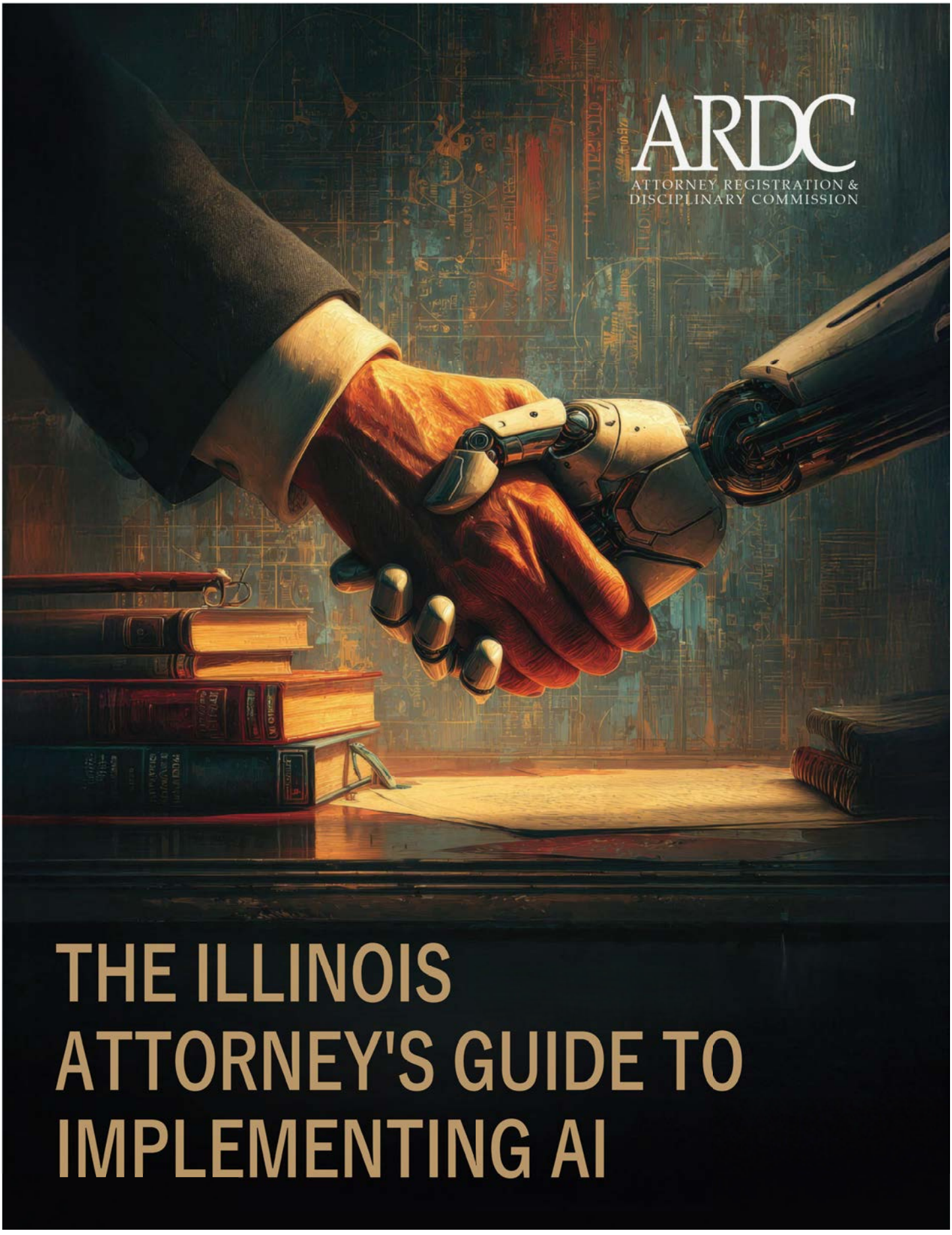
"AI holds great promise to help lawyers practice more efficiently, better serve their clients, and help close the access to justice gap," Williams said in the statement. "Further, I applaud the Court for its determination that existing ethics and court rules will govern the use of AI by lawyers, judges, and litigants."

Appellate Lawyers Association President Catherine B. Weiler said in a statement that the policy was a "reasoned and practical" approach to the use of AI.

"The court has consistently embraced new technology and encouraged its practitioners to do the same, to the great benefit of both the bar and the bench," she said in the statement. "When used properly, AI can be a valuable tool available to parties, practitioners, and judges, as have been other technological innovations like computer-assisted legal research and electronic filing. We look forward to using this new technology in exactly the way described by the supreme court: to enhance work product and promote equitable access to justice for all."

The full policy is available on the Illinois Supreme Court's website.

Practice Areas: Professional Liability



THE ILLINOIS ATTORNEY'S GUIDE TO IMPLEMENTING AI

MESSAGE FROM THE ADMINISTRATOR

As lawyers, we are living in a time of rapid change. Few innovations are reshaping our profession as quickly as artificial intelligence. While these tools hold promise to make our work more efficient and accessible, they also raise new questions about privacy, security, confidentiality, and the exercise of professional judgment. These are not the only considerations, but they are among the most important when it comes to protecting our clients, maintaining trust, and ensuring our work meets the highest standards of the profession.

The ARDC developed this guide to serve as a resource for Illinois lawyers who want to understand and implement AI responsibly in their practices. Designed with solo and small firm practitioners in mind (who may not have the IT support available in larger firms) the information here is useful for lawyers and firms of every size.

This guide complements the Illinois Supreme Court's Policy on Artificial Intelligence and judicial reference sheet. While the Court's policy sets the foundation, this guide focuses on the practical side—helping firms of all sizes apply that framework in daily practice. It includes detailed explanations of how AI systems work. Even if those parts feel technical, they are included so that every lawyer (especially those without dedicated IT staff) has the practical understanding needed to use AI tools safely and ethically.

Our goal is to support you in navigating these changes with confidence. Along with sample policies, forms, and a step-by-step framework, this guide is intended to help you evaluate AI tools, protect client data, and communicate openly with those you serve. No matter the size of your practice or where you are on this journey, you are not alone—ARDC is here as a resource and partner every step of the way.

With respect and support,

Lea S. Gutierrez

The Illinois Attorney's Guide to Implementing AI

Prepared by the Illinois Attorney Registration and Disciplinary Commission (ARDC)[1]
Effective Date: *October 1, 2025*

Contents

Introduction 3
Illinois Supreme Court Policy on Artificial Intelligence 3
The Core Framework 5
What is Generative AI? 5
Side Note: Generative Versus Extractive AI 6
Key Takeaways 7
How to Choose an Appropriate GAI Tool 7
Step 1: Classify the Information to Be Processed 7
Step 2: Categorize the GAI Tool 9
Step 3: Evaluate and Document the Applicable GAI Safeguards 12
Managing Client Rights 18
Key Takeaways 21
Implementing the Practice Resource Kit 22
GAI Terms of Use Checklist 22
Sample Notice of Artificial Intelligence Practices 22
Sample Use of GAI Tools Policy 22
Sample Informed Client Consent Form 23
The Road Ahead 23
Technical Addendum 25
Model Training 25
Conversation and Document Storage 27
Retrieval-Augmented Generation 28
Data Retention Within the Model 28

[1] The primary author of this Guide is Aaron W. Brooks, who contracts with ARDC to serve as its Chief Information Security Officer and primary legal and technical advisor on artificial intelligence. Mr. Brooks is also the Chair of ISBA's Steering Committee on Artificial Intelligence.

Data Retention for Abuse Monitoring 29
Data Isolation 29
Supporting Resources and Materials 31
Appendix 1 Illinois Supreme Court Policy on Artificial Intelligence, together with Judicial Reference Sheet on AI 32
Appendix 2 GAI Terms of Use Checklist 37
Appendix 3 Sample Notice of Artificial Intelligence Practices 38
Appendix 4 Sample Use of GAI Tools Policy 41
Appendix 5 Sample Informed Client Consent Form 46
Appendix 6 Cybersecurity Information Sheet ("CIS") Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems 48

Introduction

The Illinois Attorney Registration and Disciplinary Commission ("ARDC") has completed a careful study of Generative Artificial Intelligence ("GAI") and is pleased to provide this guidance to assist Illinois attorneys in understanding, adopting, and using GAI responsibly. This Guide should be read in conjunction with the Illinois Supreme Court Policy on Artificial Intelligence.[2] If any portion of this Guide is deemed to be inconsistent, the Court's Policy controls.

We recognize artificial intelligence as a transformational technology that, when used carefully, has the potential to streamline legal services, expand access to justice for clients across Illinois, and generally strengthen our profession for many years to come. This Guide is designed to equip lawyers with a foundational understanding of how Generative Artificial Intelligence systems function, what risks they may pose, and how they can be integrated into legal practice ethically and effectively.

Included with this Guide is a Practice Resource Kit that lawyers might consider as a means to help implement GAI tools into their practice. The Practice Resource Kit contains samples, templates, and checklists, including: A sample client notice, a sample staff policy, a sample informed consent form, and a checklist for reviewing GAI terms of service. Lawyers using these resources should do so very carefully to ensure that the language finally used fits the particular situation for which they are implemented. It is not our intent to establish practice standards. These resources are nonbinding, and not Court policy.

Illinois Supreme Court Policy on Artificial Intelligence

On December 18, 2024, the Illinois Supreme Court announced a new Policy on Artificial Intelligence, together with a judicial reference sheet on AI, both of which we reproduce at Appendix 1.[3] We believe the Policy provides a clear foundation for lawyers' responsible use of GAI. It affirms that attorneys may use AI tools, provided they do so in accordance with existing professional obligations.[4] Specifically, the Policy makes four key points:

GAI Use is Authorized. The Policy authorizes the use of artificial intelligence by attorneys, subject to the requirements set forth in the Policy.[5] For those who choose to incorporate one or more GAI tools into their practice, ARDC is fully committed to staying focused on the benefits and risks associated with GAI and providing resources to help them implement GAI in a safe and responsible manner.

Attorney Accountability. Attorneys who use artificial intelligence in their practice must thoroughly review and assume professional responsibility for any AI-generated information that is incorporated into their work

---

[2] Ill. Sup. Ct., *Policy on Artificial Intelligence* (effective Jan. 1, 2025), reproduced in App. 1.

[3] *Illinois Supreme Court Announces Policy on Artificial Intelligence*, Illinois Courts (Dec. 18, 2024), https://www.illinoiscourts.gov/News/1485/Illinois-Supreme-Court-Announces-Policy-on-Artificial-Intelligence/news-detail (last accessed Oct. 9, 2025).

[4] *Policy on Artificial Intelligence*, *supra* note 2.

[5] *Id*. ("The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards.").

product.[6] ARDC maintains a PMBR Self-Assessment program that provides several tips and resources to help manage this core duty.[7] We will continue to provide educational resources to help attorneys apply the Illinois Rules of Professional Conduct to GAI.

Duty of Competence. The Policy requires attorneys who use artificial intelligence tools to understand those tools and ensure that they are secure and legally compliant.[8] This aspect of the Policy echoes the long-standing rule set forth in Illinois Rule of Professional Conduct 1.1 that an attorney's duty of competence extends to the benefits and risks associated with technology.[9]

Privacy and Security. The Policy requires attorneys to confirm that GAI tools maintain the privacy and security of confidential and personally identifiable information. Specifically, the Policy states:

> "*The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.*"[10]

This component of the Policy corresponds to a lawyer's duty to preserve client confidentiality, including the security of any client data in the lawyer's possession.[11] Determining whether a GAI tool is appropriate for handling this type of information can be complex. For that reason, this aspect of the Policy was a central focus in drafting this Guide. We have included policies, checklists, and practical examples to support attorneys in evaluating and implementing GAI tools in a manner that protects sensitive data and complies with legal and ethical obligations.

Accountability, competence, and confidentiality form the essence of a professional and ethical approach to using artificial intelligence in the practice of law. The Court's Policy serves as a clear signal that, while the

---

[6] *Id*. ("The Rules of Professional Conduct and the Code of Judicial Conduct apply fully to the use of AI technologies. Attorneys, judges, and self-represented litigants are accountable for their final work product. All users must thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations.").

[7] Ill. Att'y Registration & Disciplinary Comm'n, *Artificial Intelligence: Benefits, Risks, and Ethical Considerations* (2024), https://pathlms.iardc.org/courses/69187/sections/76987 (last visited June 21, 2025).

[8] *Policy on Artificial Intelligence*, *supra* note 2 ("Prior to employing any technology, including generative AI applications, users must understand both general AI capabilities and the specific tools being utilized.").

[9] Ill. R. Prof'l Conduct R. 1.1 cmt. 8 (2023) ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.").

[10] *Policy on Artificial Intelligence*, *supra* note 2.

[11] Ill. R. Prof'l Conduct R. 1.6 cmt. 18 (2025) ("Paragraph (e) 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.").

Illinois Supreme Court supports the use of GAI, it expects lawyers to exercise judgment, maintain control over their work, and uphold their ethical obligations at every step.

The Core Framework

What is Generative AI?

On June 12, 2017, researchers from Google and the University of Toronto released a groundbreaking paper titled *Attention Is All You Need*, introducing a new type of technology called a *transformer*.[12] This breakthrough is widely regarded as the watershed moment for modern artificial intelligence, and it forms the technological foundation for nearly all AI systems that lawyers are likely to encounter in their daily workflow.[13]

Soon after *Attention Is All You Need* was published, researchers from OpenAI demonstrated that the new transformer technology could be configured to understand and mimic natural human language.[14] They did this using machine learning techniques now commonly referred to as "*model training*" and "*fine-tuning.*"[15] Later in this Guide, we will discuss how model training might threaten client confidentiality and what lawyers should do to mitigate this risk.

These core research efforts formed the basis of what is now commonly known as Generative Artificial Intelligence. The family of GAI tools includes two variations that frequently arise in the practice of law:

- *Large Language Models*, or "*LLMs*", which can quickly generate, interpret, and summarize human language in response to prompts; [16] and
- *Vision Models*, which can generate realistic images and video from basic descriptions or examples, and are often the subject of legal discourse regarding deepfake fraud and evidentiary manipulation.[17]

The term "model" is a very important concept for understanding GAI, because the data processing behind most AI-enabled applications (including tools marketed to the legal industry) is typically performed by one of a few central companies that specialize in building, training, and licensing GAI models.[18] These companies

---

[12] Ashish Vaswani et al., *Attention Is All You Need*, in *Advances in Neural Information Processing Systems 30* 6000 (I. Guyon et al. eds., 2017) (paper presented at the 31st Int'l Conf. on Neural Info. Processing Sys. (NIPS '17)).

[13] John Berryman & Albert Ziegler, *Prompt Engineering for LLMs* (O'Reilly Media, Inc. 2024).

[14] Alec Radford et al., *Improving Language Understanding by Generative Pre-Training* (OpenAI 2018).

[15] Numa Dhamani & Maggie Engler, *Introduction to Generative AI* (Manning Publications 2024).

[16] Edward Raff et al., *How Large Language Models Work* (Manning Publications 2025).

[17] ARDC does not currently recognize a universal term of art for image and video generation models. The term "Vision Models" is used in this Guide in a representative capacity to cover a range of technologies, including diffusion models, vision transformers, and other generative image architectures. For a useful discussion of this area, *see* Amit Bahree, *Generative AI in Action* (Manning Publications 2023).

[18] Suhas Pai, *Designing Large Language Model Applications* (O'Reilly Media 2025) (explaining the broad landscape of models and model providers in Chapter 5).

maintain and update the underlying model architecture, while legal technology vendors integrate those models into products designed for lawyers.

One analogy we find helpful is that of *makes* and *models* in the automotive industry. Automobiles are generally classified by their make, model, and sometimes a trim or body style. For example, Honda (the *make*) produces the Accord (the *model*) which comes in different versions with varying features.[19] GAI producers and their models can likewise be conceptualized this way, as depicted in Table 1 below.

Core Company	Transformer Model	Native Model Platform
OpenAI and Microsoft	GPT	ChatGPT and Copilot
Anthropic	Claude	Claude.ai
Google	Gemini	Gemini
Meta	Llama	MetaAI

Table 1: Table showing major GAI companies, models, and core applications

As you can see, many model producers use their own model to power a native application that is licensed directly by that provider. For example, OpenAI provides the "GPT" branded model for third parties to integrate into their applications, but OpenAI also uses that same model to directly provide various versions of ChatGPT.[20]

Side Note: Generative Versus Extractive AI

Throughout this Guide, we use the term *generative* to refer to the core architecture that underlies almost every modern artificial intelligence application used within the practice of law. The transformer is considered *generative* because it is designed to produce outputs in response to inputs. In some cases, those outputs take the form of new content (such as text or images); in other cases, the outputs may be reformulated queries or summaries that retrieve material from an external data source. However, you may encounter AI discussions that divide AI systems into two basic types: *generative* and *extractive*. We do not view this as a significant distinction, because the terms *generative* and *extractive* are simply descriptions of two functions that the same underlying transformer model might be used to produce.[21] Accordingly, when the terms *Generative Artificial Intelligence* and *GAI* are used throughout this Guide, we mean for those terms to encompass systems which perform both *generative* and *extractive* functions. In short, it's important for lawyers to understand the basic GAI risk assessment that applies to all GAI tools, whether they are acting in a *generative* or *extractive* capacity.

---

[19] *Honda Accord Family, Sedans and Hybrids*, Honda, https://automobiles.honda.com/accord (last visited Sept. 11, 2025).

[20] *See, e.g.*, Schellman & Co., LLC, *Independent Service Auditor's SOC 3 Report for the API and ChatGPT Business Product Services System for the Period of January 1, 2025 to June 30, 2025* (Aug. 7, 2025), https://trust.openai.com.

[21] *See*, Andrew Freed et al., *Effective Conversational AI: Chatbots that Work* (Manning Publications 2025) (explaining that, historically, "extractive" AI referred to classifier-based systems, but modern transformer-based systems can perform both extractive and generative functions within the same architecture); *See also*, Trey Grainger et al., *AI-Powered Search* (O'Reilly Media 2025) (describing how GAI models are used in various search contexts, including extractive, abstractive, and generative search modes).

Key Takeaways

Taking all this together, the key things you should understand from this section are:

- When artificial intelligence is used within the practice of law, it is almost universally focused on the 2017 technology breakthrough called a *transformer*, which is the foundation for Generative Artificial Intelligence.

- Transformers can be understood using a "*make and model*" analogy, whereby AI-focused companies (such as OpenAI and Anthropic) produce various transformer models (such as GPT and Claude).

When lawyers consider whether a particular GAI tool is appropriate for processing various types of information (including confidential or sensitive client information), it's important to understand that this information is being transmitted to, and processed inside, a particular transformer model. Thus, lawyers should know who produces that model, and what privacy and security safeguards are in place.

With that basic understanding in place, let's move ahead to the next section, in which we apply this knowledge to build a framework lawyers might use to evaluate various GAI tools for use in their practice.

How to Choose an Appropriate GAI Tool

Lawyers do not need to become AI experts to use GAI tools effectively, but they do need a structured approach to evaluating the many tools that are available, classifying the type of data these tools will process, and communicating with clients about how GAI may be used to work on their matters.

This section outlines a practical, step-by-step framework that can be adapted to most practice settings. We do not intend this to be mandatory, but we encourage lawyers to adapt this framework to their own practices. The framework is offered as a nonbinding example which, if adapted to a lawyer's specific circumstances, may help document the safeguards required under Illinois Rule 1.6 and support a showing of reasonableness.

Step 1: Classify the Information to Be Processed

It should be clear at this point that not every GAI tool on the market is appropriate for every type of data lawyers may wish to process. Therefore, when selecting a GAI tool, lawyers must first clarify what information they intend to use that system to process. We suggest the following classifications, presented in order of lowest to highest risk:

(a) General Information

If information is entirely unrelated to any matter the lawyer has undertaken professionally, and is otherwise not subject to any confidentiality protections, we consider it "General Information" and assign the lowest level of risk. Examples include using GAI tools for internal technology troubleshooting, generating forms and checklists, drafting marketing content or assisting in writing blog articles.

(b) De-Identified Information

If information relates to the representation of a client, but there is no reasonable likelihood that it could be used to ascertain the identity of the client or matter, we classify this as "*De-Identified Information*." This includes true hypotheticals and other scenarios that satisfy Rule 1.6, Comment [4], which permits discussion so long as the listener could not reasonably identify the client or matter.[22]

When evaluating whether there is a reasonable likelihood that information could be used to ascertain the identity of a client or matter, lawyers should bear in mind that artificial intelligence systems are exceptionally good at detecting patterns and correlations that may allow reidentification of information that appears anonymous to a human.[23] Accordingly, lawyers are encouraged to consider more formal methods of creating De-Identified Information, particularly in sensitive matters.[24] This concern extends beyond direct data entry into GAI tools, because these systems are frequently trained on data scraped from the internet. Similar re-identification risks can arise when lawyers post hypotheticals or case summaries in public forums, blogs, or listservs.

In short, while De-Identified Information carries less risk than identifiable client information, it is not risk-free and should still be managed appropriately when processed by a GAI tool.

(c) Confidential Information

For purposes of this Guide, "*Confidential Information*" means information that is protected by Rule 1.6, or is otherwise subject to confidentiality obligations, but does not contain Sensitive Personal Information as defined below. Confidential Information includes information that relates to the representation of a client that could reasonably be used to identify the client or the situation involved, even if direct identifiers are omitted.

(d) Sensitive Personal Information

For purposes of this Guide, we believe that some types of Confidential Information merit additional protection. In our view, Illinois public policy calls for information that is specifically listed in the Illinois Personal Information Protection Act to be granted additional safeguards.[25] This includes:

- Social Security numbers and tax returns
- Driver's license numbers or state identification card numbers
- Account, credit card, or debit card numbers
- Medical information, including mental health and substance abuse treatment records
- Health insurance information

---

[22] Ill. R. Prof'l Conduct R. 1.6 cmt. 4 (2025).

[23] John X. Morris et al., *DIRI: Adversarial Patient Reidentification with Large Language Models for Evaluating Clinical Text Anonymization*, AMIA Jt. Summits Transl. Sci. Proc. (2025).

[24] *See*, *e.g.,* U.S. Dep't of Health & Human Servs., *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (Nov. 26, 2012).

[25] 815 ILCS 530/5.

- Unique biometric identifiers or biometric information (as defined in Illinois law)
- Passwords and security question/answer pairs
- Any other information meeting PIPA's definition of "personal information," even if separated from a first name or first initial in combination with last name

Whether a lawyer may be required to take additional steps to comply with other laws, such as state and federal laws that govern data privacy, is beyond the scope of this Guide.

Step 2: Categorize the GAI Tool

For purposes of this Guide, we group GAI tools into two main categories: Third-party managed, and self-managed. Each category has distinct implications for confidentiality, security, and client communication. This section describes these broad categories and explains how best to classify any given GAI tool.

(a) Third-Party Managed GAI Tools

A GAI tool is "*third-party managed*" if the essential components of the tool are under the direct control of someone other than the lawyer or the law firm. When a lawyer transmits data to such a GAI tool for storage and processing, that data too becomes within the direct control of the third-party. Architecturally, this hosting and management structure is similar to other cloud-based systems that a lawyer may already use. Nevertheless, these tools introduce unique data processing techniques that are new to the world of cloud-based systems. Accordingly, GAI tools present unique risks above and beyond those associated with traditional cloud systems.

In some descriptions, a GAI tool may be referred to as a "*public*" tool. For purposes of this Guide only, "*public*" means a GAI tool that: (i) is operated and controlled by an entity other than the lawyer or law firm; and (ii) strongly aligns with the public category (discussed further below and illustrated in Table 2). As an illustration, and without endorsing any particular vendor, tools such as ChatGPT have some versions which are public, some that are licensed under consumer-oriented terms of service, and other versions which are licensed under business-class terms of service.[26] This terminology is used solely for the purposes of this Guide and does not constitute legal advice or state the views of the Illinois Supreme Court.

In Step 3 of this section, we outline the main safeguards that should be considered when evaluating third-party managed GAI tools. Before we do that, however, you should clearly understand the difference between two types of third-party managed GAI tools: Native Model Platforms and API Integrations. This distinction matters, because Step 3 applies differently depending on which type of third-party managed tool is being evaluated.

For example, in the case of a Native Model Platform, issues such as model training are addressed directly in the platform's Terms of Use. By contrast, when using an application that integrates with a model provider, the lawyer is not directly involved in selecting the underlying model, and additional research may be necessary to confirm whether appropriate safeguards are in place.

[26] As of the Effective Date of this Guide, the free version of ChatGPT is a "public" tool, while the ChatGPT Plus and Pro versions are consumer-aligned tools.

(1) Native Model Platforms

In a Native Model Platform, all AI processing occurs on infrastructure operated by the model provider itself. Examples include ChatGPT (built and hosted by OpenAI), Claude (built and hosted by Anthropic), and Gemini (built and hosted by Google). The same company (together with subprocessors engaged directly by this company) controls both the transformer model and the hosting environment that stores, transmits, and processes data. Accordingly, a Native Model Platform presents a security tradeoff: Users don't have direct control over how their data is stored and processed, but users also don't have direct responsibility for managing the underlying performance and security of the system. Native Model Platforms may be a practical option for some lawyers if they include safeguards that are appropriate for the type of information being processed.

One variation of this idea is an "*enterprise-walled environment*" whereby a third party is still fully managing the transformer model and the underlying infrastructure that stores and processes data; however, unlike multi-tenant systems like ChatGPT, Claude, and Gemini, the environment is more isolated and controlled by the user. Systems that are set up within the Microsoft Azure OpenAI infrastructure (discussed more in the Data Isolation sections in Step 3 and the Technical Addendum) are good examples of what we mean by "*enterprise-walled environments*." As with Native Model Platforms, enterprise-walled environments present a security tradeoff: Users have more direct control over how their data is stored and processed, but users also take on greater responsibility for managing and maintaining the performance and security of the system.

(2) API Integrations

As depicted below, API integrated applications are typically built using the same underlying infrastructure as Native Model Platforms. Many services with GAI functionality use the same underlying models and model providers to process data.[27]

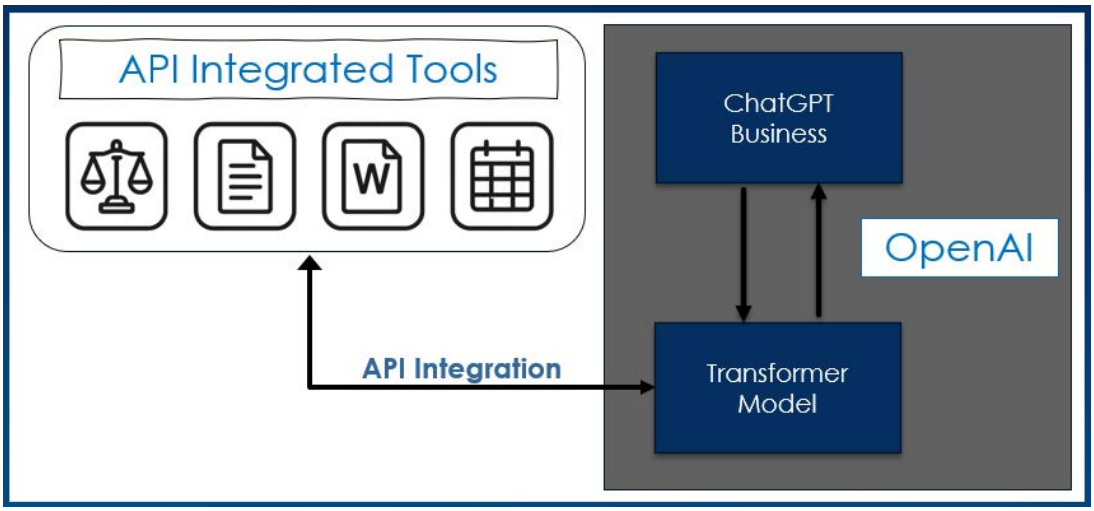


Figure 1: Conceptual illustration of data being sent from various GAI tools to an OpenAI transformer model via API integration.

[27] Schellman, *supra* note 20 (showing that the ChatGPT Enterprise Layer and third-party API users access the same cloud infrastructure).

Any software provider can add AI functionality to their application using a transmission channel called an *Application Programming Interface*, or *API*. When developers connect their software to a model provider's API, they create a two-way communication between your data and one or more underlying transformer model providers (such as OpenAI, Anthropic, or Google).

Distinguishing between the underlying model and the products that integrate these models is important. Lawyers often interact with GAI tools through branded interfaces, but the actual transformer model is typically managed directly by the underlying model provider. For example, consider a PDF application that has an AI feature allowing you to summarize PDF documents. Behind the scenes, that feature most likely works as follows:

- User clicks "Summarize Document"
- The PDF application sends the document content to a model provider (such as OpenAI) using that model provider's API interface
- The model provider processes the document with their transformer model, and sends a summary back to the PDF application
- The PDF application then displays the transformer model's output to the user

Although the user interacts directly with the application, the underlying AI processing occurs on infrastructure controlled by the model provider and is subject to whatever privacy and security assurances are negotiated between the application provider and the model provider. In short, applications with AI integrations may give the appearance of operating in an isolated environment, but this is rarely the case. In most cases, these arrangements simply shift the relationship with the transformer model provider from that of your direct vendor to that of your vendor's subprocessor.

When attorneys evaluate whether a particular GAI tool is suitable for use in their practice, it's essential for them to investigate what model is used to create the artificial intelligence experience. A reputable legal services provider should be transparent about the model vendors they use, and they should make that information readily available to lawyers prior to licensing the product. For example, and without endorsing any specific provider, at the time of this writing Thomson Reuters publicly states of its CoCounsel product: "We process all interactions with OpenAI GPT and Google Gemini in the U.S."[28]

(b) Self-Managed GAI Tools

In a self-hosted environment, the transformer model is downloaded and deployed directly onto hardware or cloud infrastructure controlled by the user. This includes models such as GPT-OSS, Mistral, or Llama, which can be run entirely within a firm's own servers or secure virtual environments, and in some cases directly on a lawyer's own computer. Self-hosted models offer the highest level of control over data storage, processing, and retention, since no information is likely to be transmitted to any third party.

---

[28] *CoCounsel: The Industry-Leading GenAI Assistant for Professionals*, Thomson Reuters, https://www.thomsonreuters.com/en/cocounsel (last visited Oct. 4. 2025).

Self-hosting an AI model provides the greatest degree of control over data handling and system configuration, but it also carries the highest level of technical complexity and security responsibility. Although Step 3 below includes the main GAI safeguards associated with self-hosted models, lawyers who choose to go this route might consider working with qualified technical support to ensure their implementation is supported by a well-documented risk management plan.

Step 3: Evaluate and Document the Applicable GAI Safeguards

At this point in the evaluation process, a lawyer should clearly understand the level of data sensitivity a GAI tool will be used to process, as well as the structural category within which the GAI tool falls. Next, the lawyer should apply the applicable GAI tool safeguards provided in this Step 3 to confirm that the tool is appropriate for the type of data it will be used to process.

Rule 1.6 of the Illinois Rules of Professional Conduct ("*Confidentiality of Information*") is helpful on this point. Specifically, Committee Comment [18] of Rule 1.6 lists five non-exclusive factors that lawyers should evaluate to determine the reasonableness of their efforts to prevent inadvertent or unauthorized disclosure of client confidential information:

1. The sensitivity of the information;
2. the likelihood of disclosure if additional safeguards are not employed;
3. the cost of employing additional safeguards;
4. the difficulty of implementing the safeguards; and
5. the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

Accordingly, as the sensitivity of the data increases, more GAI tool safeguards must be present to make a showing of reasonableness. This is particularly true where the additional safeguards do not create significant additional costs, implementation difficulty, or adverse impacts upon the lawyer's representation.

(a) Third-Party Managed GAI Safeguards

This section describes the main categories of privacy, security, and compliance safeguards to consider when evaluating third-party managed GAI tools, including both Native Model Platforms and API integrations. In the next section, we'll cover the safeguards to consider with self-managed GAI tools.

In Table 2 below, we identify the main risks associated with third-party managed GAI tools and show how those risks are typically addressed at different levels of privacy and security. Some of these safeguards are new and unique to artificial intelligence (such as not allowing Confidential Information or Sensitive Personal Information to be used in training models) while others are long-standing concerns in any cloud-based service. Yet, because GAI tools can process, store, and potentially reuse information in unique ways, even traditional risks can take new forms and deserve renewed scrutiny. Additionally, considering that GAI capabilities are becoming embedded into most technology systems attorneys already use, the approach outlined in this Guide should be applied broadly to most systems that store or process client data, even those which are not obviously "*artificial intelligence*" applications.

We divide third-party managed tools into four broad categories (public, consumer, business, and enterprise), but we acknowledge that specific GAI tools may not fit neatly within one category. The takeaway is that tools aligned with public and consumer-aligned safeguards are less likely to be appropriate for processing confidential or sensitive personal information, and tools aligned with the business or enterprise safeguards are preferable.

GAI Safeguard	Public	Consumer	Business	Enterprise
Authentication User identity verification and access control mechanisms	Open	Basic	Secure	SSO
Model Training Use of customer data to improve current and future models	Required	Opt-Out	Prohibited	Prohibited
Data Retention User data storage, retention policies, and deletion procedures	Perpetual	Platform-Defined	User-Defined	Admin-Defined
Data Isolation Separation and protection of customer data and workloads	Undefined	Noncommittal	Logical Separation	Dedicated
Supply Chain Risk Third-party dependencies, vendor security, and supply chain integrity	Undefined	Noncommittal	Transparent	Regulated
AI Risk Management AI governance, safety controls, and responsible AI practices	Undefined	Noncommittal	Industry-Standard	Framework-Based
Security Risk Management Information security controls, threat detection, and incident response	Undefined	Noncommittal	Framework-Based	Framework-Based
Terms of Use Legal agreements, service terms, and contractual protections	Pro-Platform	Consumer-Grade	Business-Class	Business-Class+

Table 2: Classification of GAI Tools by Safeguards

We recommend lawyers focus on technical fundamentals over broad labels. Don't make security assumptions based on whether a GAI tool is licensed as a free or paid version or is marketed as a consumer or business version. For example, you might find a GAI tool that allows model training by default (making it more aligned with the consumer-level safeguards in Table 2) but also allows users to opt-out of model training (changing it to be more aligned with the business-level safeguards in Table 2). It is the actual safeguards, and not the marketing label, that matter most when protecting client information.

(1) Authentication

Authentication refers to the security measures that protect the login process for a third-party managed GAI tool. As illustrated in Table 2, a public GAI tool typically provides no controls (for example, the public version of ChatGPT can be used by anyone with an internet connection and does not require creating an account or logging in). Consumer-aligned tools typically allow users to create individual accounts but may lack advanced protections such as multi-factor authentication. Business-aligned tools should require multi-factor authentication, while enterprise-aligned tools usually offer more sophisticated account-management capabilities, such as single sign-on (SSO).

(2) Model Training

As a general rule, lawyers should not transmit Confidential Information or Sensitive Personal Information to a GAI tool that permits the information to be used for model training. Security researchers have demonstrated serious data security risks when classified information is used to train models.[29] For example, in one widely discussed study, researchers demonstrated the ability to retrieve verbatim copies of personally identifiable information from an early OpenAI model even when the information was included in only one document in the training data.[30]

The indicators in Table 2 show that public GAI tools require users to consent to model training, while tools aligned with the consumer category typically allow users to opt-out of model training. GAI tools that are more closely aligned with the business and enterprise categories will have model training turned off by default and include contractual assurances that customer data will not be used for this purpose. In the Technical Addendum included with this Guide, we provide more details for how model training works and discuss potential narrow exceptions to the general rule against allowing Confidential Information to be used to train models.

(3) Data Retention

Lawyers should investigate how long the GAI tool retains information, both after the lawyer deletes it from the user interface and after the service itself is terminated. The ideal data retention setting for GAI tools is "*Zero Data Retention*," meaning that a lawyer's information is never retained by the underlying transformer model, and it is permanently removed from the provider's servers immediately after the lawyer deletes the data from the user interface.[31] Some GAI tools, despite being licensed as business-class tools and being subject to business-class privacy and security assurances, do not support Zero Data Retention, and therefore may be inappropriate for processing Sensitive Personal Information (especially without informed client consent).[32] Table 2 shows the retention policies for public and consumer aligned GAI tools are typically defined by the third-party provider, and users have limited or no control over how long their data is stored or when it is deleted. By contrast, business and enterprise aligned tools provide these controls directly to the users or organizational administrators.

Lawyers who use GAI tools to process Confidential Information or Sensitive Personal Information should understand that these tools retain data in multiple layers, and each layer might have its own retention

---

[29] Nat'l Inst. of Standards & Tech., *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1) (July 2024), https://doi.org/10.6028/NIST.AI.600-1.

[30] Nicholas Carlini et al., *Extracting Training Data from Large Language Models*, in *Proceedings of the 30th USENIX Security Symposium* 2633 (USENIX Ass'n 2021), https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting.

[31] *See Vertex AI and Zero Data Retention*, Google Cloud, https://cloud.google.com/vertex-ai/generative-ai/docs/data-governance (last visited Sept. 14, 2025) (providing a detailed discussion of Zero Data Retention applied to GAI tools).

[32] *See How We're Responding to The New York Times' Data Demands in Order to Protect User Privacy*, OpenAI (June 5, 2025), https://openai.com/index/response-to-nyt-data-demands (last visited Sept. 14, 2025) (describing OpenAI's various data retention capabilities for public, consumer, and business-class versions in response to the Preservation Order entered in *In re OpenAI, Inc., Copyright Infringement Litigation*, No. 25-md-3143 (S.D.N.Y. 2025)) (referencing *In re Openai, Inc.*, 2025 U.S. Dist. LEXIS 97943 (S.D.N.Y. Mar. 13, 2025)).

settings. We've included a more detailed discussion of layered GAI data retention in the Technical Addendum included with this Guide.

(4) Data Isolation

The level of data isolation in a GAI tool determines how closely your data is stored with that of unrelated third parties. Vendors who misconfigure their data isolation settings might expose sensitive information and allow unauthorized access to customer-specific data or resources.[33] As the sensitivity of the information being processed by a GAI tool increases, so too should the level of data isolation. Lawyers who use GAI tools to process Confidential Information or Sensitive Personal Information should document the isolation settings for those tools. To help with this, we've included a more detailed discussion of how data isolation works in the Technical Addendum included with this Guide. As shown in Table 2, a GAI tool that is aligned with the public and consumer categories typically provides only basic, and therefore higher-risk, forms of customer isolation. Business and enterprise aligned tools are built with stronger isolation, such as independently audited logical separation or customer-dedicated environments.

(5) Supply Chain Risk

GAI tools often rely on a network of downstream service providers that may process, store, or transmit the data you send to the system. Each subprocessor should apply administrative and technical safeguards appropriate to the sensitivity of the data. Lawyers should identify all subprocessors involved in providing and maintaining the GAI tool, evaluate whether their access to client data is necessary and proper, and confirm that each is bound by confidentiality and security obligations through contractual flow-down provisions. Table 2 describes public and consumer-aligned GAI tools as having few, if any, supply chain safeguards or published details about their supplier ecosystem. Business-aligned tools tend to provide full transparency for the privacy and security practices of its downstream vendors. Enterprise-aligned tools may also provide regulation-level supply chain protection (such as HIPAA Business Associate Agreements that address specific regulatory requirements for downstream providers).

(6) AI Risk Management Frameworks

Reputable GAI tool providers should publish or directly provide written assurances that they design, maintain, and test their models in accordance with recognized risk management frameworks.[34] These frameworks address areas such as data governance, security controls, bias mitigation, transparency, and incident response. By aligning with these standards, providers demonstrate that their systems have been evaluated against widely accepted criteria for safety, reliability, and trustworthiness. Lawyers should request documentation of the provider's risk management practices and confirm that those practices remain aligned with these evolving frameworks. This is an area in which industry standards and official frameworks are not yet well established; accordingly, our Table 2 designations should be understood to illustrate that

---

[33] *Multitenancy and Azure OpenAI Service*, Microsoft Learn (May 13, 2025), https://learn.microsoft.com/en-us/azure/architecture/guide/multitenant/service/openai (last visited Oct. 7, 2025).

[34] Examples include the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF) and the Open Worldwide Application Security Project (OWASP) GenAI Security Project.

business and enterprise level GAI tools have more formally documented AI risk management controls that reference independently and globally established baselines.

(7) Security Risk Management

As discussed throughout this Guide, many components of a GAI tool are not unique to artificial intelligence, and are in fact traditional network storage, transmission, and processing functions. Like any other cloud-based system, a hosted GAI tool should demonstrate compliance with established data privacy and security standards.[35] Providers that follow these standards help ensure that the underlying infrastructure supporting AI functions meets accepted industry benchmarks for confidentiality, integrity, and availability of data. Unlike AI risk management, cloud security risk management is supported by numerous mature and well-established security frameworks. To be properly within the business or enterprise categories of Table 2, a GAI tool provider should publish formal, written, and independently verified audits demonstrating compliance with the security frameworks referenced in this Guide.[36]

(8) Terms of Use

When selecting a GAI tool, lawyers should obtain written contractual assurances covering the provider's privacy and security obligations. These assurances should address both the underlying transformer model provider and the application itself. Written commitments are necessary to ensure that the handling of client data complies with professional duties of confidentiality, applicable privacy laws, and agreed security practices. You may notice in Table 2 that we designated the enterprise level to provide "Business-Class+" Terms of Use. The *plus* symbol is meant to convey that enterprise licenses typically provide customer-specific negotiating flexibility and additional safeguards for regulated data (such as a HIPAA Business Associate Agreement or GDPR-compliant Standard Contractual Clauses). We've also included a GAI Terms of Use Checklist at Appendix 2 for lawyers to consider when licensing third-party managed tools.

In addition to these key safeguards, lawyers might also consider where their GAI tools physically store and process data (including conversations, documents, and other elements of GAI storage as discussed in more detail in the Technical Addendum). The physical location of these operations can significantly affect the protections afforded to that data, and the circumstances under which the data can be accessed or deleted. Processing location could also impact the contractual or regulatory obligations lawyers may have with respect to data provided by clients.

(b) Self-Managed GAI Safeguards

Lawyers who choose to deploy a self-managed GAI tool assume responsibility, not only for client confidentiality, but also for the full range of security, availability, and compliance risks associated with hosting and operating the transformer model and its ancillary support structure. To assist in that process, we recommend consulting the Cybersecurity Information Sheet ("CIS") titled *Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems,* authored by the U.S. National Security Agency's

[35] These may include, for example, SOC 2, CSA STAR, ISO 27001, GDPR, CCPA, and other globally recognized privacy and security frameworks.

[36] *Id*.

Artificial Intelligence Security Center, the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the Australian Signals Directorate's Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the New Zealand National Cyber Security Centre, and the United Kingdom's National Cyber Security Centre. [37]

A comprehensive discussion on self-managed GAI tools is beyond the scope of this Guide. However, in addition to providing the CIS in Appendix 6, we summarize below several of the most important safeguards for those lawyers who are interested in deploying a self-managed GAI tool to consider:

- Deployment Environment Security: Self-managed tools must run in a hardened environment. Firms are responsible for applying secure configurations, enforcing strong access controls, segmenting networks, and adopting defense-in-depth practices across the entire deployment.

- Supply Chain and Model Integrity: Open-weight models and external data sources must be carefully validated. Law firms should confirm the digital integrity of key transformer components and maintain version control to protect against tampered or malicious models. For example, we are aware of incidents in which malicious models were downloaded from widely used distribution sites.[38]

- Model Weight Protection: The trained "weights" of a self-hosted model are highly sensitive. Lawyers must ensure that weights are stored securely, access is restricted to essential personnel, and exposure through APIs is minimized to reduce risks of exfiltration or inversion attacks.

- Monitoring and Incident Response: Self-managed deployments require continuous monitoring for anomalies and suspicious activity. Law firms or their outsourced IT providers should maintain logs, alerting systems, and a documented incident response plan that supports isolation, patching, and rollback of compromised systems.

- Data Protection and Secure Deletion: When no external provider manages storage, the firm is directly responsible for encryption, secure key management, and verified deletion of data, logs, and training inputs when no longer needed.

- Patching and Updates: Self-managed GAI tools require regular updates and security patches, both for the application itself and the underlying hardware or cloud environment. Before deployment, firms should also test whether their systems can be restored quickly and securely if something goes wrong.

Lawyers using self-managed systems may use the safeguards in the Cybersecurity Information Sheet (CIS, Appendix 6) to assess whether a system is appropriate for each information classification (Table 2) and to guide client communications (Table 3). The following non-binding examples show one way to document that approach:

---

[37] Nat'l Sec. Agency Artificial Intelligence Sec. Ctr. et al., *Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems* (Apr. 2024).

[38] N.J. Cybersecurity & Commc'ns Integration Cell, *Hugging Face AI Platform's Problem with Malicious AI* (Mar. 7, 2024), https://www.cyber.nj.gov/Home/Components/News/News/1216/214 (last visited Sept. 13, 2025).

- Enterprise-aligned. Professionally deployed; governed by written policies and procedures; periodic, framework-based security risk assessments that expressly address a self-managed GAI deployment (see CIS, Appendix 6).

- Business-aligned. Managed by individuals reasonably skilled in GAI deployment, system administration, and security configuration; uses business-class hardware, operating systems, and applications; employs prudent safeguards (e.g., strong authentication, encryption, regular updates); may lack a formal written security program or independent assessments.

- Consumer-aligned. Operated by individuals with limited security and administration experience; relies on default settings; lacks rigorous access controls or encryption; often uses personal-grade hardware/software not intended for client information.

These examples illustrate a method to evaluate and document how client information is processed and how client communications are managed in a self-managed environment.

In summary, while self-managed GAI tools avoid the risk of allowing a third-party to process and store client data, they also carry the heaviest operational burden. Firms that choose this path must be prepared to treat the GAI tool as part of their critical infrastructure, subject to the same rigor as their other on-premise servers and related network equipment. With the right planning, governance, and support, self-managed GAI tools can be a safe and effective option for processing highly sensitive client information, but they are not risk free.

Managing Client Rights

By this point, you should have a basic understanding of how GAI tools work, and you should be capable of choosing appropriate GAI tools for all types of data we've discussed, including Confidential Information and Sensitive Personal Information. The next important idea is how best to communicate with clients when using GAI tools to process their matters, Confidential Information, and Sensitive Personal Information.

Taken as a whole, the approach presented in this Guide is a notice and opt-out paradigm, with enhanced protection for highly sensitive information. There are analogous examples within Illinois public policy. In the context of health information exchange systems, for example, the Illinois Health Information Exchange Authority determined that a notice and opt-out system would afford patients a greater degree of choice without the relatively burdensome documentation requirements of a more formal patient-by-patient consent system.[39] While not directly applicable to the use of GAI tools and the practice of law, the relationships described in this report (between technology, healthcare providers, and patients) parallel the relationships between artificial intelligence, lawyers, and their clients.

Client communication, including client notice, client opt-out rights, and informed client consent, should be understood as an additional safeguard that a lawyer might employ when using GAI tools, and not as a method of shifting risk from the lawyer to the client. In other words, lawyers must be reasonable when selecting and

[39] Ill. Health Info. Exch. Auth., Data Sec. & Privacy Comm., *Report of Preliminary Findings and Recommendations* (Sept. 19, 2012).

using GAI tools to process their data and simply obtaining a client's consent cannot be used as a substitute for the due diligence we've outlined throughout this Guide.

The non-exclusive considerations identified in Comment [18] to Illinois Rule of Professional Conduct 1.6 remain relevant when evaluating the use of GAI tools:

1. The sensitivity of the information;
2. the likelihood of disclosure if additional safeguards are not employed;
3. the cost of employing additional safeguards;
4. the difficulty of implementing the safeguards; and
5. the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

Although Comment [18] predates modern GAI tools, lawyers can still use its technology-neutral balancing test to determine what safeguards are appropriate when using GAI tools, including providing notice and opt-out rights, or, in appropriate cases, seeking informed client consent.

The table below shows one example of how a lawyer might use the GAI categories we reviewed in Step 3 above (public, consumer, business, and enterprise) to determine how best to manage client communications for different levels of information sensitivity. They are not endorsements and do not constitute legal advice.

Data Classification	Public	Consumer	Business	Enterprise
General Information Non-confidential information entirely unrelated to any client matter	Unrestricted	Unrestricted	Unrestricted	Unrestricted
De-Identified Information No reasonable likelihood of identifying the client or matter	Consent	Opt-Out	Opt-Out	Unrestricted
Confidential Information Information protected by Rule 1.6, but without Sensitive Personal Information	Prohibited	Consent	Opt-Out	Opt-Out
Sensitive Personal Information Highly sensitive data including PII, PHI, or other regulated personal data	Prohibited	Prohibited	Consent	Opt-Out
System-Wide Processing GAI systems used in firm-wide administrative, security, or operational functions	Prohibited	Prohibited	Prohibited	Notice Only

Table 3: Relationship between data classification, GAI tool classification, and client communication strategy

In this example, the lawyer has determined that General Information (which we defined in Step 1 as information that is entirely unrelated to any matter the lawyer has undertaken professionally and is otherwise not subject to any confidentiality protections) does not require any client communication regardless of the level of safeguards incorporated into the GAI tool. Despite the fact that no client information is being processed, the lawyer should still exercise caution when entering information into a public GAI tool due to the absence of privacy and security safeguards.

With respect to De-Identified Information (which we defined in Step 1 as information that relates to the representation of a client, but for which there is no reasonable likelihood that it could be used to ascertain the identity of the client or matter), the lawyer has determined that clients should receive reasonable notice

and opt-out rights when this information will be processed by a consumer or business-class tool, but that an enterprise-grade tool has sufficient safeguards to allow unrestricted processing. By contrast, even if the lawyer determines it is reasonable to process De-Identified Information using a public tool, informed client consent is still advised prior to doing so.

With respect to Confidential Information (which we defined in Step 1 as information that is protected by Rule 1.6, or is otherwise subject to confidentiality obligations, but without Sensitive Personal Information), the lawyer has determined that it cannot be processed using a public GAI tool under any circumstances, but that business-class and enterprise-grade tools provide sufficient safeguards to allow processing with only notice and opt-out rights. In Step 2, we defined "public" to mean GAI tools that are operated and controlled by a third party and strongly aligned with the public category shown in Table 2. A lawyer might reasonably determine that Confidential Information can be processed using a consumer-aligned tool if the available security options described in Table 2 are enabled (such as, for example, opting out of model training) and informed client consent is obtained as an additional safeguard.

With respect to Sensitive Personal Information (which we defined in Step 1 to include highly sensitive elements such as medical records and financial accounts), the lawyer has determined that it cannot be processed using a public or consumer GAI tool under any circumstances. The lawyer has also determined that informed written consent should be obtained prior to processing this information using a business-class GAI tool that has not fully incorporated all the enterprise-level safeguards described in Table 2.

Clients and lawyers should also understand that certain types of GAI processing, described in Table 3 as "System-Wide Processing," may be difficult or infeasible to disable. For example, if a major cloud platform (like Microsoft 365) begins actively incorporating GAI functionality into its basic computational structure, the law firm's entire data repository could be subject to GAI processing, even involving Sensitive Personal Information. Clients should still be made aware that this processing happens, but there might not be a clear path for them to opt out. In these cases, and again using the five factors set forth in Rule 1.6, Committee Comment [18], a lawyer might conclude that even though the sensitivity of the information is high (factor 1), the difficulty of allowing opt-out rights for systemic AI processing (factor 4) and the extent to which allowing opt-out rights will adversely affect the lawyer's ability to represent clients (factor 5) are too high. In such a case, the lawyer might choose to focus on reducing the likelihood of disclosure (factor 2) by allocating more resources to employing additional safeguards (factor 3). In that case, the lawyer should ensure that the tools used for system-wide processing are closely aligned with the enterprise-level safeguards shown in Table 2.

Rule 1.6 references informed consent in two different contexts, and the distinction is useful when managing GAI-related client conversations. Rule 1.6(a) states that lawyers may not "reveal information relating to the representation of a client unless the client gives informed consent." This has not typically been interpreted to require informed consent when lawyers process client information through a third-party vendor, and it seems plausible that this understanding should continue in the context of third-party managed GAI tools.[40] However, Committee Comment [18] to Rule 1.6 also states: "A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures

[40] *See*, *e.g.*, Ill. State Bar Ass'n, Prof'l Conduct Advisory Op. No. 16-06 (2016). ("A lawyer's use of an outside provider for cloud-based services is not, in and of itself, a violation of Rule 1.6, provided that the lawyer employs, supervises and oversees the outside provider.").

that would otherwise be required by this Rule." This latter use is particularly relevant to discussions about client notice, opt-out rights, and use of informed consent as an additional safeguard.

We align with the American Bar Association's view that, where client consent is required, it must be informed.[41] This Guide focuses on implementation; lawyers retain professional judgment, consistent with Rules 1.4 and 1.6, to determine the nature and extent of client communication appropriate to the particular engagement and the type of data processing contemplated. To support that judgment, this Guide offers a Sample Notice of Artificial Intelligence Practices (Appendix 3) that firms may adapt for use in engagement materials or on firm websites. Firms may also designate a knowledgeable point of contact for AI-related client inquiries; depending on the firm's structure, this may be a lawyer or a non-lawyer (e.g., a vendor or outsourced IT professional), subject to confidentiality and supervision obligations. Where more extensive AI processing or Sensitive Personal Information is involved, enhanced matter-specific explanations and informed written consent may be prudent.

Key Takeaways

Summarizing everything we've discussed in this Section:

- The baseline for our hypotheticals and sample forms is that of a GAI tool aligned with the business category in Table 2. When using such a tool to process information that is classified no higher than Confidential Information (as defined in Step 1 of the Core Framework), lawyers are encouraged to provide clients with notice and a right to opt out. A sample notice form provided at Appendix 3.
- When processing Sensitive Personal Information, lawyers are encouraged to incorporate additional safeguards, such as those aligned with the enterprise category in Table 2 and/or seeking informed client consent. A sample informed consent form is provided in Appendix 5.
- Lawyers should exercise caution when using GAI tools that align with the public or consumer category in Table 2, even for De-Identified Information. Where a lawyer reasonably determines that such a tool is appropriate for limited use, it is generally prudent to also obtain informed client consent.
- As GAI becomes more integrated into our computers and applications, Lawyers and clients should understand that it may become infeasible to disable some GAI features. In such cases, lawyers are encouraged to focus on enterprise-aligned safeguards, where possible, to offset the infeasibility of providing clients with opt-out or consent rights.

We recognize that these concepts are evolving rapidly, and we do not expect lawyers to become artificial intelligence experts or dedicate extensive research to mastering every nuance in the universe of artificial

[41] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 512 (July 29, 2024) (addressing Generative Artificial Intelligence tools) ("When consent is required, it must be informed. For the consent to be informed, the client must have the lawyer's best judgment about why the GAI tool is being used, the extent of and specific information about the risk, including particulars about the kinds of client information that will be disclosed, the ways in which others might use the information against the client's interests, and a clear explanation of the GAI tool's benefits to the representation.").

intelligence technology. Rather, the intent is to highlight reasonable considerations lawyers might apply in evaluating GAI tools consistent with their existing professional responsibilities. Lawyers should use informed judgement in selecting and monitoring GAI tools, provide clients with appropriate information when their data may be processed using such tools, and remain attentive to client questions or concerns about these emerging technologies.

Implementing the Practice Resource Kit

To help lawyers document the various ideas presented throughout this Guide, we are providing a "Practice Resource Kit." These materials are based on a hypothetical law firm named "ACME Law, LLC" and reflect a set of decisions and risk assessments that this hypothetical small firm has undertaken. Lawyers using these resources should do so very carefully to ensure the language finally used fits the particular situation for which they are designed. It is not the intent of these resources to suggest or establish practice standards. The following is a brief summary of each component of the Practice Resource Kit.

GAI Terms of Use Checklist

The GAI Terms of Use Checklist, included as Appendix 2, is designed to help lawyers evaluate whether a provider's contract terms adequately address the safeguards described in this Guide. It distills the key legal, ethical, and technical considerations into a practical review tool that can be applied when negotiating or reviewing agreements with GAI vendors. The checklist is not mandatory and does not constitute legal advice; lawyers are encouraged to adapt it to their own practice needs and the sensitivity of the data they intend to process.

Sample Notice of Artificial Intelligence Practices

The Sample Notice of Artificial Intelligence Practices is attached as Appendix 3. We encourage lawyers and law firms to document their own risk assessments and decision-making processes when applying the GAI safeguards and making determinations about how to manage client communications. For example, lawyers might consider using the sample methodology provided in Table 2 and Table 3 above to document their selection of GAI tools and their corresponding client communication strategy.

Sample Use of GAI Tools Policy

The Sample Use of GAI Tools Policy is intended to provide an example of the type of written policy that lawyers and law firms might use to ensure everyone in the firm is aligned about their responsibilities when using artificial intelligence. The Policy is designed to be distributed to everyone in the firm, including lawyers, staff, paralegals, and other individuals who have access to the firm's resources.

The Sample Use of GAI Tools Policy assumes that a lawyer or law firm has already worked through the analysis outlined in the Core Framework section of this Guide and has selected appropriate GAI tools that will be made available to the workforce. Those tools are called "Approved GAI Tools" and should be listed on a Schedule of Approved GAI Tools as described in the Policy. The Sample Use of GAI Tools Policy also provides guidance for managing client rights and communications. Finally, the Policy is meant to address several other

ethical obligations that lawyers should observe when using GAI tools, such as retaining professional responsibility for GAI tool output, avoiding hallucinations, and candor towards the tribunal.

Sample Informed Client Consent Form

As discussed throughout this Guide, there may be times when lawyers and law firms determine it is necessary or prudent to obtain informed client consent prior to using a GAI tool to process the client's information or matters. To assist with that process, we provide a Sample Informed Client Consent Form that lawyers and law firms might adopt for their own use.

In reviewing this sample form, we suggest lawyers reference the definition of informed consent provided in Rule 1.0(e). We also recommend considering the Federal Trade Commission's approach to "Affirmative Express Consent", which focuses on providing clear notice of the types of information to be processed and the purpose for which it's being used.[42]

Note also, as outlined in Section 6(d) of the Sample Use of GAI Tools policy, clients must have the authority to provide consent to all the personal information a lawyer intends to process using its GAI tools. Thus, if the data includes Sensitive Personal Information of separate third parties, it may be prudent to inquire whether the client possesses this authority.

The Road Ahead

Artificial intelligence changed almost daily as this Guide was written. Rather than attempting to track every change, we have focused on core principles that are likely to remain constant as GAI becomes more deeply embedded in the practice of law. Our aim is to help lawyers adapt thoughtfully, regardless of which new tools, models, or regulations emerge in the months and years ahead.

For example, we believe the fundamental concept of the transformer model as expressed in the *Attention Is All You Need* research paper is likely to persist as a bedrock algorithm throughout the foreseeable development of GAI-powered legal applications. We also believe transformer models will continue to be utilized via the basic pathways we've described in the Core Framework section (Native Model Platforms, API integrations, and self-managed downloadable GAI models).

Still, we see new implementations of these basic concepts emerging quickly. For example, as this Guide is being written, "*agentic*" AI systems are starting to become mainstream. Agentic systems have the ability to access information on their own and take action directly. For example, we're not far from a future in which lawyers can instruct their AI agents to book a trip out of town and reliably expect the agent to review the available flight and hotel accommodations, choose the best room and flight, and then book the trip directly.[43] Clearly, this level of access and autonomy will raise a variety of novel risks; accordingly, we intend to track these developments closely and update the Guide regularly.

---

[42] *In re X-Mode Social, Inc. & Outlogic, LLC*, Docket No. C-4802 (F.T.C. 2023).

[43] Anjanava Biswas & Wrick Talukdar, *Building Agentic AI Systems* (Packt Publishing 2025).

Our working view is that, when used with appropriate safeguards, artificial intelligence can strengthen legal practice, including for solo and small firms. Lawyers should continue to exercise diligence, care, and adaptability. Prudent practices include remaining curious, applying appropriate safeguards, documenting decisions, and maintaining meaningful human oversight.

We look forward to taking this journey together and supporting you along the way.

Technical Addendum

In the main body of this Guide, we presented the Core Framework for evaluating GAI tools for use with different levels of data sensitivity. That framework is sufficient to responsibly choose and implement GAI tools in most legal practices. However, some lawyers may wish to explore these issues in more detail (particularly when considering tools that will store or process highly sensitive or regulated data).

This Technical Addendum illustrates how typical GAI systems work and provides a deeper analysis of key GAI safeguards that comprise the Core Framework. The concepts outlined here apply broadly to most GAI tools, including ChatGPT, Claude, Gemini, Copilot, and many AI-driven legal industry tools. At a high level, these systems share the same essential building blocks; thus, understanding this model can help lawyers more easily evaluate and compare the tools they are likely to encounter in practice.

Figure 2 illustrates the major components of a typical GAI system:

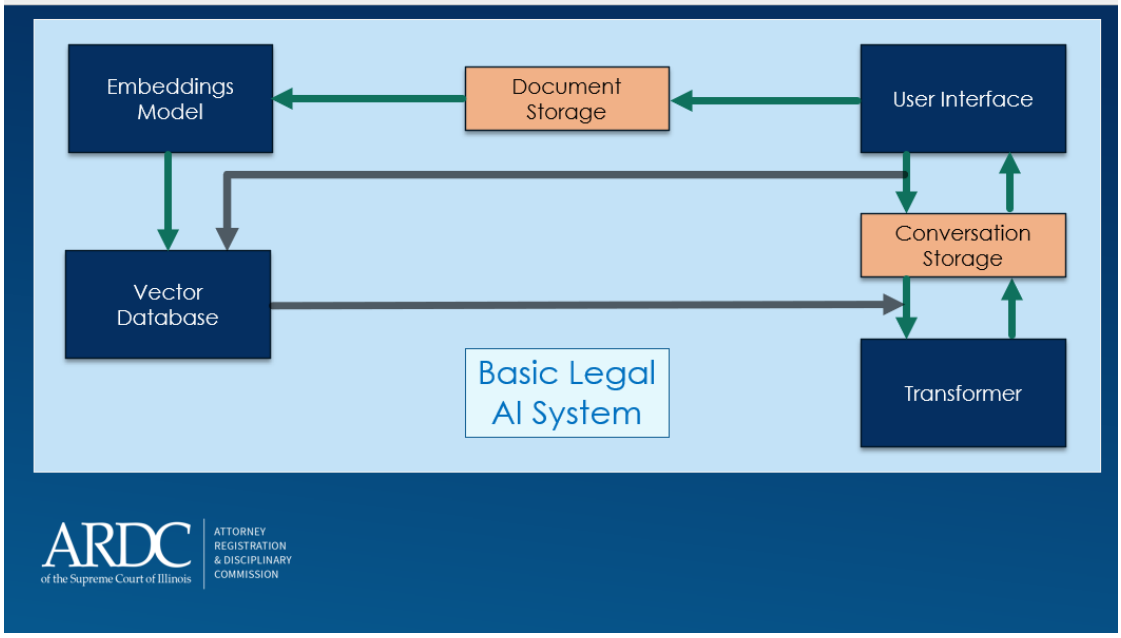


Figure 2: Functional Diagram of a Basic Legal AI System. This model shows how user prompts interact with stored documents and conversation history, using embeddings, retrieval augmented generation, and a transformer-based language model to generate responses.

Most of the lawyer's experience takes place in the user interface, which is where we log into the application, manage settings, engage in AI conversations, and upload documents for use within the GAI tool. Behind the scenes, however, there's a lot going on.

Model Training

The Core Framework introduced the transformer model and explained why it is the essence of any GAI tool. We also cautioned lawyers about the risks associated with model training and identified the ability to disable model training as a principal safeguard for protecting client information.

Training is the method by which a model provider sets the "weights" or "parameters" of the transformer models they produce. Think of a model weight like a pre-set multiplier that is used to process any kind of input that a human user might provide. Figure 3 provides a visual representation to help conceptualize this idea.

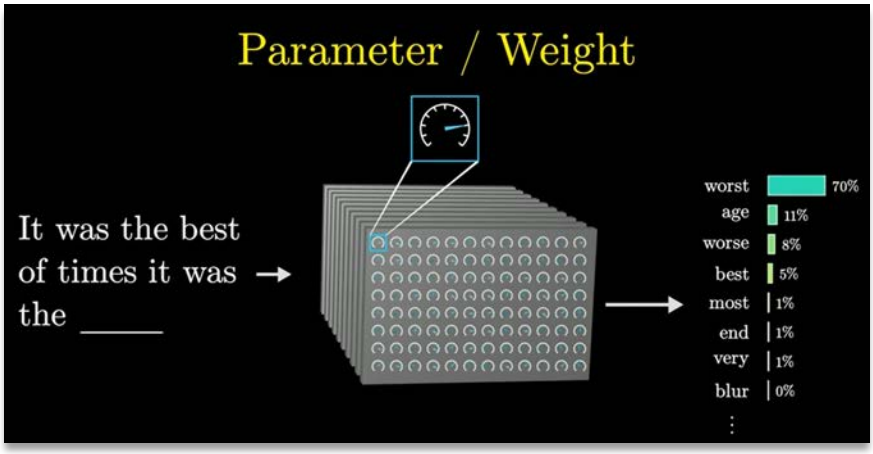


Figure 3: Conceptualization of transformer model weights being set during training. Image courtesy of 3Blue1Brown.com.

LLMs work by multiplying the numeric values of input text against a set of "weights" or "parameters" that are set while a model is being built.[44] This weighted multiplication operation happens each and every time a new word[45] is processed by the model, resulting in the entire vocabulary of the model being ranked from most to least likely as the next appropriate word.[46] In the specific example depicted in Figure 3, the model has ranked the word "*worst*" as the most likely next word, because its numeric weights produced that outcome when multiplied through.

Before a model is trained, its internal numeric weights are initialized with no patterns at all, effectively just random numbers.[47] Thus, if you ask an untrained model to finish the sentence "It was the best of times it was the _____", the untrained model is likely to respond with randomly selected words from its default vocabulary such as "It was the best of times it was the lorem ipsum."

In simple terms, a large language model (LLM) is trained by providing it with a large body of pre-existing text, one word at a time, and directing it to guess each successive word before it is revealed. If the model guesses correctly, that outcome is reinforced. If it guesses incorrectly, its internal weights are adjusted to

[44] Jay Alammar & Maarten Grootendorst, *Hands-On Large Language Models* (O'Reilly Media 2024).

[45] Technically, the term is "*tokens,*" but we have opted to reduce the use of technical terms in this Guide to promote readability.

[46] Alammar & Grootendorst, *supra* note 44.

[47] Andrew Glassner, *Deep Learning: A Visual Approach* (No Starch Press, June 2021) (explaining that neural network training begins with random weights, producing meaningless output until adjusted through learning).

reduce the error.[48] As this process continues across millions and millions of words, the weights become increasingly precise, and the model's output begins to sound more like the data it was trained on.[49]

Conversation and Document Storage

GAI tools are typically built around traditional storage systems that are not significantly different from any other cloud-based service. In most GAI tools, these databases hold conversation history, documents, and other interactions with the system. We've illustrated these components in Figure 2 above using orange shading. Following the flow shown in Figure 2, the user might enter text or a document into the user interface (such as, for example, asking ChatGPT a question). That text or document is then formatted into an AI-compatible form and sent to the transformer model to be processed. The transformer returns a human-readable response. The combination of the user's input (or "*prompt*") and the transformer's output now forms a conversation which is stored in the same type of cloud storage that any other text-based information might be stored.

Retention settings for these databases determine how long content remains accessible after a user deletes it, and how long it is retained after an account is closed. Deleted items may also remain in backup storage for weeks or months before being permanently removed, depending on the provider's policies.[50]

Based on our review of several major model providers, deleted conversations are generally removed from the provider's systems within a fixed period (often about 30 days). Enterprise-grade systems may offer additional protection, such as:

- Administrative controls that allow the organization to set retention limits for conversations, removing this discretion from individual users;
- Account configurations that give the customer direct, unilateral control over storage areas holding documents, conversation history, and other model outputs; and
- Encryption of traditional storage containers at rest within the provider's platform.

Because the traditional database layer often contains the most complete record of a user's interactions with the GAI tool, it is critical for lawyers to determine whether these retention periods and controls are appropriate for the sensitivity of the data being stored.

There are a few reasons we feel that lawyers should understand the distinction between AI components and traditional storage and networking components. First, having this understanding can help demystify the overall idea of using GAI tools. It's helpful to think of these systems as traditional computer and cloud services that have the addition of transformer-based processors. Second, the AI components used to process and store

---

[48] Matthew Burtell & Helen Toner, *The Surprising Power of Next-Word Prediction: Large Language Models Explained, Part 1*, Ctr. for Sec. & Emerging Tech., Georgetown Univ. (Mar. 8, 2024), https://cset.georgetown.edu/article/the-surprising-power-of-next-word-prediction-large-language-models-explained-part-1 (last visited June 18, 2025).

[49] *See, e.g.*, *ChatGPT Consumer Terms of Use*, OpenAI (Dec. 11, 2024), https://openai.com/policies/terms-of-use (providing that, unless users opt out, OpenAI may use content submitted through ChatGPT to improve its models).

[50] *AI Logs and Legal Holds: How to Build a Defensible Retention Strategy*, Hanzo (Sept. 17, 2025), https://www.jdsupra.com/legalnews/ai-logs-and-legal-holds-how-to-build-a-7261821 (last visited October 1, 2025).

data present different types of privacy and security risks than traditional components. In general, understanding which parts of the system are AI-based and which parts are not can help lawyers make better decisions about client confidentiality, vendor due diligence, and ethical compliance.

Retrieval-Augmented Generation

Many GAI tools use retrieval-augmented generation ("*RAG*") to help reduce hallucinations and provide the system with specific knowledge about individual situations. The RAG database might be provided by an entirely separate company, and these databases often store verbatim confidential information for extended periods. Because RAG databases can retain sensitive data and operate largely behind the scenes, it is important for lawyers to verify what subcontractors are involved in managing the GAI tool, including the RAG database and what privacy and security assurances apply across the entire supply chain.

The RAG process is depicted using grey arrows in Figure 2 and can be understood as follows:

- *First*, the user enters a prompt into the user interface (such as, for example, asking ChatGPT a question). Normally, this would be sent directly to the transformer model for processing, but, since the system uses RAG, something else happens behind the scenes.
- *Second*, the user's prompt is redirected to a special type of AI-compatible database. The purpose of this database is to hold specific information the user is likely to need in a way that is pre-formatted for processing by the transformer model. For example, in a legal research system, the AI-compatible database might hold statutes, cases, law review articles, and other law-related resources.
- *Third*, the system pulls relevant snippets of AI-formatted information from the AI-compatible database and prepends this additional information to the user's original prompt.
- *Fourth*, the combination of the user's original prompt and the augmented information from the AI-compatible database is sent to the transformer model for processing.
- *Finally*, the transformer model generates output in response to the user's augmented input. In other words, the transformer model's generation is *augmented* by what it has *retrieved* from the AI-compatible database, so we call it "*retrieval-augmented generation*."

While lawyers do not need to understand the technical details of how RAG and AI-compatible databases function, lawyers *should* understand that multiple providers are likely to be involved in the process of storing, processing, and transmitting information that moves through a typical GAI system. One provider might supply the transformer model, while a different provider might supply the RAG database. When reviewing any cloud-based system used to store, process, and transmit confidential information, it's important to have a basic understanding of what third parties have access to that information and what privacy and security assurances are in place to support these disclosures.

Data Retention Within the Model

As we've learned, the portion of a GAI tool that performs the actual "artificial intelligence" processing is the transformer model. Accordingly, a key data retention issue to consider is whether the transformer model

itself retains any data that it processes and, if so, for how long. Based upon our review of several major model providers, we believe data retention at the transformer level falls broadly into the following categories:

- By default, model providers tend to keep data for a fixed period (typically 30 days) after it is processed.
- With specific approval, model providers may agree to convert the transformer to Zero Data Retention. With this configuration in place, the model will not retain any data that it processes.

Lawyers using a Native Model Platform must negotiate and manage the transformer's retention period directly. By contrast, if a lawyer's application is based on an API Integration, it is the application provider, and not the lawyer, who controls this setting. A transformer operating in Zero Data Retention mode is generally more appropriate for processing sensitive information, including Sensitive Personal Information.

Data Retention for Abuse Monitoring

Closely related to transformer-level retention, many GAI tools also log user inputs and outputs for abuse monitoring purposes. These logs are intended to detect and prevent prohibited activities such as malicious code generation, harassment, or other uses that violate the provider's terms of service.[51]

By default, model providers are likely to retain abuse monitoring logs for a defined period, often 30 days, even if the transformer's data retention is set to Zero Data Retention. These logs may contain user content, and they may be reviewed by human moderators or analyzed automatically for compliance purposes.[52] Some providers allow these logs to be disabled or to operate in a Zero Data Retention mode for approved accounts. Due to the risk of storage and disclosure, systems with abuse monitoring logs disabled are generally more appropriate for processing sensitive information.

Data Isolation

Anytime you store or process data in a cloud environment, there is some level of resource sharing among the customers of that service. In a fully multi-tenant environment, most of the components of the environment are shared by all customers of the service, subject only to basic logical separation. Multi-tenant environments are less expensive, but they increase the risk of data leakage between customers. Isolated environments tend to be more expensive but are also more appropriate for storing and processing highly sensitive data.

Figure 4 below shows how a GAI tool developer might deploy their architecture within the Microsoft Azure OpenAI service.[53] As stated by Microsoft "this solution is the easiest to implement, but it provides the least data isolation and performance isolation."

---

[51] *Abuse Monitoring*, Microsoft Learn (Sept. 30, 2025), https://learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring (last visited October 2, 2025).

[52] *Id*.

[53] *Multitenancy and Azure OpenAI Service*, *supra* note 33.

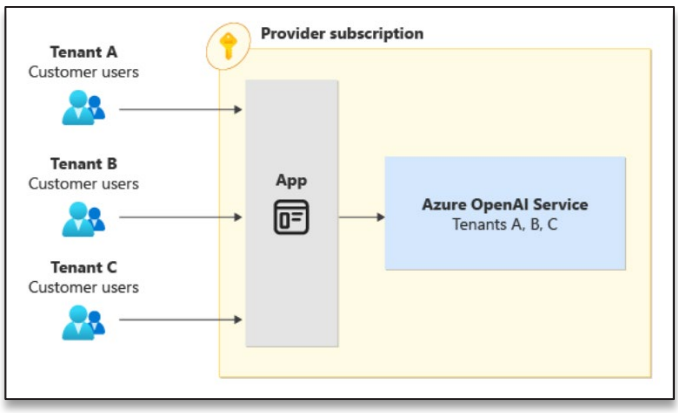


Figure 4: Illustration of an AI system deployment using the Microsoft Azure OpenAI isolated tenant configuration.

By contrast, Figure 5 below shows another option that GAI tool developers might choose to better isolate their customers' data. As described by Microsoft "this approach provides data isolation for each tenant [but] it requires you to deploy and manage an increasing number of Azure OpenAI resources as you increase the number of tenants."

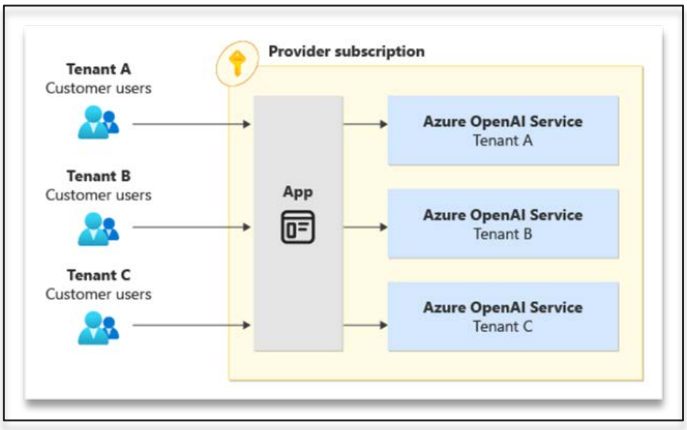


Figure 5: Illustration of AI system deployment using Microsoft Azure OpenAI multi-tenant configuration.

The more sensitive the data, the more carefully a lawyer should examine the provider's data isolation practices and require that the agreement include explicit safeguards addressing data isolation.

Supporting Resources and Materials

Appendix 1: Illinois Supreme Court Policy on Artificial Intelligence, together with Judicial Reference Sheet on AI

Appendix 2: GAI Terms of Use Checklist

Appendix 3: Sample Notice of Artificial Intelligence Practices

Appendix 4: Sample Use of GAI Tools Policy

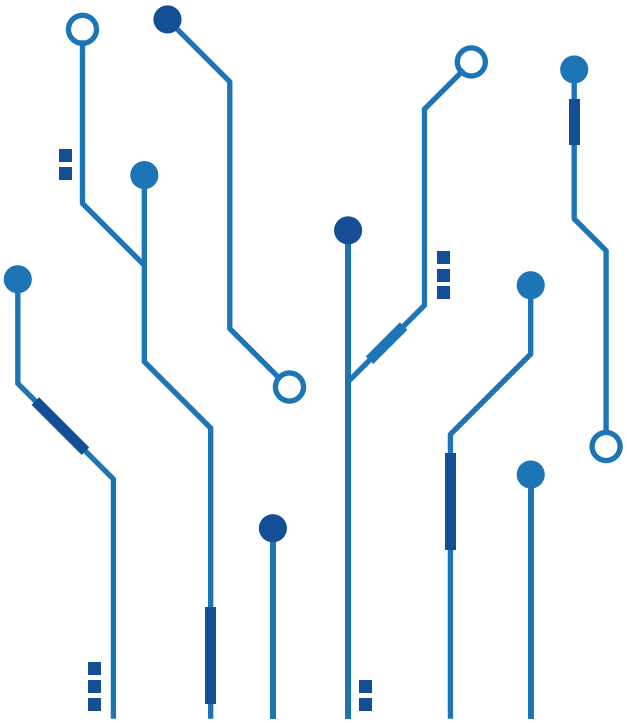
Appendix 5: Sample Informed Client Consent Form

Appendix 6: Cybersecurity Information Sheet ("CIS"): Deploying AI Systems Securely – Best Practices for Deployment

Appendix 1
Illinois Supreme Court Policy on Artificial Intelligence, together with Judicial Reference Sheet on AI

ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE

EFFECTIVE JANUARY 1, 2025



Embracing the advancements of artificial intelligence (AI), the Illinois Supreme Court remains steadfast in its commitment to upholding the highest ethical standards in the administration of justice. We acknowledge the rapid development of generative AI technologies capable of producing human-like text, images, video, audio, and other content. The integration of AI with the courts is increasingly pervasive, offering potential efficiencies and improved access to justice. However, it also raises critical concerns about authenticity, accuracy, bias, and the integrity of court filings, proceedings, evidence, and decisions. Understanding the capabilities and limitations of AI technology is essential for the Illinois Judicial Branch.

The Illinois Courts will be vigilant against AI technologies that jeopardize due process, equal protection, or access to justice. Unsubstantiated or deliberately misleading AI-generated content that perpetuates bias, prejudices litigants, or obscures truth-finding and decision-making will not be tolerated.

The use of AI by litigants, attorneys, judges, judicial clerks, research attorneys, and court staff providing similar support may be expected, should not be discouraged, and is authorized provided it complies with legal and ethical standards. Disclosure of AI use should not be required in a pleading.

The Rules of Professional Conduct and the Code of Judicial Conduct apply fully to the use of AI technologies. Attorneys, judges, and self-represented litigants are accountable for their final work product. All users must thoroughly review AI-generated content before submitting it in any court proceeding to ensure accuracy and compliance with legal and ethical obligations. Prior to employing any technology, including generative AI applications, users must understand both general AI capabilities and the specific tools being utilized.

The Court acknowledges the necessity of safe AI use, adhering to laws and regulations concerning privacy and confidentiality. AI applications must not compromise sensitive information, such as confidential communications, personal identifying information (PII), protected health information (PHI), justice and public safety data, security-related information, or information conflicting with judicial conduct standards or eroding public trust.

This policy reflects the Illinois Supreme Court's commitment to upholding foundational principles while exploring the potential benefits of new AI technologies in a dynamic landscape. The Court will regularly reassess policies as these technologies evolve, prioritizing public trust and confidence in the judiciary and the administration of justice. **Judges remain ultimately responsible for their decisions, irrespective of technological advancements.**

The Court encourages the development of technologies that enhance service to all court users and promote equitable access to justice. To facilitate this, the judicial branch will support ongoing education on emerging technologies, including AI.

ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE

JUDICIAL REFERENCE SHEET

JANUARY 1, 2025

WHAT IS ARTIFICIAL INTELLIGENCE?

Technology that simulates human intelligence, enabling machines to learn, reason, perceive, and make decisions.
Artificial Intelligence is not new technology.

1950s Origins of AI

Examples: Spell check, predicative typing, facial recognition, and computer based legal research.

2022 Mainstream Availability of Generative AI

Examples:
Text Composition Prompts
"Summarize the following legal brief and identify key arguments."

"Rewrite this paragraph in a respectful and neutral tone using plain language so it can be understood by people without legal expertise."

"Prepare a speech about the importance of procedural due process for an audience of judges."

Photo/Audio/Video Prompts
"Create image of an Illinois Courtroom."

"Create movie depicting President Abraham Lincoln conducting legal research on a computer."

WHAT IS GENERATIVE ARTIFICIAL INTELLIGENCE?

A subset of artificial intelligence focused on creating new content, such as text, images, and video, by learning from existing data.
Generative AI is a relatively new tool.

WANT TO KNOW MORE?

National Center for State Courts AI Resource Center

Description of AI and Court Use Cases Video

JUDICIAL DECISIONS

Judges remain ultimately responsible for their decisions, irrespective of technological advancements.

Code of Judicial Conduct - Rule 2.7
A judge shall hear and **decide** matters assigned to the judge...

Code of Judicial Conduct - Rule 1.2
A judge shall act at all times in a manner that promotes public confidence in the independence, integrity, and impartiality of the judiciary...

PLEADINGS

Lawyers & Self Represented Litigants are subject to sanctions for submitting legally or factually unfounded pleadings.

Illinois Supreme Court Rule 137
The signature of an attorney or party constitutes a certificate by him that he has read the pleading, motion or other document; that to the best of his knowledge, information, and belief formed after reasonable inquiry it is well grounded in fact and is warranted by existing law...

THINKING ABOUT USING GENERATIVE AI? JUDICIAL AI UTILIZATION GUIDELINES

Ethical Oversight - The Code of Judicial Conduct applies fully to the use of AI technologies. You maintain ultimate responsibility for all rulings and legal documents.

Competence - The judicial branch must stay informed about evolving AI technologies. Prior to using any technology, including generative AI applications, you need to understand both general AI capabilities and the specific tools being used.

Accuracy - Be mindful that content from generative AI applications comes from sourced material. AI-generated content must be thoroughly reviewed to ensure accuracy and compliance with legal and ethical obligations, including a specific need to guard against technology lending to unintentional bias or prejudice.

Attribution - Ensure your work product does not infringe upon copyright or intellectual property rights by proper attribution to sources as necessary.

Confidentiality - If using a public generative AI tool (like ChatGPT), your input prompt is being handed over to the technology. Ensure you do not compromise sensitive information. Do not input any information such as (non-exhaustive list):

- Confidential or privileged information;
- Personal identifying information;
- Protected health information;
- Justice and public safety information;
- Code containing passwords or security-related information; and
- Information that has potential to erode public trust.

WHAT TO WATCH FOR AS A JUDGE

AI is ubiquitously present in modern technology. It is safe to assume AI was used in pleadings and other written materials. Generative AI applications gives rise to these considerations:

Hallucinations - When generative AI produces output that appears realistic but is misleading or made up by the AI itself rather than real-world data or input. If generative AI was used in a legal pleading or brief, included citations may be entirely made up or be a real case but not contain the purported language cited. Read a case decision on hallucinations.

Deepfakes - When generative AI is intentionally used to produce convincing/deceptive media - images, audio, video, etc. Fake evidence is relatively easy to create and reliable technology solutions do not exist to identify real vs fake evidence. Learn more about identification of deepfakes.

Extended Reality - Technology can seamlessly be integrated with our person though wearable devices. Recognize that technology may allow an individual to record and analyze audio and video and channel information from other sources in real-time, potentially without detection. Learn more about extended reality.

CHECK CITATIONS

HEAR EVIDENCE ON FOUNDATIONS

ENFORCE EXISTING TECHNOLOGY RULES

Appendix 2
GAI Terms of Use Checklist

To assist with choosing appropriate third-party managed GAI tools, we prepared the following checklist. This is intended to help identify and evaluate important contractual protections, but should not be interpreted as a mandatory or exhaustive set of requirements.

- No Model Training: Neither the model provider nor any integrated application provider may use customer data to develop or improve its services without explicit, written customer consent.
- Purpose Limitation: Use of customer data should be limited to providing the services, complying with applicable law, enforcing provider policies, and preventing abuse. These purposes may be further limited where Zero Data Retention is enabled.
- Data Retention: Customer data must be permanently deleted from the provider's servers within a reasonable period after it is deleted from the user interface, or after account termination, except where retention is required by law.
- Data Isolation: Where higher degrees of data isolation are critical for the type of data being processed, the contract should address the specific isolation requirements for both the application and the transformer model.
- Data Residency: Where specific geographic hosting location is critical for the type of data being processed, the contract should specify the permitted data processing jurisdictions and include any applicable supplemental provisions (e.g. a Data Processing Addendum).
- User Anonymity: Where anonymous GAI inputs are critical to user privacy, the provider must ensure API requests do not include identifiable client or firm information.
- Compliance with Privacy Laws: Provider must comply with all privacy laws applicable to the data, customer, and clients.
- Breach Notification: Providers should clearly agree to provide timely breach notification requirements and specify their incident response obligations.
- Risk Management: The application must be developed, deployed, and maintained in accordance with recognized information security frameworks (such as SOC 2, ISO 27001, CSA STAR) and AI risk management frameworks (e.g., NIST AI RMF, OWASP GenAI Security Project). The provider should publish or provide supporting documentation demonstrating compliance.
- Third-Party Access Controls: Define and limit third-party access rights and include an obligation of the primary provider to bind downstream third parties to all relevant data management obligations.
- Supplementary Agreements: Explore the availability of a Data Processing Addendum for personal data processing or a HIPAA business associate agreement when required for protected health information.

The specific protections to include will depend on the type of data being processed, applicable regulations, and the lawyer's professional obligations in the given context.

Appendix 3
Sample Notice of Artificial Intelligence Practices

SAMPLE NOTICE OF ARTIFICIAL INTELLIGENCE PRACTICES

Acme Law, LLC provides this Notice of Artificial Intelligence Practices to explain how and when artificial intelligence tools may be used in providing our services. We believe it is important for clients to understand the circumstances under which personally identifiable information and client confidential information may be processed using artificial intelligence, the safeguards we apply to protect that information, and your rights relating to our use of such tools.

GENERATIVE ARTIFICIAL INTELLIGENCE DEFINED

When lawyers refer to "AI," they are typically referencing a specific type of computer algorithm that predicts and generates text by analyzing patterns in numerical representations of language and images. These algorithms are often referred to as *Generative Artificial Intelligence* ("*GAI*").

HOW WE USE AI

Some of our systems and professionals use business-class GAI tools. The attached Schedule of Generative Artificial Intelligence Tools provides representative examples of the tools we use.[54] Clients who have an active matter with us may request a current list of our GAI tools using the information provided at the end of this Notice. Our GAI Tools are used in the following contexts:

- System-Wide Processing. "System-Wide Processing" means using GAI systems in firm-wide administrative, security, or operational tools as part of standard functions, such as document management, email filtering, cybersecurity, or automated billing.

- De-Identified Processing. Some professionals at Acme Law, LLC may use GAI tools as work assistants without inputting any personally identifiable or client confidential information. When this type of processing relates directly to an active matter, clients have opt-out rights as described under "Your Rights" below.

- Confidential Processing. Professionals may, in some cases, use GAI tools to process personally identifiable or client confidential information. For example, a document may be uploaded to a GAI tool to support efficient review of that document. Clients have consent and opt-out rights for this type of processing, as described under "Your Rights" below.

[54] Lawyers may consider omitting the schedule of representative tools entirely, removing it from public-facing materials, or limiting distribution to active clients who request more information.

HOW WE PROTECT YOUR INFORMATION

We maintain a formal written policy to ensure responsible and secure use of Generative Artificial Intelligence (GAI) tools. Among other things, our written policy provides the following safeguards:

- We take direct professional responsibility for the output of any GAI tool used in connection with our work. We believe GAI tools help make lawyers more efficient, but we do not rely on them to make legal judgments or decisions.

- When GAI tools are used for System-Wide Processing, we take reasonable and appropriate measures to ensure those tools are suitable for handling such protected information.

- We review all GAI tools for compliance with appropriate privacy assurances and security requirements before use. We do not use consumer-grade GAI tools such as the free or personal versions of ChatGPT.

- We maintain a written policy and train all lawyers and staff members to ensure that your rights, described below, are honored.

YOUR RIGHTS

Clients have the right to remain informed about how GAI tools may be used in matters we undertake for them. We will regularly update the attached Schedule of Generative Artificial Intelligence Tools, and clients with an active matter may request a current version at any time.[55]

Clients may opt out of De-Identified Processing and Confidential Processing (defined above). To exercise this right, send us written notice using the contact information provided below.

Other than for System-Wide Processing, we will not use GAI tools to process information listed in the Illinois Personal Information Protection Act without your informed written consent. Individual clients may provide consent for use of their data directly. Organizational clients may provide consent if they are the lawful controller or processor of the data or are otherwise permitted to consent under applicable law. Consent may be revoked any time and for any reason. Revocation applies prospectively from the date it is received.

If we use GAI tools for System-Wide Processing (as defined above), we will take reasonable and appropriate measures to ensure such tools are suitable for processing personally identifiable and client confidential information.

Contact Information

Johnathan A. Doe, Managing Partner
ACME Law, LLC
1234 Justice Lane, Suite 800
Sampleville, IL 54321
Phone: (555) 867-5309
Email: jdoe@acmelawfictional.com

Effective Date: October 1, 2025

[55] Refer to note 54.

SCHEDULE OF GENERATIVE ARTIFICIAL INTELLIGENCE TOOLS[56]

The following table sets forth the Generative Artificial Intelligence tools in use at ACME Law, LLC as of the Effective Date of this Notice. Clients having an active matter with us may request a current list of our GAI tools using the contact information in this Notice.

Tool[57]	Representative Uses	Provider Safeguards
ChatGPT Team	document summarization or analysis, drafting assistance	https://trust.openai.com
Microsoft Copilot	AI integrations in Microsoft Office and Teams	https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy
Adobe AI Assistant	Document summarization and analysis	https://experienceleague.adobe.com/en/docs/experience-platform/ai-assistant/privacy
vLex	Legal research, document drafting and analysis	https://trust.vlex.com
Lexis+AI	Legal research, document drafting and analysis	https://www.lexisnexis.com/pdf/relx-responsible-ai-principles.pdf
CoCounsel	Legal research, document drafting and analysis	https://help.casetext.com/en/collections/6255626-trust-security-and-privacy

The GAI tools listed above may rely on third-party providers and infrastructure to deliver their services. We enter into agreements with these providers that require appropriate privacy and security safeguards throughout the supply chain, including confidentiality, data protection, and access control measures.

[56] Refer to note 54.

[57] ARDC does not recommend or endorse any specific technology or provider. The examples given in this table are simply provided to illustrate how a typical law firm might choose to disclose the GAI tools it uses.

Appendix 4

Sample Use of GAI Tools Policy

POLICY Use of GAI Tools	
Policy ID: AI G-100.1 Approved By: _____ Johnathan A. Doe, Managing Partner	References: ❖ https://openai.com ❖ https://www.microsoft.com/en-us/ai ❖ Illinois Supreme Court Policy on Artificial Intelligence ❖ Illinois Rule of Professional Conduct Rule 1.1 (Competence) ❖ Illinois Rule of Professional Conduct Rule 1.4 (Communication) ❖ Illinois Rule of Professional Conduct Rule 1.6 (Confidentiality of Information)

1. Purpose. This Policy addresses the use of Generative Artificial Intelligence (as defined below) at ACME Law, LLC. ("ACME"). Generative Artificial Intelligence is a rapidly evolving technology that can bring great value to our efforts. However, its legal and technical risks are not well-known, and its potential for unintentional misuse merits a consistent policy-based approach to using this technology within our environment.

2. Scope. This Policy applies to all members of the ACME Workforce. The term "ACME Workforce" means ACME employees, as well as independent contractors, interns, volunteers, and other individuals who are appointed or engaged to provide services or create work product on ACME's behalf.

   This Policy does not apply to activities outside the scope of one's work for ACME unless such activities adversely affect the confidentiality, security, or reputation of ACME.

   This Policy covers all company systems, devices, technologies, and platforms, including software applications, hardware devices, cloud platforms, mobile applications, and any other technology interfaces.

3. Definition of Generative Artificial Intelligence. For purposes of this Policy, the term "Generative Artificial Intelligence" or "GAI" refers to an artificial intelligence tool that is designed to produce new, previously unseen, data in response to human input using predictive algorithms applied to an underlying database of training data and may include systems that generate new images, text, sounds, or other data types in response to human input.

4. Approved GAI Tools. The ACME Managing Partner may designate one or more GAI tools as approved for use by the ACME Workforce (each an "Approved GAI Tool"). Approved GAI Tools will be posted at [***insert link or document ID***] (the "Schedule of Approved GAI Tools"). Only Approved GAI Tools may be used on ACME devices or to process ACME information (including ACME client information).

5. Professional Responsibility. Members of the ACME Workforce who use Approved GAI Tools may do so solely as supplementary instruments, such as to generate ideas or assist in the review or preparation of documents. While GAI can serve as a valuable tool, ultimate responsibility for the accuracy, relevance, and appropriateness of any final work product rests solely with the ACME Workforce member using the Approved GAI Tool.

   (a) General Rule. GAI Tools are prone to generate fictitious case and statutory citations (a phenomenon often referred to as a "*hallucination*"). Accordingly, except as provided in Section 5(b), it is imperative that all outputs derived from Approved GAI Tools be meticulously reviewed, validated, and edited as necessary by the user before finalization. Use of Approved GAI Tools should not substitute or diminish the critical thinking, judgment, and expertise that our ACME Workforce members bring to their respective roles.

   (b) Exception for Mass Data Processing. Where the value of using an Approved GAI Tool would be diminished by the requirement that all GAI outputs be meticulously reviewed and validated, the ACME Managing Partner may grant case-by-case exceptions to Section 5(a). For example, ACME might use an Approved GAI Tool to search or summarize large datasets that cannot reasonably be validated by humans or even traditional computer algorithms. In this example, requiring the output of the GAI process to be reviewed and validated by humans might defeat the purpose of using the GAI tool.

   (c) Client Consent for Allocation of Responsibility. In such cases where ACME cannot reasonably exercise full professional responsibility for the GAI output, the client's informed written consent shall be obtained as described in Section 6(c). The responsible attorney should consult Illinois Rule of Professional Conduct 1.2 when structuring a matter in this way.

6. Client Rights. Our clients have a right to be informed about how ACME uses GAI tools to process their matters and confidential information. This section outlines the rules for informing clients about our use of GAI tools. This section also describes when and how clients may opt out of our use of GAI tools to process their matters and confidential information. This section also describes the circumstances under which we are required to obtain a client's informed written consent prior to processing their information using a GAI tool.

   (a) Notice of Artificial Intelligence Practices. At all times after implementation of this Policy, ACME will maintain a current and accurate Notice of Artificial Intelligence Practices describing how ACME uses GAI tools and safeguards client confidential information. This

Notice should be clearly posted on the ACME website. Clients should be provided with this Notice as part their engagement documents, and within a reasonable time after we make any material changes to our policies and procedures for using GAI tools. No information related to client matters or confidential information should be processed in GAI tools prior to the client receiving this Notice.

(b) Client Opt-Out Rights. Except as provided in Section 6(e), Clients have the right to restrict or prohibit the use of GAI tools in connection with their matters or to process their confidential information. A client may exercise this right at any time by providing written notice. Upon receipt of such notice, the client's preferences should be clearly and prominently documented in the client file. All ACME Workforce members on the file should be notified of the client's opt-out and take immediate steps to ensure that GAI tools are not used in any manner that violates the client's expressed restrictions.

Accordingly, unless a client has opted out, members of the ACME Workforce may use Approved GAI Tools for the following purposes:

i. De-Identified Processing. Approved GAI Tools may be used as a work assistant without inputting any personally identifiable or client confidential information. This could include posing hypothetical questions to an Approved GAI Tool to help generate a checklist for drafting documents.

ii. Non-Sensitive Confidential Processing. Approved GAI Tools may also be used to process client identifying or confidential information **other than Sensitive Personal Information as defined in the next section**. For example, a document may be uploaded to an Approved GAI Tool to support efficient review of that document, provided any Sensitive Personal Information has first been redacted.

(c) Sensitive Personal Information. Prior to using an Approved GAI Tool to process Sensitive Personal Information, as defined below, ACME must obtain the client's informed written consent using the procedure described in Section 6(d). For the purposes of this Policy, Sensitive Personal Information includes:

- Social security numbers or tax returns
- Driver's license numbers or state identification card numbers
- Account, credit card, or debit card numbers
- Medical information, including mental health or substance abuse treatment records
- Health insurance information
- Unique biometric identifiers or biometric information (as defined in Illinois law)
- Passwords and security questions and answers used to access computer accounts
- Any other information meeting PIPA's definition of "personal information," even if separated from a first name or first initial in combination with last name

(d) Informed Client Consent. Where client consent is required, it must be informed. The client must receive a clear explanation of the purpose of the processing, the type of data involved, the type of GAI tool to be used, the potential risks (including risks of disclosure or misuse), and the safeguards in place to protect the data. This information must be provided separately from other materials, and the client must be given the opportunity to ask questions before providing consent. Consent must be voluntary and may be revoked at any time and for any reason.

i. Authority to Consent. The client may provide consent to process personal data that is (i) the personal data of the client or (ii) personal data of which the client is the lawful controller or processor. If the responsible attorney has reason to doubt the client's authority to consent to the processing for the personal data provided, they must refrain from processing the data using GAI until appropriate authorization is confirmed.

ii. Discretionary Consents. The attorney responsible for any client or matter is free to require informed written consent for the use of Approved GAI Tools using criteria that is more restrictive than this Policy provides. If, in the professional judgment of the responsible attorney, informed written consent is prudent in any matter, then the responsible attorney's judgment shall control.

(e) System-Wide Processing. "*System-Wide Processing*" means using GAI systems in firm-wide administrative, security, or operational tools as part of standard functions, such as document management, email filtering, cybersecurity, or automated billing. These GAI tools are exempt from client opt-out or consent rights described above.

7. Implementation of Client and Project Level Restrictions. Prior to using Approved GAI Tools for any client or client project, the responsible attorney for the matter must complete an evaluation to determine whether any regulatory, contractual, or other specific obligations apply to the client or project. Approved GAI Tools may not be used unless such requirements are identified and complied with. For example:

i. Client-Imposed Restrictions. Clients may include GAI-related restrictions in their agreements or engagement letters. As described above, clients may also file an opt-out request to limit or prohibit the use of GAI tools to process their data.

ii. Flow-Down Restrictions. Clients may be subject to GAI limitations that flow down to ACME, such as public-sector procurement rules (e.g. the California State GenAI Procurement Guidelines).

iii. Data Protection Requirements. Certain client data may be subject to heightened privacy or security obligations that require additional safeguards around GAI use, including but not limited to the CCPA, GDPR, or HIPAA.

8. Court and Regulatory Rules. Some courts or regulators may require the use of GAI tools to be disclosed, documented, or certified. These rules may require a party to: (i) identify which GAI tool was used in drafting a court filing; (ii) explain how the GAI tool was used in preparing court filings or regulated submissions; (iii) verify the accuracy of AI-generated content using non-GAI authoritative sources; and/or (iv) confirm that no confidential or proprietary information was disclosed to unauthorized parties. Accordingly, prior to using Approved GAI Tools to prepare any materials that will be used in a judicial or regulatory proceeding, the supervising attorney will confirm what GAI rules apply to that proceeding.

9. Data Minimization. Each ACME Workforce member must limit the retention of data in Approved GAI Tools to only what is reasonably necessary to support the project or matter for which the Approved GAI Tools are used. Approved GAI Tools should not be used as long-term storage or recordkeeping systems. For example, Workforce members should delete conversations, documents, prompts, instructions, memory functions, and other related data when the associated client matter is closed, or if no longer reasonably needed to manage that specific project or matter.

10. Education and Training. The ACME Managing Partner will coordinate education and training for all members of the ACME Workforce on the responsible use of artificial intelligence, including the requirements of this Policy. This training should include understanding ethical implications, data privacy and security risks, and the effective practical use of approved GAI tools and extensions.

11. Intellectual Property. The output of a Generative Artificial Intelligence tool may not be subject to intellectual property protection. Accordingly, Generative Artificial Intelligence output may not be incorporated into materials intended to have intellectual property protection without specific review and approval on a case-by-case basis. Accordingly, absent such review and approval, all work product intended to receive intellectual property protection must be original work produced by ACME Workforce members acting within the scope of their employment or engagement and not work product that is produced by a GAI tool.

12. Enhanced Periodic Review. As previously noted, the field of Artificial Intelligence is evolving rapidly. Accordingly, this Policy must be reviewed on a more frequent basis than provided in other ACME policies. The ACME Managing Partner is therefore directed to establish an Artificial Intelligence Review Committee and a policy review schedule that is appropriate to the speed at which this technology is evolving and the rate at which AI-related tools are adopted within ACME (and our clients and vendors).

13. Version Control. Any amendments or additions to this Policy shall be reflected in a new version and summarized in the attached Revision Management Log.

Revision Management Log		
Revision ID	Date	Brief Description
AI-100.1	**********	Initial Policy Adoption

Appendix 5
Sample Informed Client Consent Form

Informed Consent for the Use of Generative Artificial Intelligence

Matter: [Insert Matter Title]
Client: [Insert Client Name]

Acme Law, LLC may use Generative Artificial Intelligence ("GAI") tools to support legal work such as document analysis, summarization, legal research, or drafting. These tools can improve efficiency and enhance the quality of legal services when used responsibly and with appropriate safeguards. In your matter, we believe it may be beneficial and appropriate to process certain sensitive personal information using GAI tools. Accordingly, we request your written consent to use GAI tools to process sensitive personal information related to your matter.

Categories of Sensitive Personal Information to be Processed

Absent additional written consent, we will only use GAI tools to process the following categories of Sensitive Personal Information:

- Social Security numbers
- Driver's license or state ID numbers
- Financial account numbers or payment card data
- Medical or health insurance information
- Other information covered by the Illinois Personal Information Protection Act

Purpose of Processing

We will only process sensitive personal information using GAI tools if it is directly relevant to the legal services we are providing and necessary to achieve a meaningful benefit, such as faster document review, clearer summarization, or improved accuracy in analysis. Due to the volume of documents that must be reviewed in your matter, we believe the use of GAI tools will improve accuracy and reduce the time needed to perform our work.

GAI Tools to be Used

If you consent, we will only use business-class GAI tools which are subject to appropriate privacy and security assurances. The specific GAI tools used by ACME Law, LLC are available in our Notice of Artificial Intelligence Practices that is updated no less than quarterly.

Client Consent

I have read and understand this form and ACME Law, LLC's Notice of Artificial Intelligence Practices. I understand the nature and purpose of this request, and I have been given the opportunity to discuss any questions or concerns I may have with individuals who are knowledgeable about the specific GAI tools that will be used to process my sensitive personal information.

I understand that I may revoke this consent at any time and for any reason by using the contact information provided in ACME Law, LLC's Notice of Artificial Intelligence Practices. I also understand that my revocation will only be effective for uses of my personal information after the effective date of my revocation, and that my revocation will not apply to the use of GAI for system-wide processing within ACME Law, LLC's network and computer systems.

Accordingly, I consent to Acme Law, LLC's use of GAI tools as described above.

_____

Dated: _____

Appendix 6
Cybersecurity Information Sheet ("CIS")
Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems




Deploying AI Systems Securely

Best Practices for Deploying Secure and Resilient AI Systems

Executive summary

Deploying artificial intelligence (AI) systems securely requires careful setup and configuration that depends on the complexity of the AI system, the resources required (e.g., funding, technical expertise), and the infrastructure used (i.e., on premises, cloud, or hybrid). This report expands upon the 'secure deployment' and 'secure operation and maintenance' sections of the Guidelines for secure AI system development and incorporates mitigation considerations from Engaging with Artificial Intelligence (AI). It is for organizations deploying and operating AI systems designed and developed by another entity. The best practices may not be applicable to all environments, so the mitigations should be adapted to specific use cases and threat profiles. [1], [2]

AI security is a rapidly evolving area of research. As agencies, industry, and academia discover potential weaknesses in AI technology and techniques to exploit them, organizations will need to update their AI systems to address the changing risks, in addition to applying traditional IT best practices to AI systems.

This report was authored by the U.S. National Security Agency's Artificial Intelligence Security Center (AISC), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK). The goals of the AISC and the report are to:

1. Improve the confidentiality, integrity, and availability of AI systems;
2. Assure that known cybersecurity vulnerabilities in AI systems are appropriately mitigated; and
3. Provide methodologies and controls to protect, detect, and respond to malicious activity against AI systems and related data and services.

U/OO/143395-24 | PP-24-1538 | April 2024 Ver. 1.0

Scope and audience

The term AI systems throughout this report refers to machine learning (ML) based artificial intelligence (AI) systems.

These best practices are most applicable to organizations deploying and operating externally developed AI systems on premises or in private cloud environments, especially those in high-threat, high-value environments. They are not applicable for organizations who are not deploying AI systems themselves and instead are leveraging AI systems deployed by others.

Not all of the guidelines will be directly applicable to all organizations or environments. The level of sophistication and the methods of attack will vary depending on the adversary targeting the AI system, so organizations should consider the guidance alongside their use cases and threat profile.

See Guidelines for secure AI system development for design and development aspects of AI systems. [1]

Introduction

The rapid adoption, deployment, and use of AI capabilities can make them highly valuable targets for malicious cyber actors. Actors, who have historically used data theft of sensitive information and intellectual property to advance their interests, may seek to co-opt deployed AI systems and apply them to malicious ends.

Malicious actors targeting AI systems may use attack vectors unique to AI systems, as well as standard techniques used against traditional IT. Due to the large variety of attack vectors, defenses need to be diverse and comprehensive. Advanced malicious actors often combine multiple vectors to execute operations that are more complex. Such combinations can more effectively penetrate layered defenses.

Organizations should consider the following best practices to secure the deployment environment, continuously protect the AI system, and securely operate and maintain the AI system.

The best practices below align with the cross-sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on

existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

Secure the deployment environment

Organizations typically deploy AI systems within existing IT infrastructure. Before deployment, they should ensure that the IT environment applies sound security principles, such as robust governance, a well-designed architecture, and secure configurations. For example, ensure that the person responsible and accountable for AI system cybersecurity is the same person responsible and accountable for the organization's cybersecurity in general [CPG 1.B].

The security best practices and requirements for IT environments apply to AI systems, too. The following best practices are particularly important to apply to the AI systems and the IT environments the organization deploys them in.

Manage deployment environment governance

- If an organization outside of IT is deploying or operating the AI system, work with the IT service department to identify the deployment environment and confirm it meets the organization's IT standards.
    - Understand the organization's risk level and ensure that the AI system and its use is within the organization's risk tolerance overall and within the risk tolerance for the specific IT environment hosting the AI system. Assess and document applicable threats, potential impacts, and risk acceptance. [3], [4]
    - Identify the roles and responsibilities for each stakeholder along with how they are accountable for fulfilling them; identifying these stakeholders is especially important should the organization manage their IT environment separately from their AI system.
    - Identify the IT environment's security boundaries and how the AI system fits within them.
- Require the primary developer of the AI system to provide a threat model for their system.

  - The AI system deployment team should leverage the threat model as a guide to implement security best practices, assess potential threats, and plan mitigations. [5], [6]

- Consider deployment environment security requirements when developing contracts for AI system products or services.
- Promote a collaborative culture for all parties involved, including the data science, infrastructure, and cybersecurity teams in particular, to allow for teams to voice any risks or concerns and for the organization to address them appropriately.

Ensure a robust deployment environment architecture

- Establish security protections for the boundaries between the IT environment and the AI system [CPG 2.F].
- Identify and address blind spots in boundary protections and other security-relevant areas in the AI system the threat model identifies. For example, ensure the use of an access control system for the AI model weights and limit access to a set of privileged users with two-person control (TPC) and two-person integrity (TPI) [CPG 2.E].
- Identify and protect all proprietary data sources the organization will use in AI model training or fine-tuning. Examine the list of data sources, when available, for models trained by others. Maintaining a catalog of trusted and valid data sources will help protect against potential data poisoning or backdoor attacks. For data acquired from third parties, consider contractual or service level agreement (SLA) stipulations as recommended by CPG 1.G and CPG 1.H.
- Apply secure by design principles and Zero Trust (ZT) frameworks to the architecture to manage risks to and from the AI system. [7], [8], [9]

Harden deployment environment configurations

- Apply existing security best practices to the deployment environment. This includes sandboxing the environment running ML models within hardened containers or virtual machines (VMs) [CPG 2.E], monitoring the network [CPG 2.T], configuring firewalls with allow lists [CPG 2.F], and other best practices, such as those in NSA's Top Ten Cloud Mitigation Strategies for cloud deployments.
- Review hardware vendor guidance and notifications (e.g., for GPUs, CPUs, memory) and apply software patches and updates to minimize the risk of exploitation of vulnerabilities, preferably via the Common Security Advisory Framework (CSAF). [10]

- Secure sensitive AI information (e.g., AI model weights, outputs, and logs) by encrypting the data at rest, and store encryption keys in a hardware security module (HSM) for later on-demand decryption [CPG 2.L].
- Implement strong authentication mechanisms, access controls, and secure communication protocols, such as by using the latest version of Transport Layer Security (TLS) to encrypt data in transit [CPG 2.K].
- Ensure the use of phishing-resistant multifactor authentication (MFA) for access to information and services. [2] Monitor for and respond to fraudulent authentication attempts [CPG 2.H]. [11]
- Understand and mitigate how malicious actors exploit weak security controls by following the mitigations in Weak Security Controls and Practices Routinely Exploited for Initial Access.

Protect deployment networks from threats

Adopt a ZT mindset, which assumes a breach is inevitable or has already occurred. Implement detection and response capabilities, enabling quick identification and containment of compromises. [8], [9]

- Use well-tested, high-performing cybersecurity solutions to identify attempts to gain unauthorized access efficiently and enhance the speed and accuracy of incident assessments [CPG 2.G].
- Integrate an incident detection system to help prioritize incidents [CPG 3.A]. Also integrate a means to immediately block access by users suspected of being malicious or to disconnect all inbound connections to the AI models and systems in case of a major incident when a quick response is warranted.

Continuously protect the AI system

Models are software, and, like all other software, may have vulnerabilities, other weaknesses, or malicious code or properties.

Validate the AI system before and during use

- Use cryptographic methods, digital signatures, and checksums to confirm each artifact's origin and integrity (e.g., encrypt safetensors to protect their integrity and confidentiality), protecting sensitive information from unauthorized access during AI processes. [14]

- Create hashes and encrypted copies of each release of the AI model and system for archival in a tamper-proof location, storing the hash values and/or encryption keys inside a secure vault or HSM to prevent access to both the encryption keys and the encrypted data and model at the same location. [1]
- Store all forms of code (e.g., source code, executable code, infrastructure as code) and artifacts (e.g., models, parameters, configurations, data, tests) in a version control system with proper access controls to ensure only validated code is used and any changes are tracked. [1]
- Thoroughly test the AI model for robustness, accuracy, and potential vulnerabilities after modification. Apply techniques, such as adversarial testing, to evaluate the model's resilience against compromise attempts. [4]
- Prepare for automated rollbacks and use advanced deployments with a human-in-the-loop as a failsafe to boost reliability, efficiency, and enable continuous delivery for AI systems. In the context of an AI system, rollback capabilities ensure that if a new model or update introduces problems or if the AI system is compromised, the organization can quickly revert to the last known good state to minimize the impact on users.
- Evaluate and secure the supply chain for any external AI models and data, making sure they adhere to organizational standards and risk management policies, and preferring ones developed according to secure by design principles. Make sure that the risks are understood and accepted for parts of the supply chain that cannot adhere to organizational standards and policies. [1], [7]
- Do not run models right away in the enterprise environment. Carefully inspect models, especially imported pre-trained models, inside a secure development zone prior to considering them for tuning, training, and deployment. Use organization-approved AI-specific scanners, if and when available, for the detection of potential malicious code to assure model validity before deployment.
- Consider automating detection, analysis, and response capabilities, making IT and security teams more efficient by giving them insights that enable quick and targeted reactions to potential cyber incidents. Perform continuous scans of AI models and their hosting IT environments to identify possible tampering.
    - When considering whether to use other AI capabilities to make automation more efficient, carefully weigh the risks and benefits, and ensure there is a human-in-the-loop where needed.

Secure exposed APIs

- If the AI system exposes application programming interfaces (APIs), secure them by implementing authentication and authorization mechanisms for API access. Use secure protocols, such as HTTPS with encryption and authentication [CPG 2.C, 2.D, 2.G, 2.H]. [1]
- Implement validation and sanitization protocols for all input data to reduce the risk of undesired, suspicious, incompatible, or malicious input being passed to the AI system (e.g., prompt injection attacks). [1]

Actively monitor model behavior

- Collect logs to cover inputs, outputs, intermediate states, and errors; automate alerts and triggers [CPG 2.T].
- Monitor the model's architecture and configuration settings for any unauthorized changes or unexpected modifications that might compromise the model's performance or security. [1]
- Monitor for attempts to access or elicit data from the AI model or aggregate inference responses. [1]

Protect model weights

- Harden interfaces for accessing model weights to increase the effort it would take for an adversary to exfiltrate the weights. For example, ensure APIs return only the minimal data required for the task to inhibit model inversion.
- Implement hardware protections for model weight storage as feasible. For example, disable hardware communication capabilities that are not needed and protect against emanation or side channel techniques.
- Aggressively isolate weight storage. For example, store model weights in a protected storage vault, in a highly restricted zone (HRZ) (i.e., a separate dedicated enclave), or using an HSM [CPG 2.L]. [12]

Secure AI operation and maintenance

Follow organization-approved IT processes and procedures to deploy the AI system in an approved manner, ensuring the following controls are implemented.

Enforce strict access controls

- Prevent unauthorized access or tampering with the AI model. Apply role-based access controls (RBAC), or preferably attribute-based access controls (ABAC) where feasible, to limit access to authorized personnel only.
    - Distinguish between users and administrators. Require MFA and privileged access workstations (PAWs) for administrative access [CPG 2.H].

Ensure user awareness and training

Educate users, administrators, and developers about security best practices, such as strong password management, phishing prevention, and secure data handling. Promote a security-aware culture to minimize the risk of human error. If possible, use a credential management system to limit, manage, and monitor credential use to minimize risks further [CPG 2.I].

Conduct audits and penetration testing

- Engage external security experts to conduct audits and penetration testing on ready-to-deploy AI systems. This helps identify vulnerabilities and weaknesses that may have been overlooked internally. [13], [15]

Implement robust logging and monitoring

- Monitor the system's behavior, inputs, and outputs with robust monitoring and logging mechanisms to detect any abnormal behavior or potential security incidents [CPG 3.A]. [16] Watch for data drift or high frequency or repetitive inputs (as these could be signs of model compromise or automated compromise attempts). [17]
- Establish alert systems to notify administrators of potential oracle-style adversarial compromise attempts, security breaches, or anomalies. Timely detection and response to cyber incidents are critical in safeguarding AI systems. [18]

Update and patch regularly

- When updating the model to a new/different version, run a full evaluation to ensure that accuracy, performance, and security tests are within acceptable limits before redeploying.

Prepare for high availability (HA) and disaster recovery (DR)

- Use an immutable backup storage system, depending on the requirements of the system, to ensure that every object, especially log data, is immutable and cannot be changed [CPG 2.R]. [2]

Plan secure delete capabilities

- Perform autonomous and irretrievable deletion of components, such as training and validation models or cryptographic keys, without any retention or remnants at the completion of any process where data and models are exposed or accessible. [19]

Conclusion

The authoring agencies advise organizations deploying AI systems to implement robust security measures capable of both preventing theft of sensitive data and mitigating misuse of AI systems. For example, model weights, the learnable parameters of a deep neural network, are a particularly critical component to protect. They uniquely represent the result of many costly and challenging prerequisites for training advanced AI models, including significant compute resources; collected, processed, and potentially sensitive training data; and algorithmic optimizations.

AI systems are software systems. As such, deploying organizations should prefer systems that are secure by design, where the designer and developer of the AI system takes an active interest in the positive security outcomes for the system once in operation. [7]

Although comprehensive implementation of security measures for all relevant attack vectors is necessary to avoid significant security gaps, and best practices will change as the AI field and techniques evolve, the following summarizes some particularly important measures:

- Conduct ongoing compromise assessments on all devices where privileged access is used or critical services are performed.
- Harden and update the IT deployment environment.
- Review the source of AI models and supply chain security.
- Validate the AI system before deployment.
- Enforce strict access controls and API security for the AI system, employing the concepts of least privilege and defense-in-depth.

- Use robust logging, monitoring, and user and entity behavior analytics (UEBA) to identify insider threats and other malicious activities.
- Limit and protect access to the model weights, as they are the essence of the AI system.
- Maintain awareness of current and emerging threats, especially in the rapidly evolving AI field, and ensure the organization's AI systems are hardened to avoid security gaps and vulnerabilities.

In the end, securing an AI system involves an ongoing process of identifying risks, implementing appropriate mitigations, and monitoring for issues. By taking the steps outlined in this report to secure the deployment and operation of AI systems, an organization can significantly reduce the risks involved. These steps help protect the organization's intellectual property, models, and data from theft or misuse. Implementing good security practices from the start will set the organization on the right path for deploying AI systems successfully.

Works cited

[1] National Cyber Security Centre et al. Guidelines for secure AI system development. 2023. https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf
[2] Australian Signals Directorate et al. Engaging with Artificial Intelligence (AI). 2024. https://www.cyber.gov.au/sites/default/files/2024-01/Engaging%20with%20Artificial%20Intelligence%20%28AI%29.pdf
[3] MITRE. ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) Matrix version 4.0.0. 2024. https://atlas.mitre.org/matrices/ATLAS
[4] National Institute of Standards and Technology. AI Risk Management Framework 1.0. 2023. https://www.nist.gov/itl/ai-risk-management-framework
[5] The Open Worldwide Application Security Project (OWASP®). LLM AI Cybersecurity & Governance Checklist. 2024. https://owasp.org/www-project-top-10-for-large-language-model-applications/llm-top-10-governance-doc/LLM_AI_Security_and_Governance_Checklist-v1.pdf
[6] The Open Worldwide Application Security Project (OWASP®). OWASP Machine Learning Security Top Ten Security Risks. 2023. https://owasp.org/www-project-machine-learning-security-top-10/
[7] Cybersecurity and Infrastructure Security Agency. Secure by Design. 2023. https://www.cisa.gov/securebydesign
[8] National Security Agency. Embracing a Zero Trust Security Model. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
[9] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. 2022. https://www.cisa.gov/zero-trust-maturity-model
[10] Cybersecurity and Infrastructure Security Agency. Transforming the Vulnerability Management Landscape. 2022. https://www.cisa.gov/news-events/news/transforming-vulnerability-management-landscape

[11] Cybersecurity and Infrastructure Security Agency. Implementing Phishing-Resistant MFA. 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
[12] Canadian Centre for Cyber Security. Baseline security requirements for network security zones Ver. 2.0 (ITSP.80.022). 2021. https://www.cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-version-20-itsp80022
[13] Ji, Jessica. What Does AI Red-Teaming Actually Mean? 2023. https://cset.georgetown.edu/article/what-does-ai-red-teaming-actually-mean/
[14] Hugging Face GitHub. Safetensors. 2024. https://github.com/huggingface/safetensors.
[15] Michael Feffer, Anusha Sinha, Zachary C. Lipton, Hoda Heidari. Red-Teaming for Generative AI: Silver Bullet or Security Theater? 2024. https://arxiv.org/abs/2401.15897
[16] Google. Google's Secure AI Framework (SAIF). 2023. https://safety.google/cybersecurity-advancements/saif/
[17] Government Accountability Office (GAO). Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities. 2021. https://www.gao.gov/assets/gao-21-519sp.pdf
[18] RiskInsight. Attacking AI? A real-life example!. 2023. https://riskinsight-wavestone.com/en/2023/06/attacking-ai-a-real-life-example
[19] National Cyber Security Centre. Principles for the security of machine learning. 2022. https://www.ncsc.gov.uk/files/Principles-for-the-security-of-machine-learning.pdf

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring organizations' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

U.S. organizations:

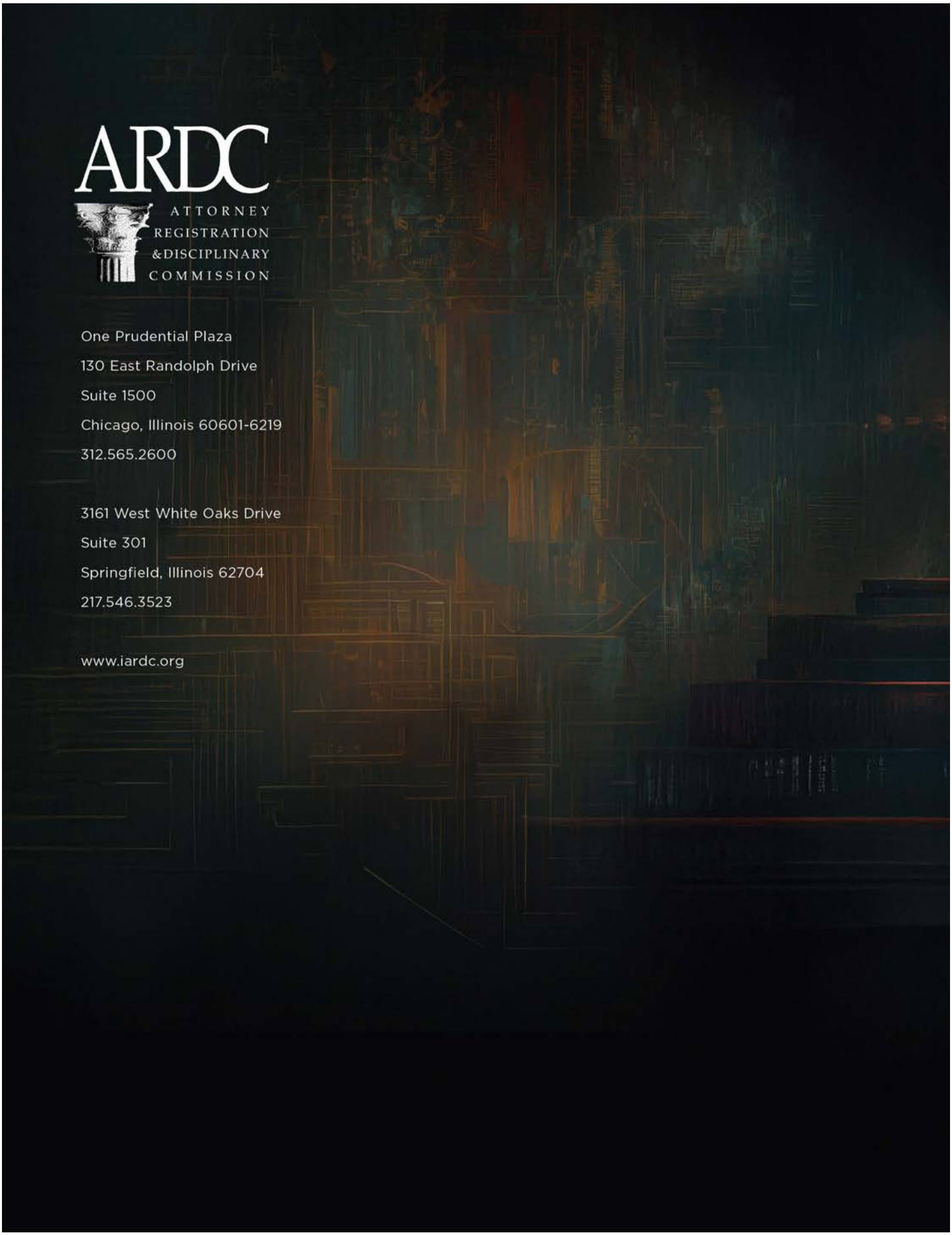
NSA Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
NSA General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
NSA Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov
Report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office.

Australian organizations: For more information or to report a cybersecurity incident, visit cyber.gov.au or call 1300 292 371 (1300 CYBER1).

Canadian organizations: For more information contact the Cyber Centre at contact@cyber.gc.ca or report a cyber security incident to our portal at https://www.cyber.gc.ca/en/incident-management.

New Zealand organizations: Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations: Report a significant cyber security incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.


ARDC
ATTORNEY
REGISTRATION
&DISCIPLINARY
COMMISSION
One Prudential Plaza
130 East Randolph Drive
Suite 1500
Chicago, Illinois 60601-6219
312.565.2600
3161 West White Oaks Drive
Suite 301
Springfield, Illinois 62704
217.546.3523
www.iardc.org

Chicago Daily Law Bulletin.

Lawyerport

ARDC shares guidance on AI in the legal profession

By Emma Oxnevad eoxnevad@lawbulletinmedia.com
Posted October 17, 2025 10:57 AM CDT

The Illinois Attorney Registration and Disciplinary Commission released guidance on the use of artificial intelligence in the legal profession.

The Illinois Attorney's Guide to Implementing AI, effective Oct. 1, is intended to complement the Illinois Supreme Court's official policy on AI usage, according to a written introduction from ARDC Administrator Lea S. Gutierrez. But the guide also includes detailed explanations about how different AI systems work, she wrote.

"While the court's policy sets the foundation, this guide focuses on the practical side — helping firms of all sizes apply that framework in daily practice," she wrote.

The guide states that attorneys must take a "structured approach" in selecting generative artificial intelligence (GAI) tools, which includes classifying the processed information by its risk classification: general information, de-identified information, confidential information and sensitive personal information.

It also distinguishes between different types of GAI tools. A third-party GAI tool is one where its essential components are "under the direct control of someone other than the lawyer or the law firm," according to the guide, and data transmitted by the tool becomes controlled by the same third-party.

Attorneys using third-party GAIs should employ the proper safeguards, like not transmitting confidential or sensitive personal information to platforms that allow the information to be used for model training. They should also investigate how long the tool retains information once deleted by the attorney or the service is terminated, in addition to requesting documentation about the provider's risk management practices to confirm, among other practices.

Lawyers can also use self-managed GAI tools, where the service is downloaded or deployed directly onto their own hardware or cloud infrastructure. But attorneys who use self-managed GAIs assume responsibility "for the full range of security, availability and compliance risks" associated.

The guide stated law firms that use self-managed GAI are responsible for developing secure deployment of platforms, monitoring for anomalies and suspicious activities, in addition to encryption and deletion of data, among other practices.

The guide also provides that attorneys "must be reasonable when selecting and using GAI tools to process their data" and that a client's consent is not a reasonable substitute for the previously stipulated diligence.

"We align with the American Bar Association's view that, where client consent is required, it must be informed," the guide states. "This guide focuses on implementation; lawyers retain professional judgment, consistent with Rules 1.4 and 1.6, to determine the nature and extent of client communication appropriate to the particular engagement and type of data processing contemplated."

The guide also provides detailed information into how different aspects of how GAIs operate, including model training, conversion and document storage and data isolation, among others.

The Illinois Supreme Court released its policy on AI in December, which stipulated that the Rules of Professional Conduct and the Code of Judicial Conduct "apply fully" to the use of AI.

Specifically, the high court stated that lawyers were permitted to use GAI but must thoroughly review and assume professional responsibility for any AI-generated work, in addition to requiring that attorneys understand GAI tools and maintain the privacy and security of confidential information with their use.

The full guide is available on the ARDC's website.

Practice Areas: Professional Liability

RULE 1.1: COMPETENCE

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

Adopted July 1, 2009, effective January 1, 2010.

Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] 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.

[4] A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person. See also Rule 6.2.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may

limit the matters for which the lawyer is responsible. See Rule 1.2(c).

Retaining Or Contracting With Other Lawyers

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. See also Rules 1.2(e) and Comment [15], 1.4, 1.5(f), 1.6, and 5.5(a). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the education, experience, and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[7] When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other and the client about the scope of their respective representations and the allocation of responsibility among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Maintaining Competence

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

Adopted July 1, 2009, effective January 1, 2010; amended Oct. 15, 2015, eff. Jan. 1, 2016; amended July 6, 2023, eff. immediately.

RULE 1.4: COMMUNICATION

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

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

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

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

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

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

Adopted July 1, 2009, effective January 1, 2010.

Comment

[1] Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.

Communicating with Client

[2] If these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client's consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously indicated that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. See Rule 1.2(a).

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations–depending on both the importance of the action under consideration and the feasibility of consulting with the client–this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with

the request, or if a prompt response is not feasible, that the lawyer, or a member of the lawyer's staff, acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications.

Explaining Matters

[5] The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, when there is time to explain a proposal made in a negotiation, the lawyer should review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(e).

[6] Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. See Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to the appropriate officials of the organization. See Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

Withholding Information

[7] In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client. Rule 3.4(c) directs compliance with such rules or orders.

Adopted July 1, 2009, effective January 1, 2010; amended Oct. 15, 2015, eff. Jan. 1, 2016.

RULE 1.6: CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b) or required by paragraph (c).

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

(1) to prevent the client from committing a crime in circumstances other than those specified in paragraph (c);

(2) to prevent the client from committing fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

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

(4) to secure legal advice about the lawyer's compliance with these Rules;

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

(6) to comply with other law or a court order; or

(7) to detect and resolve conflicts of interest if the revealed information would not prejudice the client.

(c) A lawyer shall reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to prevent reasonably certain death or substantial bodily harm.

(d) Information received by a lawyer participating in a meeting or proceeding with a trained intervener or panel of trained interveners of an approved lawyers' assistance program, or in an intermediary program approved by a circuit court in which nondisciplinary complaints against judges or lawyers can be referred, and information contained in communications between a user of an intermediary connecting service (ICS) and the ICS for purposes of the user seeking or obtaining a connection with a lawyer for the rendition of legal services or for the ICS facilitating the rendition of legal services by the lawyer, shall be considered information relating to the representation of a client for purposes of these Rules.

(e) 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.

Adopted July 1, 2009, effective January 1, 2010; amended Oct. 15, 2015, eff. Jan. 1, 2016; amended Apr. 1, 2025, eff. July 1, 2025.

Comment

[1] This Rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. See Rule 1.18 for the lawyer's duties with respect to information provided to the lawyer by a prospective client, Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client and Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Almost without exception, clients come to lawyers in order to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

[3] The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope.

[4] Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

Authorized Disclosure

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. Lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

Disclosure Adverse to Client

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions. Paragraph (c) recognizes the overriding value of life and physical integrity and requires disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial threat that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows from information relating to a representation that a client or other person has accidentally discharged toxic waste into a town's water must reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to eliminate the threat or reduce the number of victims.

[6A] Paragraph (b)(1) preserves the policy of the 1980 Illinois Code of Professional Responsibility and the 1990 Illinois Rules of Professional Conduct that permitted a lawyer to reveal the intention of a client to commit a crime. This general provision would permit disclosure where the client's intended conduct is a crime, including a financial crime, and the situation is not covered by paragraph (c).

[7] Paragraph (b)(2) is a limited exception to the rule of confidentiality that permits the lawyer to reveal information to the extent necessary to enable affected persons or appropriate authorities to prevent the client from committing fraud, as defined in Rule 1.0(d), that is reasonably certain to result in substantial injury to the financial or property interests of another and in furtherance of which the client has used or is using the lawyer's services. Such a serious abuse of the client-lawyer relationship by the client forfeits the protection of this Rule. The client can, of course, prevent such disclosure by refraining from the wrongful conduct. Like paragraph (b)(1), paragraph (b)(2) does not require the lawyer to reveal the client's misconduct, but the lawyer may not counsel or assist the client in conduct the lawyer knows is criminal or fraudulent. See Rule 1.2(d). See also Rule 1.16 with respect to the lawyer's obligation or right to withdraw from the representation of the client in such circumstances, and Rule 1.13(c), which permits the lawyer, where the client is an organization, to reveal information relating to the representation in limited circumstances.

[8] Paragraph (b)(3) addresses the situation in which the lawyer does not learn of the client's crime or fraud until after it has been consummated. Although the client no longer has the option of preventing disclosure by refraining from the wrongful conduct, there will be situations in which the loss suffered by the affected person can be prevented, rectified or mitigated. In such situations, the lawyer may disclose information relating to the representation to the extent necessary to enable the affected persons to prevent or mitigate reasonably certain losses or to attempt to recoup their losses. Paragraph (b)(3) does not apply when a person who has committed a crime or fraud thereafter employs a lawyer for representation concerning that offense.

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer's personal responsibility to comply with these Rules. In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

[10] Where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true with respect to a claim involving the conduct or representation of a former client. Such a charge can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, for example, a person claiming to have been defrauded by the lawyer and client acting together. The lawyer's right to respond arises when an assertion of such complicity has been made. Paragraph (b)(5) does not require the lawyer to await the commencement of an action or proceeding that charges such complicity, so that the defense may be established by responding directly to a third party who has made such an assertion. The right to defend also applies, of course, where a proceeding has been commenced.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the Rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Other law may require that a lawyer disclose information about a client. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of information relating to the representation appears to be required by other law, the lawyer must discuss the matter with the client to the extent required by Rule 1.4. If, however, the other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

Detection of Conflicts of Interest

[13] Paragraph (b)(7) recognizes that lawyers in different firms may need to disclose limited information to each other to detect and resolve conflicts of interest, such as when a lawyer is considering an association with another firm, two or more firms are considering a merger, or a lawyer is considering the purchase of a law practice. See Rule 1.17, Comment [7]. Under these circumstances, lawyers and law firms are permitted to disclose limited information, but only once substantive discussions regarding the new relationship have occurred. Even limited information should be disclosed only to the extent reasonably necessary. Moreover, the disclosure of any information is prohibited if it would prejudice the client (e.g., disclosure would compromise the attorney-client privilege; the fact that a corporate client is seeking advice on a corporate takeover that has not been publicly announced; that a person has consulted a lawyer about the possibility of divorce before the person's intentions are known to the person's spouse; or that a person has consulted a lawyer about a criminal investigation that has not led to a public charge). Under those

circumstances, paragraph (a) prohibits disclosure unless the client or former client gives informed consent. A lawyer's fiduciary duty to the lawyer's firm may also govern a lawyer's conduct when exploring an association with another firm and is beyond the scope of these Rules.

[14] Paragraph (b)(7) does not restrict the use of information acquired by means independent of any disclosure pursuant to paragraph (b)(7). Paragraph (b)(7) also does not affect the disclosure of information within a law firm when the disclosure is otherwise authorized, see Comment [5], such as when a lawyer in a firm discloses information to another lawyer in the same firm to detect and resolve conflicts of interest that could arise in connection with undertaking a new representation.

[15] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4. Unless review is sought, however, paragraph (b)(6) permits the lawyer to comply with the court's order.

[16] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified. Where practicable, the lawyer should first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose. If the disclosure will be made in connection with a judicial proceeding, the disclosure should be made in a manner that limits access to the information to the tribunal or other persons having a need to know it and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[17] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(7). In exercising the discretion conferred by this Rule, the lawyer may consider such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may be required, however, by other Rules. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). See Rules 1.2(d), 4.1(b), and 8.1. Rules 3.3 and 8.3, on the other hand, requires disclosure in some circumstances regardless of whether such disclosure is permitted by this Rule. See Rule 3.3(c).

Withdrawal

[17A] If the lawyer's services will be used by a client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw, as stated in Rule 1.16(a)(1). The lawyer may give notice of the fact of withdrawal regardless of whether the lawyer decides to disclose

information relating to a client's representation as permitted by paragraph (b). The lawyer may also withdraw or disaffirm any opinion or other document that had been prepared for the client or others. Where the client is an organization, the lawyer must also consider the provisions of Rule 1.13.

Acting Competently to Preserve Confidentiality

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

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

Former Client

[20] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the

disadvantage of the former client.

Lawyers' Assistance and Court Intermediary Programs

[21] Information about the fitness or conduct of a law student, lawyer or judge may be received by a lawyer while participating in an approved lawyers' assistance program. Protecting the confidentiality of such information encourages law students, lawyers and judges to seek assistance through such programs. Without such protection, law students, lawyers and judges may hesitate to seek assistance, to the detriment of clients and the public. Similarly, lawyers participating in an approved intermediary program established by a circuit court to resolve nondisciplinary issues among lawyers and judges may receive information about the fitness or conduct of a lawyer or judge. Paragraph (d) therefore provides that any information received by a lawyer participating in an approved lawyers' assistance program or an approved circuit court intermediary program will be protected as confidential client information for purposes of the Rules. See also Comment [5] to Rule 8.3.

Intermediary Connecting Services

[22] An intermediary connecting service (ICS) may require information from users who are seeking a lawyer, the disclosure of which could negatively impact their interests. For instance, a lead generator could require users to include their name, e-mail address, phone number, and specific information about their matter and then send an e-mail to participating lawyers, informing them that they have a new lead while including all the user's disclosed information. Without protecting information users of an ICS provide to the ICS for the purpose of seeking a lawyer or receiving legal assistance, the users may believe that disclosing information on an online form or website is not confidential and could be readily attainable by the public. Alternatively, a user may believe that his or her information is protected when that may not be true. By protecting that information, the public may be willing to seek representation through an ICS more freely.

[23] Additionally, paragraph (d) recognizes that an ICS may act as a participating lawyer's agent when the ICS is transmitting information between the user and lawyer for purposes of the lawyer rendering legal services, for instance, when an ICS provides a system by which a participating lawyer may communicate with the client. Consequently, a lawyer must act competently to safeguard information that is provided to or transmitted through the ICS. If a lawyer knows that an ICS will or plans to engage in the unauthorized disclosure of information relating to the representation of client, the lawyer shall make reasonable efforts to prevent the disclosure, including by remonstrating with the ICS, notifying the ICS of the lawyer's duty to take reasonable precautions to prevent the unauthorized disclosure of the information, and requesting the ICS not to disclose the information. The unauthorized disclosure of information relating to the representation of a client does not constitute a violation of paragraph (e) if the lawyer has made reasonable efforts to prevent the disclosure.

Adopted July 1, 2009, effective January 1, 2010; amended Oct. 15, 2015, eff. Jan. 1, 2016; Apr. 1, 2025, eff. July 1, 2025.

RULE 3.3: CANDOR TOWARD THE TRIBUNAL

(a) A lawyer shall not knowingly:

(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;

(2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or

(3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.

(d) In an *ex parte* proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

Adopted July 1, 2009, effective January 1, 2010.

Comment

[1] This Rule governs the conduct of a lawyer who is representing a client in the proceedings of a tribunal. See Rule 1.0(m) for the definition of "tribunal." It also applies when the lawyer is representing a client in an ancillary proceeding conducted pursuant to the tribunal's adjudicative authority, such as a deposition. Thus, for example, paragraph (a)(3) requires a lawyer to take reasonable remedial measures if the lawyer comes to know that a client who is testifying in a deposition has offered evidence that is false.

[2] This Rule sets forth the special duties of lawyers as officers of the court to avoid conduct that undermines the integrity of the adjudicative process. A lawyer acting as an advocate in an adjudicative proceeding has an obligation to present the client's case with persuasive force. Performance of that duty while maintaining confidences of the client, however, is qualified by the advocate's duty of candor to the tribunal. Consequently, although a lawyer in an adversary proceeding is not required to present an impartial exposition of the law or to vouch for the evidence submitted in a cause, the lawyer must not allow the tribunal to be misled by false statements of law or fact or evidence that the lawyer knows to be false.

Representations by a Lawyer

[3] An advocate is responsible for pleadings and other documents prepared for litigation, but is usually not required to have personal knowledge of matters asserted therein, for litigation documents ordinarily present assertions by the client, or by someone on the client's behalf, and not assertions by the lawyer. Compare Rule 3.1. However, an assertion purporting to be on the lawyer's own knowledge, as in an affidavit by the lawyer or in a statement in open court, may properly be made only when the lawyer knows the assertion is true or believes it to be true on the basis of a reasonably diligent inquiry. There are circumstances where failure to make a disclosure is the equivalent of an affirmative misrepresentation. The obligation prescribed in Rule 1.2(d) not to counsel a client to commit or assist the client in committing a fraud applies in litigation. Regarding compliance with Rule 1.2(d), see the Comment to that Rule. See also the Comment to Rule 8.4 (b).

Legal Argument

[4] Legal argument based on a knowingly false representation of law constitutes dishonesty toward the tribunal. A lawyer is not required to make a disinterested exposition of the law, but must recognize the existence of pertinent legal authorities. Furthermore, as stated in paragraph (a)(2), an advocate has a duty to disclose directly adverse authority in the controlling jurisdiction that has not been disclosed by the opposing party. The underlying concept is that legal argument is a discussion seeking to determine the legal premises properly applicable to the case.

Offering Evidence

[5] Paragraph (a)(3) requires that the lawyer refuse to offer evidence that the lawyer knows to be false, regardless of the client's wishes. This duty is premised on the lawyer's obligation as an officer of the court to prevent the trier of fact from being misled by false evidence. A lawyer does not violate this Rule if the lawyer offers the evidence for the purpose of establishing its falsity.

[6] If a lawyer knows that the client intends to testify falsely or wants the lawyer to introduce false evidence, the lawyer should seek to persuade the client that the evidence should not be offered. If the persuasion is ineffective and the lawyer continues to represent the client, the lawyer must refuse to offer the false evidence. If only a portion of a witness's testimony will be false, the lawyer may call the witness to testify but may not elicit or otherwise permit the witness to present the testimony that the lawyer knows is false.

[7] The duties stated in paragraphs (a) and (b) apply to all lawyers, including defense counsel in criminal cases. In some jurisdictions, however, courts have required counsel to present the accused as a witness or to give a narrative statement if the accused so desires, even if counsel knows that the testimony or statement will be false. The obligation of the advocate under the Rules of Professional Conduct is subordinate to such requirements. See also Comment [9].

[8] The prohibition against offering false evidence only applies if the lawyer knows that the evidence is false. A lawyer's reasonable belief that evidence is false does not preclude its presentation to the trier of fact. A lawyer's knowledge that evidence is false, however, can be inferred from the circumstances. See Rule 1.0(f). Thus, although a lawyer should resolve doubts

about the veracity of testimony or other evidence in favor of the client, the lawyer cannot ignore an obvious falsehood.

[9] Although paragraph (a)(3) only prohibits a lawyer from offering evidence the lawyer knows to be false, it permits the lawyer to refuse to offer testimony or other proof that the lawyer reasonably believes is false. Offering such proof may reflect adversely on the lawyer's ability to discriminate in the quality of evidence and thus impair the lawyer's effectiveness as an advocate. Because of the special protections historically provided criminal defendants, however, this Rule does not permit a lawyer to refuse to offer the testimony of such a client where the lawyer reasonably believes but does not know that the testimony will be false. Unless the lawyer knows the testimony will be false, the lawyer must honor the client's decision to testify. See also Comment [7].

Remedial Measures

[10] Having offered material evidence in the belief that it was true, a lawyer may subsequently come to know that the evidence is false. Or, a lawyer may be surprised when the lawyer's client, or another witness called by the lawyer, offers testimony the lawyer knows to be false, either during the lawyer's direct examination or in response to cross-examination by the opposing lawyer. In such situations or if the lawyer knows of the falsity of testimony elicited from the client during a deposition, the lawyer must take reasonable remedial measures. In such situations, the advocate's proper course is to remonstrate with the client confidentially, advise the client of the lawyer's duty of candor to the tribunal and seek the client's cooperation with respect to the withdrawal or correction of the false statements or evidence. If that fails, the advocate must take further remedial action. If withdrawal from the representation is not permitted or will not undo the effect of the false evidence, the advocate must make such disclosure to the tribunal as is reasonably necessary to remedy the situation, even if doing so requires the lawyer to reveal information that otherwise would be protected by Rule 1.6. It is for the tribunal then to determine what should be done–making a statement about the matter to the trier of fact, ordering a mistrial or perhaps nothing.

[11] The disclosure of a client's false testimony can result in grave consequences to the client, including not only a sense of betrayal but also loss of the case and perhaps a prosecution for perjury. But the alternative is that the lawyer cooperate in deceiving the court, thereby subverting the truth-finding process which the adversary system is designed to implement. See Rule 1.2(d). Furthermore, unless it is clearly understood that the lawyer will act upon the duty to disclose the existence of false evidence, the client can simply reject the lawyer's advice to reveal the false evidence and insist that the lawyer keep silent. Thus the client could in effect coerce the lawyer into being a party to fraud on the court.

Preserving Integrity of Adjudicative Process

[12] Lawyers have a special obligation to protect a tribunal against criminal or fraudulent conduct that undermines the integrity of the adjudicative process, such as bribing, intimidating or otherwise unlawfully communicating with a witness, juror, court official or other participant in the

proceeding, unlawfully destroying or concealing documents or other evidence or failing to disclose information to the tribunal when required by law to do so. Thus, paragraph (b) requires a lawyer to take reasonable remedial measures, including disclosure if necessary, whenever the lawyer knows that a person, including the lawyer's client, intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding.

Duration of Obligation

[13] A practical time limit on the obligation to rectify false evidence or false statements of law and fact has to be established. The conclusion of the proceeding is a reasonably definite point for the termination of the obligation. A proceeding has concluded within the meaning of this Rule when a final judgment in the proceeding has been affirmed on appeal or the time for review has passed.

***Ex Parte* Proceedings**

[14] Ordinarily, an advocate has the limited responsibility of presenting one side of the matters that a tribunal should consider in reaching a decision; the conflicting position is expected to be presented by the opposing party. However, in any *ex parte* proceeding, such as an application for a temporary restraining order, there is no balance of presentation by opposing advocates. The object of an *ex parte* proceeding is nevertheless to yield a substantially just result. The judge has an affirmative responsibility to accord the absent party just consideration. The lawyer for the represented party has the correlative duty to make disclosures of material facts known to the lawyer and that the lawyer reasonably believes are necessary to an informed decision.

Withdrawal

[15] Normally, a lawyer's compliance with the duty of candor imposed by this Rule does not require that the lawyer withdraw from the representation of a client whose interests will be or have been adversely affected by the lawyer's disclosure. The lawyer may, however, be required by Rule 1.16(a) to seek permission of the tribunal to withdraw if the lawyer's compliance with this Rule's duty of candor results in such an extreme deterioration of the client-lawyer relationship that the lawyer can no longer competently represent the client. Also see Rule 1.16(b) for the circumstances in which a lawyer will be permitted to seek a tribunal's permission to withdraw. In connection with a request for permission to withdraw that is premised on a client's misconduct, a lawyer may reveal information relating to the representation only to the extent reasonably necessary to comply with this Rule or as otherwise permitted by Rule 1.6.

Adopted July 1, 2009, effective January 1, 2010.

RULE 8.4: MISCONDUCT

It is professional misconduct for a lawyer to:

(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another.

(b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness, or fitness as a lawyer in other respects.

(c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.

(d) engage in conduct that is prejudicial to the administration of justice.

(e) state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law.

(f) knowingly assist a judge or judicial officer in conduct that is a violation of applicable rules of judicial conduct or other law. Nor shall a lawyer give or lend anything of value to a judge, official, or employee of a tribunal, except those gifts or loans that a judge or a member of the judge's family may receive under Canon 3, Rule 3.13, of the Illinois Code of Judicial Conduct of 2023. Permissible campaign contributions to a judge or candidate for judicial office may be made only by check, draft, or other instrument payable to or to the order of an entity that the lawyer reasonably believes to be a political committee supporting such judge or candidate. Provision of volunteer services by a lawyer to a political committee shall not be deemed to violate this paragraph.

(g) present, participate in presenting, or threaten to present criminal or professional disciplinary charges to obtain an advantage in a civil matter.

(h) enter into an agreement with a client or former client limiting or purporting to limit the right of the client or former client to file or pursue any complaint before the Illinois Attorney Registration and Disciplinary Commission.

(i) avoid in bad faith the repayment of an education loan guaranteed by the Illinois Student Assistance Commission or other governmental entity. The lawful discharge of an education loan in a bankruptcy proceeding shall not constitute bad faith under this paragraph, but the discharge shall not preclude a review of the lawyer's conduct to determine if it constitutes bad faith.

(j) engage in conduct in the practice of law that the lawyer knows or reasonably should know is harassment or discrimination on the basis of race, color, ancestry, sex, religion, national origin, ethnicity, disability, age, sexual orientation, gender identity, gender expression, marital status, military or veteran status, pregnancy, or socioeconomic status. This paragraph does not limit the ability of a lawyer to accept, decline, or, in accordance with Rule 1.16, withdraw from a representation. This paragraph does not preclude or limit the giving of advice, assistance, or advocacy consistent with these Rules.

(k) if the lawyer holds public office:

(1) use that office to obtain, or attempt to obtain, a special advantage in a legislative matter for a client under circumstances where the lawyer knows or reasonably should know that such action is not in the public interest;

(2) use that office to influence, or attempt to influence, a tribunal to act in favor of a client;

or

(3) represent any client, including a municipal corporation or other public body, in the promotion or defeat of legislative or other proposals pending before the public body of which such lawyer is a member or by which such lawyer is employed.

Adopted July 1, 2009, effective January 1, 2010; amended May 25, 2022, eff. immediately; amended Dec. 30, 2022, eff. Jan. 1, 2023; amended May 30, 2024, eff. July 1, 2024.

Comment

[1] Lawyers are subject to discipline when they violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so or do so through the acts of another, as when they request or instruct an agent to do so on the lawyer's behalf. Paragraph (a), however, does not prohibit a lawyer from advising a client concerning action the client is legally entitled to take.

[2] Many kinds of illegal conduct reflect adversely on fitness to practice law, such as offenses involving fraud and the offense of willful failure to file an income tax return. However, some kinds of offenses carry no such implication. Traditionally, the distinction was drawn in terms of offenses involving "moral turpitude." That concept can be construed to include offenses concerning some matters of personal morality, such as adultery and comparable offenses, that have no specific connection to fitness for the practice of law. Although a lawyer is personally answerable to the entire criminal law, a lawyer should be professionally answerable only for offenses that indicate lack of those characteristics relevant to law practice. Offenses involving violence, dishonesty, breach of trust, or serious interference with the administration of justice are in that category. A pattern of repeated offenses, even ones of minor significance when considered separately, can indicate indifference to legal obligation.

[3] Discrimination and harassment by lawyers in the practice of law in violation of paragraph (j) undermines confidence in the legal profession and the legal system. Conduct in the practice of law includes representing clients; interacting with witnesses, coworkers, court personnel, lawyers, and others when representing clients; operating or managing a law firm or law practice; and participating in law-related professional activities or events, including law firm or bar association educational or social events. Conduct protected by the Constitutions of the United States or the State of Illinois, including a lawyer's expression of views on matters of public concern in the context of teaching, public speaking, or other forms of public advocacy, does not violate this paragraph.

[3A] The Rules of Professional Conduct are rules of reason, and whether conduct violates paragraph (j) must be judged in context and from an objectively reasonable perspective. See Scope, paragraph [14]. Discrimination means harmful verbal or physical conduct directed at another person or group that manifests bias or prejudice on the basis of any characteristics identified in paragraph (j). Harassment includes conduct directed at another person or group that is invasive, pressuring, or intimidating in relation to any characteristic identified in paragraph (j). It includes

sexual harassment and derogatory or demeaning verbal or physical conduct. Sexual harassment includes unwelcome sexual advances, requests for sexual favors, and other unwelcome verbal or physical conduct of a sexual nature. The substantive law of antidiscrimination and antiharassment statutes and caselaw may guide the application of paragraph (j) and the evaluation of whether specific conduct constitutes discrimination or harassment. In addition, any judicial or administrative tribunal findings involving the same conduct may be considered in assessing whether a lawyer has violated paragraph (j). A trial judge's finding that preemptory challenges were exercised on a discriminatory basis does not alone establish a violation of paragraph (j).

[3B] Lawyers may engage in conduct undertaken to promote diversity and inclusion without violating paragraph (j) by, for example, implementing initiatives to encourage recruiting, hiring, retaining, and advancing diverse employees or sponsoring diverse law student organizations. A lawyer does not violate paragraph (j) by limiting the scope or subject matter of the lawyer's practice or by limiting the lawyer's practice to members of underserved populations in accordance with these Rules and other law. A lawyer may charge and collect reasonable fees and expenses for a representation. See Rule 1.5(a). Lawyers should be mindful of their obligation under Rule 6.2 not to avoid appointments from a tribunal except for good cause. A lawyer's representation of a client does not constitute an endorsement by the lawyer of the client's views or activities. See Rule 1.2(b).

[4] A lawyer may refuse to comply with an obligation imposed by law upon a good-faith belief that no valid obligation exists. The provisions of Rule 1.2(d) concerning a good-faith challenge to the validity, scope, meaning or application of the law apply to challenges of legal regulation of the practice of law.

[5] Lawyers holding public office assume legal responsibilities going beyond those of other citizens. A lawyer's abuse of public office can suggest an inability to fulfill the professional role of lawyers. The same is true of abuse of positions of private trust such as trustee, executor, administrator, guardian, agent and officer, director or manager of a corporation or other organization.

Adopted July 1, 2009, effective January 1, 2010; amended May 30, 2024, eff. July 1, 2024.

PANEL 6 — 3:55 - 4:55pm

Whose work is it when you use AI or other tech? Does it matter? Know your duties under the rules

Panelists: **Richard C. Gleason,** Litigation Group Manager, *Illinois ARDC*

Kathryne "Katie" R. Hayes, Partner, *Collins Bargione & Vuckovich*

Daniel F. Konicek, Partner, *Konicek & Dillon, P.C.*

Richard C. Gleason, Litigation Group Manager, *Illinois ARDC*

Rich is Litigation Counsel at the Illinois Attorney Registration and Disciplinary Commission of the Supreme Court of Illinois (ARDC), where he investigates and prosecutes allegations of lawyer misconduct. Prior to joining the ARDC, Rich worked as a managing partner at O'Mara, Gleason, & O'Callaghan, LLC in Chicago and as a Cook County Assistant State's Attorney. He received his undergraduate degree from University of Iowa and his law degree from Northern Illinois University.

Kathryne "Katie" R. Hayes, Partner, *Collins Bargione & Vuckovich*

Katie is a partner at Collins Bargione & Vuckovich where her practice includes ARDC defense, legal malpractice, ethics counseling, commercial litigation and civil appeals. She serves as outside ethics counsel to solo practitioners and law firms in Chicago in various matters relating to professional responsibility and liability.

Katie was peer selected as a Leading Lawyer Emerging Lawyer (2023, 2022) in the areas of Commercial Litigation and Professional Malpractice Defense Law: Including Legal/Technical/Financial. Katie also is a member of Illinois State Bar Association and the Chicago Bar Association and previously served as a co-chair of the CBA's YLS Professional Responsibility Committee. She was appointed to serve as the Vice-Chair of the ISBA Standing Committee on Professional Conduct for 2022-2023 and to serve as the Vice-Chair of the ISBA Attorney Registration & Disciplinary Commission committee for 2022-2023.

Daniel F. Konicek, Partner, *Konicek & Dillon, P.C.*

Dan is founding partner of Konicek & Dillon, P.C., where he practices in the areas of professional liability, commercial litigation, and personal injury. He has tried over 100 jury trials to verdict in the state and federal courts. He has represented clients in administrative hearings before the Department of Professional Regulation and before the Attorney Disciplinary Commission.

In 2016, Dan was awarded Outstanding Defense Verdict in a legal malpractice case by the Illinois Jury Verdict Reporter at their Annual JVR Awards for Trial Lawyer Excellence. In 2000, Dan was honored as one of Illinois' top lawyers by inclusion in the 40 Under 40 Illinois Attorneys to Watch and has been named as an Illinois Super Lawyer since 2006. He is a current member of the Leading Lawyers Network, the Multi-Million Dollar Advocates Forum, Illinois Trial Lawyers, where he serves on the ITLA Board of Managers, and Litigation Counsel of America.

His jury trials include complex commercial cases involving fraud, aiding and abetting, conspiracy, professional negligence, medical negligence, product liability, and breach of fiduciary duty. Dan has successfully resolved many cases for millions of dollars for his clients, including recent settlements for $8,000,000 against multiple defendants in a breach of fiduciary duty case; $18,000,000 in an aiding and abetting fraud case; $1,000,000 in a legal malpractice. In terms of trials, Dan most recently he successfully tried a medical negligence case against a neurologist and large hospital securing a $10,500,000 verdict that was paid in 28 days.

Dan's recent defense cases include a successful "not guilty" for his prominent client who ran for Senate. Dan defended his client in a legal negligence case in the Northern District Federal Court of Iowa, where Plaintiff sought over $5,000,000 for alleged malfeasance in handling a complex shareholder dispute. In the Northern District Federal Court of Illinois, Dan obtained a "not guilty" for his lawyer client in an aiding and abetting wire fraud case seeking $10,000,000. Notably, in the Northern Illinois District case, the alleged co-conspirators all plead guilty to federal wire fraud charges and were serving prison terms at the time of trial. Their pleas of guilt were admitted and read to the jury, over objection, and used against Dan's client. Notwithstanding, Dan successfully argued his client was an unwitting and unknowing "participant" in the criminal scheme.

Whose work is it when you use AI or other tech? Does it matter? Know your duties under the rules

Richard C. Gleason, Litigation Group Manager, *Illinois ARDC*

Kathryne "Katie" R. Hayes, Partner, *Collins Bargione & Vuckovich*

Daniel F. Konicek, Partner, *Konicek & Dillon, P.C.*

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Does what I don't know even matter anymore since AI can give me the answer?

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Why my use and understanding of AI matters:

- Will I know if AI is wrong or missed something?
- Will I know if I am using AI wrong or in a dangerous manner?
- Who is arguing the case and answering questions from the Court? (Probably not AI.)
- Do the Illinois Rules of Professional Conduct apply to AI?

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Thoughts for this discussion:

- Can I sign a pleading/brief that was generated by AI?
- Does a lawyer's signature mean they are representing that they authored the product or simply that they are taking responsibility for the filing?
- Can I submit someone else's work?
- Is this a new problem? Have non-drafters been signing other people's work since the beginning of the profession?
- Is checking/correcting the citations enough to avoid a potential problem?

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Short answer:

"You maintain ultimate responsibility …"

THINKING ABOUT USING GENERATIVE AI?
JUDICIAL AI UTILIZATION GUIDELINES

Ethical Oversight - The Code of Judicial Conduct applies fully to the use of AI technologies. You maintain ultimate responsibility for all rulings and legal documents.

Attribution - Ensure your work product does not infringe upon copyright or intellectual property rights by proper attribution to sources as necessary.

Competence - The judicial branch must stay informed about evolving AI technologies. Prior to using any technology, including generative AI applications, you need to understand both general AI capabilities and the specific tools being used.

Confidentiality - If using a public generative AI tool (like ChatGPT), your input prompt is being handed over to the technology. Ensure you do not compromise sensitive information. Do not input any information such as (non-exhaustive list):

- Confidential or privileged information;
- Personal identifying information;
- Protected health information;
- Justice and public safety information;
- Code containing passwords or security-related information; and
- Information that has potential to erode public trust.

Accuracy - Be mindful that content from generative AI applications comes from sourced material. AI-generated content must be thoroughly reviewed to ensure accuracy and compliance with legal and ethical obligations, including a specific need to guard against technology lending to unintentional bias or prejudice.

WHAT TO WATCH FOR AS A JUDGE

AI is ubiquitously present in modern technology. It is safe to assume AI was used in pleadings and other written materials. Generative AI applications gives rise to these considerations:

Hallucinations - When generative AI produces output that appears realistic but is misleading or made up by the AI itself rather than real-world data or input. If generative AI was used in a legal pleading or brief, included citations may be entirely made up or be a real case but not contain the purported language cited. Read a case decision on hallucinations.

CHECK CITATIONS

Deepfakes - When generative AI is intentionally used to produce convincing/deceptive media - images, audio, video, etc. Fake evidence is relatively easy to create and reliable technology solutions do not exist to identify real vs fake evidence. Learn more about identification of deepfakes.

HEAR EVIDENCE ON FOUNDATIONS

Extended Reality - Technology can seamlessly be integrated with our person though wearable devices. Recognize that technology may allow an individual to record and analyze audio and video and channel information from other sources in real-time, potentially without detection. Learn more about extended reality.

ENFORCE EXISTING TECHNOLOGY RULES

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

AI is not the lawyer responsible for my case.

- Rule 1.1 (Competence) - A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
  - Comment [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.
  - (Proposed change to CA Rule and comment - "a lawyer must independently review, verify and exercise professional judgment regarding any output generated by the technology that is used in connection with representing a client."
    - Is this additional proposed language necessary?
- Rule 1.3 (Diligence) – A lawyer shall act with reasonable diligence and promptness in representing a client.

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Do I need to be concerned about the content AI is suggesting?

- *In re Steinberg*, 620 N.Y.S.2d 345 (N.Y. App. Div. 1994) (lawyer seeking to be named to court's panel of attorneys eligible for appointment in felony cases submitted plagiarized writing samples)
- Cooper J. Strickland, *The Dark Side of Unattributed Copying and the Ethical Implications of Plagiarism in the Legal Profession*, 90 N.C. L. Rev. 920 (2012) (proposing comment to Rule 8.4 clarifying when it is acceptable to copy without attribution). See also Andrew M. Carter, *The Case for Plagiarism*, 9 UC Irvine L. Rev. 531 (2019)
- *Tremblay v. OpenAI*, 2024 U.S. Dist. Lexis 141362 (N.D. Cal. Feb. 12, 2024)

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Do I need to be concerned about the content AI is suggesting?

- Judge orders OpenAI to turn over 20,000,000 ChatGPT queries to NYT in lawsuit (January 2026): https://www.abajournal.com/news/article/chatgpt-creator-must-turn-over-20m-chat-logs-in-copyright-litigation-federal-judge-says
- United States v Heppner, No, 25 CR 503 (S.D.N.Y. Feb. 17, 2026)
- Coder shares Anthropic code: https://www.nytimes.com/2026/04/22/technology/anthropic-code-leak-copyright.html?unlocked_article_code=1.eVA.5cbV.TR52wk2lNUBX&smid=url-share
- Rule 8.4(c)(Misconduct) – It is professional misconduct for a lawyer to: (c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Who controls how the work is completed?

- Your employer
- (Maybe) your client
  - Rule 1.2 (Scope of Representation and Allocation of Authority Between Client and Lawyer)
  - Rule 1.2(a) – Subject to paragraphs and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. …
  - Rule 1.2(e) – After accepting employment on behalf of a client, a lawyer shall not thereafter delegate to another lawyer not in the lawyer's firm the responsibility for performing or completing that employment, without the client's informed consent.

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Should I talk to my client before using generative AI?

- Rule 1.4(a)(2) – A lawyer shall: (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished[.]
- See also Comment [2] to Rule 1.4 – If these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client's consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take. …

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

Hypo: AI as Junior Associate.

A partner instructs associates to use AI to draft first versions of all memos to improve efficiency. Associates rely heavily on AI and reduce independent legal analysis.

Rule 5.1 (supervisory responsibilities)

Rule 5.3 (nonlawyer assistance)

Are there [long-term] competency risks under Rule 1.1?

Does overreliance on AI erode professional judgment—and is that an ethical issue or just a training concern?

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

What input/influence does the client have on how the work is completed?

- Can a client insist upon or forbid the use of generative AI?
  - "Informed consent" (Rule 1.0.) – denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.
    - Is informed consent from a client required before I use AI?
  - What if a client wants me to use generative AI to save time (money), but I think it's a bad idea? Can I protect myself? (See Rule 1.8(h)(h)(1) – A lawyer shall **NOT**: (1) make an agreement prospectively limiting the lawyer's liability to a client for malpractice unless the client is independently represented in making the agreement[.].)
    - A lawyer is their client's fiduciary and owes a duty to a client.
    - Lawyers are (often) blamed when something goes wrong.

ETHICS 2026 HOSTED BY Law Bulletin SEMINARS Knowledge for Success

How is the work billed?

Rule 1.5 (Fees)

https://ilcourtsaudio.blob.core.windows.net/antilles-resources/resources/ce9cba94-4700-49ed-9183-a43cfcd0c3a5/RULE%201.5.pdf

Iowa Sup. Ct. Bd. of Prof'l Ethics & Conduct v. Lane, 642 N.W.2d 296 (Iowa 2002) (lawyer suspended for submitting an application for attorneys' fees that included a charge of $16,000 for a brief that the lawyer had plagiarized from a treatise)

Hypo (Ghostwriter) - A litigation associate uses generative AI to draft a motion to dismiss. The lawyer revises it but 60–70% of the structure and language originated from AI. (Optional: The client is billed for 8 hours of "drafting and research.")

Who is the author of the work produced?

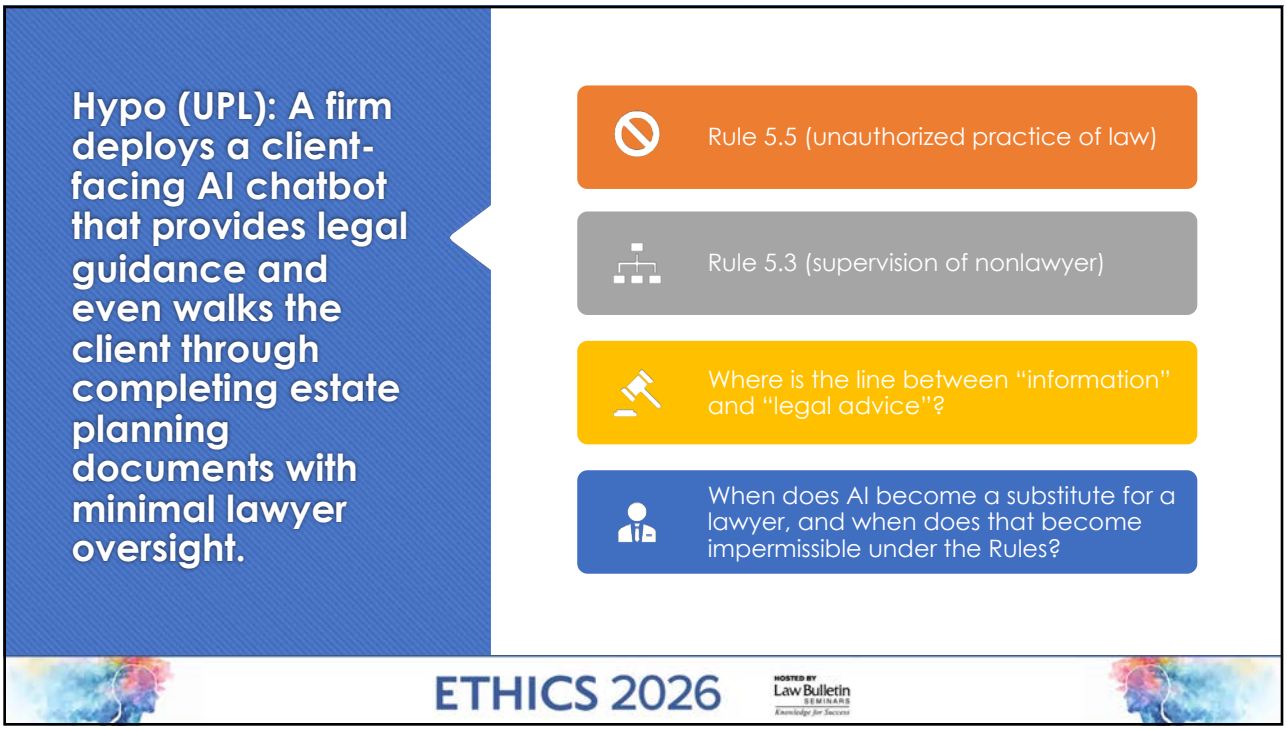
What due diligence is required under Rule 1.1 (technology competence)?

Does Rule 1.1 (competence) require disclosure if the lawyer cannot fully explain the AI's reasoning?

Should the lawyer disclose AI use to the client?

Are there copyright considerations?

(Optional: Does billing implicate Rule 1.5 (reasonableness/value)?)


Hypo (UPL): A firm deploys a client-facing AI chatbot that provides legal guidance and even walks the client through completing estate planning documents with minimal lawyer oversight.
Rule 5.5 (unauthorized practice of law)
Rule 5.3 (supervision of nonlawyer)
Where is the line between "information" and "legal advice"?
When does AI become a substitute for a lawyer, and when does that become impermissible under the Rules?
ETHICS 2026
HOSTED BY Law Bulletin SEMINARS

ILLINOIS SUPREME COURT POLICY ON ARTIFICIAL INTELLIGENCE

JUDICIAL REFERENCE SHEET

JANUARY 1, 2025

WHAT IS ARTIFICIAL INTELLIGENCE?

Technology that simulates human intelligence, enabling machines to learn, reason, perceive, and make decisions.
Artificial Intelligence is not new technology.

1950s Origins of AI

Examples: Spell check, predicative typing, facial recognition, and computer based legal research.

2022 Mainstream Availability of Generative AI

Examples:
Text Composition Prompts
"Summarize the following legal brief and identify key arguments."

"Rewrite this paragraph in a respectful and neutral tone using plain language so it can be understood by people without legal expertise."

"Prepare a speech about the importance of procedural due process for an audience of judges."

Photo/Audio/Video Prompts
"Create image of an Illinois Courtroom."

"Create movie depicting President Abraham Lincoln conducting legal research on a computer."

WHAT IS GENERATIVE ARTIFICIAL INTELLIGENCE?

A subset of artificial intelligence focused on creating new content, such as text, images, and video, by learning from existing data.
Generative AI is a relatively new tool.

WANT TO KNOW MORE?

National Center for State Courts AI Resource Center

Description of AI and Court Use Cases Video

JUDICIAL DECISIONS

Judges remain ultimately responsible for their decisions, irrespective of technological advancements.

Code of Judicial Conduct - Rule 2.7
A judge shall hear and **decide** matters assigned to the judge...

Code of Judicial Conduct - Rule 1.2
A judge shall act at all times in a manner that promotes public confidence in the independence, integrity, and impartiality of the judiciary...

PLEADINGS

Lawyers & Self Represented Litigants are subject to sanctions for submitting legally or factually unfounded pleadings.

Illinois Supreme Court Rule 137
The signature of an attorney or party constitutes a certificate by him that he has read the pleading, motion or other document; that to the best of his knowledge, information, and belief formed after reasonable inquiry it is well grounded in fact and is warranted by existing law...

THINKING ABOUT USING GENERATIVE AI? JUDICIAL AI UTILIZATION GUIDELINES

Ethical Oversight - The Code of Judicial Conduct applies fully to the use of AI technologies. You maintain ultimate responsibility for all rulings and legal documents.

Competence - The judicial branch must stay informed about evolving AI technologies. Prior to using any technology, including generative AI applications, you need to understand both general AI capabilities and the specific tools being used.

Accuracy - Be mindful that content from generative AI applications comes from sourced material. AI-generated content must be thoroughly reviewed to ensure accuracy and compliance with legal and ethical obligations, including a specific need to guard against technology lending to unintentional bias or prejudice.

Attribution - Ensure your work product does not infringe upon copyright or intellectual property rights by proper attribution to sources as necessary.

Confidentiality - If using a public generative AI tool (like ChatGPT), your input prompt is being handed over to the technology. Ensure you do not compromise sensitive information. Do not input any information such as (non-exhaustive list):

- Confidential or privileged information;
- Personal identifying information;
- Protected health information;
- Justice and public safety information;
- Code containing passwords or security-related information; and
- Information that has potential to erode public trust.

WHAT TO WATCH FOR AS A JUDGE

AI is ubiquitously present in modern technology. It is safe to assume AI was used in pleadings and other written materials. Generative AI applications gives rise to these considerations:

Hallucinations - When generative AI produces output that appears realistic but is misleading or made up by the AI itself rather than real-world data or input. If generative AI was used in a legal pleading or brief, included citations may be entirely made up or be a real case but not contain the purported language cited. Read a case decision on hallucinations.

Deepfakes - When generative AI is intentionally used to produce convincing/deceptive media - images, audio, video, etc. Fake evidence is relatively easy to create and reliable technology solutions do not exist to identify real vs fake evidence. Learn more about identification of deepfakes.

Extended Reality - Technology can seamlessly be integrated with our person though wearable devices. Recognize that technology may allow an individual to record and analyze audio and video and channel information from other sources in real-time, potentially without detection. Learn more about extended reality.

CHECK CITATIONS

HEAR EVIDENCE ON FOUNDATIONS

ENFORCE EXISTING TECHNOLOGY RULES

RULE 1.1: COMPETENCE

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

Adopted July 1, 2009, effective January 1, 2010.

Comment

Legal Knowledge and Skill

[1] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] 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.

[4] A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person. See also Rule 6.2.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more extensive treatment than matters of lesser complexity and consequence. An agreement between the lawyer and the client regarding the scope of the representation may

limit the matters for which the lawyer is responsible. See Rule 1.2(c).

Retaining Or Contracting With Other Lawyers

[6] Before a lawyer retains or contracts with other lawyers outside the lawyer's own firm to provide or assist in the provision of legal services to a client, the lawyer should ordinarily obtain informed consent from the client and must reasonably believe that the other lawyers' services will contribute to the competent and ethical representation of the client. See also Rules 1.2(e) and Comment [15], 1.4, 1.5(f), 1.6, and 5.5(a). The reasonableness of the decision to retain or contract with other lawyers outside the lawyer's own firm will depend upon the circumstances, including the education, experience, and reputation of the nonfirm lawyers; the nature of the services assigned to the nonfirm lawyers; and the legal protections, professional conduct rules, and ethical environments of the jurisdictions in which the services will be performed, particularly relating to confidential information.

[7] When lawyers from more than one law firm are providing legal services to the client on a particular matter, the lawyers ordinarily should consult with each other and the client about the scope of their respective representations and the allocation of responsibility among them. See Rule 1.2. When making allocations of responsibility in a matter pending before a tribunal, lawyers and parties may have additional obligations that are a matter of law beyond the scope of these Rules.

Maintaining Competence

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

Adopted July 1, 2009, effective January 1, 2010; amended Oct. 15, 2015, eff. Jan. 1, 2016; amended July 6, 2023, eff. immediately.

RULE 1.2: SCOPE OF REPRESENTATION AND ALLOCATION OF AUTHORITY BETWEEN CLIENT AND LAWYER

(a) Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. A lawyer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.

(b) A lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities.

(c) A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.

(d) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may

(1) discuss the legal consequences of any proposed course of conduct with a client,

(2) counsel or assist a client to make a good-faith effort to determine the validity, scope, meaning or application of the law, and

(3) counsel or assist a client in conduct expressly permitted by Illinois law that may violate or conflict with federal or other law, as long as the lawyer advises the client about that federal or other law and its potential consequences.

(e) After accepting employment on behalf of a client, a lawyer shall not thereafter delegate to another lawyer not in the lawyer's firm the responsibility for performing or completing that employment, without the client's informed consent.

Adopted July 1, 2009, effective January 1, 2010; amended Oct. 15, 2015, eff. Jan. 1, 2016.

Comment

Allocation of Authority between Client and Lawyer

[1] Paragraph (a) confers upon the client the ultimate authority to determine the purposes to be served by legal representation, within the limits imposed by law and the lawyer's professional obligations. The decisions specified in paragraph (a), such as whether to settle a civil matter, must also be made by the client. See Rule 1.4(a)(1) for the lawyer's duty to communicate with the client about such decisions. With respect to the means by which the client's objectives are to be pursued, the lawyer shall consult with the client as required by Rule 1.4(a)(2) and may take such action as is impliedly authorized to carry out the representation.

[2] On occasion, however, a lawyer and a client may disagree about the means to be used to accomplish the client's objectives. Clients normally defer to the special knowledge and skill of their lawyer with respect to the means to be used to accomplish their objectives, particularly with respect to technical, legal and tactical matters. Conversely, lawyers usually defer to the client regarding such questions as the expense to be incurred and concern for third persons who might

be adversely affected. Because of the varied nature of the matters about which a lawyer and client might disagree and because the actions in question may implicate the interests of a tribunal or other persons, this Rule does not prescribe how such disagreements are to be resolved. Other law, however, may be applicable and should be consulted by the lawyer. The lawyer should also consult with the client and seek a mutually acceptable resolution of the disagreement. If such efforts are unavailing and the lawyer has a fundamental disagreement with the client, the lawyer may withdraw from the representation. See Rule 1.16(b)(4). Conversely, the client may resolve the disagreement by discharging the lawyer. See Rule 1.16(a)(3).

[3] At the outset of a representation, the client may authorize the lawyer to take specific action on the client's behalf without further consultation. Absent a material change in circumstances and subject to Rule 1.4, a lawyer may rely on such an advance authorization. The client may, however, revoke such authority at any time.

[4] In a case in which the client appears to be suffering diminished capacity, the lawyer's duty to abide by the client's decisions is to be guided by reference to Rule 1.14.

Independence from Client's Views or Activities

[5] Legal representation should not be denied to people who are unable to afford legal services, or whose cause is controversial or the subject of popular disapproval. By the same token, representing a client does not constitute approval of the client's views or activities.

Agreements Limiting Scope of Representation

[6] The scope of services to be provided by a lawyer may be limited by agreement with the client or by the terms under which the lawyer's services are made available to the client. When a lawyer has been retained by an insurer to represent an insured, for example, the representation may be limited to matters related to the insurance coverage. A limited representation may be appropriate because the client has limited objectives for the representation. In addition, the terms upon which representation is undertaken may exclude specific means that might otherwise be used to accomplish the client's objectives. Such limitations may exclude actions that the client thinks are too costly or that the lawyer regards as repugnant or imprudent.

[7] Although this Rule affords the lawyer and client substantial latitude to limit the representation, the limitation must be reasonable under the circumstances. If, for example, a client's objective is limited to securing general information about the law the client needs in order to handle a common and typically uncomplicated legal problem, the lawyer and client may agree that the lawyer's services will be limited to a brief telephone consultation. Such a limitation, however, would not be reasonable if the time allotted was not sufficient to yield advice upon which the client could rely. Although an agreement for a limited representation does not exempt a lawyer from the duty to provide competent representation, the limitation is a factor to be considered when determining the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. See Rule 1.1.

[8] All agreements concerning a lawyer's representation of a client must accord with the Rules

of Professional Conduct and other law. See, *e.g.*, Rules 1.1, 1.8 and 5.6, and Supreme Court Rules 13(c)(6) and 137(e).

Criminal, Fraudulent and Prohibited Transactions

[9] Paragraph (d) prohibits a lawyer from knowingly counseling or assisting a client to commit a crime or fraud. This prohibition, however, does not preclude the lawyer from giving an honest opinion about the actual consequences that appear likely to result from a client's conduct. Nor does the fact that a client uses advice in a course of action that is criminal or fraudulent of itself make a lawyer a party to the course of action. There is a critical distinction between presenting an analysis of legal aspects of questionable conduct and recommending the means by which a crime or fraud might be committed with impunity.

[10] Paragraph (d)(3) was adopted to address the dilemma facing a lawyer in Illinois after the passage of the Illinois Compassionate Use of Medical Cannabis Pilot Program Act effective January 1, 2014. The Act expressly permits the cultivation, distribution, and use of marijuana for medical purposes under the conditions stated in the Act. Conduct permitted by the Act may be prohibited by the federal Controlled Substances Act, 21 U.S.C. §§801-904 and other law. The conflict between state and federal law makes it particularly important to allow a lawyer to provide legal advice and assistance to a client seeking to engage in conduct permitted by Illinois law. In providing such advice and assistance, a lawyer shall also advise the client about related federal law and policy. Paragraph (d)(3) is not restricted in its application to the marijuana law conflict. A lawyer should be especially careful about counseling or assisting a client in other contexts in conduct that may violate or conflict with federal, state, or local law.

[11] When the client's course of action has already begun and is continuing, the lawyer's responsibility is especially delicate. The lawyer is required to avoid assisting the client, for example, by drafting or delivering documents that the lawyer knows are fraudulent or by suggesting how the wrongdoing might be concealed. A lawyer may not continue assisting a client in conduct that the lawyer originally supposed was legally proper but then discovers is criminal or fraudulent. The lawyer must, therefore, withdraw from the representation of the client in the matter. See Rule 1.16(a). In some cases, withdrawal alone might be insufficient. It may be necessary for the lawyer to give notice of the fact of withdrawal and to disaffirm any opinion, document, affirmation or the like. See Rule 4.1. In such situations, the lawyer should also consider whether disclosure of information relating to the representation is appropriate. See Rule 1.6(b).

[12] Where the client is a fiduciary, the lawyer may be charged with special obligations in dealings with a beneficiary.

[13] Paragraph (d) applies whether or not the defrauded party is a party to the transaction. Hence, a lawyer must not participate in a transaction to effectuate criminal or fraudulent avoidance of tax liability. Paragraph (d) does not preclude undertaking a criminal defense incident to a general retainer for legal services to a lawful enterprise. The last clause of paragraph (d) recognizes that determining the validity or interpretation of a statute or regulation may require a course of action involving disobedience of the statute or regulation or of the interpretation placed upon it by governmental authorities.

[14] If a lawyer comes to know or reasonably should know that a client expects assistance not permitted by the Rules of Professional Conduct or other law or if the lawyer intends to act contrary to the client's instructions, the lawyer must consult with the client regarding the limitations on the lawyer's conduct. See Rule 1.4(a)(5).

[15] The prohibition stated in paragraph (e) has existed in Illinois ethics rules and in the prior Code since 1980. It is intended to curtail abuses that occasionally occur when a lawyer attempts to transfer complete or substantial responsibility for a matter to an unaffiliated lawyer without the client's awareness or consent. The Rule is designed to clarify the lawyer's obligation to complete the employment contemplated unless the client gives informed consent to substitution by an unaffiliated lawyer. The Rule is not intended to prohibit lawyers from hiring lawyers outside of their firm to perform certain services on the client's or the law firm's behalf. Nor is it intended to prevent lawyers from engaging lawyers outside of their firm to stand in for discrete events in situations such as personal emergencies, illness or schedule conflicts.

Adopted July 1, 2009, effective January 1, 2010; amended June 14, 2013, eff. July 1, 2013; amended Oct. 15, 2015, eff. Jan. 1, 2016.

RULE 1.3: DILIGENCE

A lawyer shall act with reasonable diligence and promptness in representing a client.

Adopted July 1, 2009, effective January 1, 2010.

Comment

[1] A lawyer should pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor. A lawyer must also act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf. A lawyer is not bound, however, to press for every advantage that might be realized for a client. For example, a lawyer may have authority to exercise professional discretion in determining the means by which a matter should be pursued. See Rule 1.2. The lawyer's duty to act with reasonable diligence does not require the use of offensive tactics or preclude the treating of all persons involved in the legal process with courtesy and respect.

[2] A lawyer's work load must be controlled so that each matter can be handled competently.

[3] Perhaps no professional shortcoming is more widely resented than procrastination. A client's interests often can be adversely affected by the passage of time or the change of conditions; in extreme instances, as when a lawyer overlooks a statute of limitations, the client's legal position may be destroyed. Even when the client's interests are not affected in substance, however, unreasonable delay can cause a client needless anxiety and undermine confidence in the lawyer's trustworthiness. A lawyer's duty to act with reasonable promptness, however, does not preclude the lawyer from agreeing to a reasonable request for a postponement that will not prejudice the lawyer's client.

[4] Unless the relationship is terminated as provided in Rule 1.16, a lawyer should carry through to conclusion all matters undertaken for a client. If a lawyer's employment is limited to a specific matter, the relationship terminates when the matter has been resolved. If a lawyer has served a client over a substantial period in a variety of matters, the client sometimes may assume that the lawyer will continue to serve on a continuing basis unless the lawyer gives notice of withdrawal. Doubt about whether a client-lawyer relationship still exists should be clarified by the lawyer, preferably in writing, so that the client will not mistakenly suppose the lawyer is looking after the client's affairs when the lawyer has ceased to do so. For example, if a lawyer has handled a judicial or administrative proceeding that produced a result adverse to the client and the lawyer and the client have not agreed that the lawyer will handle the matter on appeal, the lawyer must consult with the client about the possibility of appeal before relinquishing responsibility for the matter. See Rule 1.4(a)(2). Whether the lawyer is obligated to prosecute the appeal for the client depends on the scope of the representation the lawyer has agreed to provide to the client. See Rule 1.2.

[5] To prevent neglect of client matters in the event of a sole practitioner's death or disability, the duty of diligence may require that each sole practitioner prepare a plan, in conformity with applicable rules, that designates another competent lawyer to review client files, notify each client of the lawyer's death or disability, and determine whether there is a need for immediate protective action. See Illinois Supreme Court Rule 776, Appointment of Receiver in Certain Cases.

Adopted July 1, 2009, effective January 1, 2010.

RULE 1.4: COMMUNICATION

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

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

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

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

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

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

Adopted July 1, 2009, effective January 1, 2010.

Comment

[1] Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.

Communicating with Client

[2] If these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client's consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously indicated that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. See Rule 1.2(a).

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations–depending on both the importance of the action under consideration and the feasibility of consulting with the client–this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with

the request, or if a prompt response is not feasible, that the lawyer, or a member of the lawyer's staff, acknowledge receipt of the request and advise the client when a response may be expected. A lawyer should promptly respond to or acknowledge client communications.

Explaining Matters

[5] The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, when there is time to explain a proposal made in a negotiation, the lawyer should review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(e).

[6] Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. See Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to the appropriate officials of the organization. See Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

Withholding Information

[7] In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client. Rule 3.4(c) directs compliance with such rules or orders.

Adopted July 1, 2009, effective January 1, 2010; amended Oct. 15, 2015, eff. Jan. 1, 2016.

RULE 1.5: FEES

(a) A lawyer shall not make an agreement for, charge, or collect an unreasonable fee or an unreasonable amount for expenses. The factors to be considered in determining the reasonableness of a fee include the following:

(1) the time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly;

(2) the likelihood, if apparent to the client, that the acceptance of the particular employment will preclude other employment by the lawyer;

(3) the fee customarily charged in the locality for similar legal services;

(4) the amount involved and the results obtained;

(5) the time limitations imposed by the client or by the circumstances;

(6) the nature and length of the professional relationship with the client;

(7) the experience, reputation, and ability of the lawyer or lawyers performing the services; and

(8) whether the fee is fixed, contingent, or some type of retainer.

(b) The scope of the representation and the basis or rate of the fee and expenses for which the client will be responsible shall be communicated to the client, preferably in writing, before or within a reasonable time after commencing the representation, except when the lawyer will charge a regularly represented client on the same basis or rate. Any changes in the basis or rate of the fee or expenses shall also be communicated to the client.

(c) Nonrefundable fees and nonrefundable retainers are prohibited. Any agreement that purports to restrict a client's right to terminate the representation or that unreasonably restricts a client's right to obtain a refund of unearned or unreasonable fees is prohibited.

(d) Common Types of Fee Agreements

(1) Fixed Fees: A fixed fee, also described as a "flat" or "lump-sum" fee, is a sum of money paid by a client to the lawyer to provide a specific service for a fixed amount. The fixed amount constitutes complete payment for the performance of the described services and may be paid in whole or in part in advance of the lawyer providing those services. A fixed fee may not be deposited in the lawyer's client trust account.

(2) Contingent Fees: A fee may be contingent on the outcome of the matter for which the service is rendered, except in a matter in which a contingent fee is prohibited by paragraph (c) or other law. A contingent fee agreement shall be in a writing signed by the client and shall state the method by which the fee is to be determined, including the percentage or percentages that shall accrue to the lawyer in the event of settlement, trial or appeal; litigation and other expenses to be deducted from the recovery; and whether such expenses are to be deducted before or after the contingent fee is calculated. The agreement must clearly notify the client of any expenses for which the client will be liable whether or not the client is the prevailing party. Upon conclusion of a contingent fee matter, the lawyer shall provide the client with a written statement stating the outcome of the matter and, if there is a recovery, showing the remittance to the client and the method of its determination.

(3) Engagement Retainers: An engagement retainer, also described as a "general," "classic," or "true" retainer, is a fixed sum of money paid by a client to the lawyer to ensure a lawyer's availability during a specified period of time or for a specified matter. Funds received as an engagement retainer are earned when paid and immediately become property of the lawyer, regardless of whether the lawyer ever actually performs any services for the client. A lawyer is compensated separately for any legal services actually rendered by the lawyer. Funds received as an engagement retainer may not be deposited into a client trust account.

(4) Security Retainers: A security retainer, also referred to as a "security payment retainer," describes funds paid to the lawyer intended to secure payment of fees and expenses for future services and costs the lawyer is expected to perform or incur. Funds received as a security retainer remain the property of the client and, therefore, must be deposited in a client trust account and kept separate from the lawyer's own property until the lawyer applies the retainer to charges for services that are actually rendered. The term "security retainer" should be used in any written agreement describing the retainer.

(5) Special Purpose Retainers: A special purpose retainer, also referred to as an "advance payment retainer," describes funds paid to the lawyer intended by the client to be present payment to the lawyer in exchange for the commitment to provide legal services in the future and may be used only when necessary to accomplish some purpose for the client that cannot be accomplished by using a security retainer. Ownership of a special purpose retainer passes to the lawyer immediately upon payment and is generally the lawyer's property and, therefore, may not be deposited in the lawyer's client trust account. An agreement for a special purpose retainer shall be in a writing signed by the client that uses the term "special purpose retainer" to describe the retainer, and states the following:

(i) the special purpose for the special purpose retainer and an explanation as to why it is advantageous to the client;

(ii) that the retainer will not be held in a client trust account, that it will become the property of the lawyer upon payment, and that it will be deposited in the lawyer's general account;

(iii) the manner in which the retainer will be applied for services rendered and expenses incurred;

(iv) that any portion of the retainer that is not earned or required for expenses will be refunded to the client; and

(v) that the client has the option to employ a security retainer, provided, however, that if the lawyer is unwilling to represent the client without receiving a special purpose retainer, the agreement must so state and provide the lawyer's reasons for that condition.

(e) A lawyer shall not enter into an arrangement for, charge, or collect:

(1) any fee in a domestic relations matter, the payment or amount of which is contingent upon the securing of a divorce or upon the amount of alimony or support, or property settlement in lieu thereof; or

(2) a contingent fee for representing a defendant in a criminal case.

(f) A division of a fee between lawyers who are not in the same firm may be made only if:

(1) the division is in proportion to the services performed by each lawyer, or if the primary service performed by one lawyer is the referral of the client to another lawyer and each lawyer assumes joint financial responsibility for the representation;

(2) the client agrees to the arrangement, including the share each lawyer will receive, and the agreement is confirmed in writing; and

(3) the total fee is reasonable.

Adopted July 1, 2009, effective January 1, 2010; amended Mar. 1, 2023, eff. July 1, 2023.

Comment

Reasonableness of Fee and Expenses

[1] Paragraph (a) requires that lawyers charge fees that are reasonable under the circumstances. The factors specified in (1) through (8) are not exclusive. Nor will each factor be relevant in each instance. Paragraph (a) also requires that expenses for which the client will be charged must be reasonable. A lawyer may seek reimbursement for the cost of services performed in-house, such as copying, or for other expenses incurred in-house, such as telephone charges, either by charging a reasonable amount to which the client has agreed in advance or by charging an amount that reasonably reflects the cost incurred by the lawyer.

Basis or Rate of Fee

[2] When the lawyer has regularly represented a client, they ordinarily will have evolved an understanding concerning the basis or rate of the fee and the expenses for which the client will be responsible. In a new client-lawyer relationship, however, an understanding as to fees and expenses must be promptly established. Generally, it is desirable to furnish the client with at least a simple memorandum or copy of the lawyer's customary fee arrangements that states the general nature of the legal services to be provided, the basis, rate or total amount of the fee and whether and to what extent the client will be responsible for any costs, expenses or disbursements in the course of the representation. A written statement concerning the terms of the engagement reduces the possibility of misunderstanding.

[3] Fixed fees are generally not subject to the obligation to refund any portion to the client if the lawyer completes the agreed-upon services; however, fixed fees are subject, like any other fees, to the reasonableness standard of paragraph (a) of this Rule, and when circumstances so warrant, the attorney is obligated to return the portion that is not earned pursuant to Rule 1.16(d).

[4] Contingent fees, like any other fees, are subject to the reasonableness standard of paragraph (a) of this Rule. In determining whether a particular contingent fee is reasonable, or whether it is reasonable to charge any form of contingent fee, a lawyer must consider the factors that are relevant under the circumstances. Applicable law may impose limitations on contingent fees, such as a ceiling on the percentage allowable, or may require a lawyer to offer clients an alternative

basis for the fee. Applicable law also may apply to situations other than a contingent fee, for example, government regulations regarding fees in certain tax matters.

[5] In *Dowling v. Chicago Options Associates, Inc.,* 226 Ill. 2d 277 (2007), the Court distinguished different types of retainers. It recognized advance payment retainers (referred to in this Rule as special purpose retainers) and approved their use in limited circumstances where the lawyer and client agree that a retainer should become the property of the lawyer upon payment. Prior to *Dowling*, the Court recognized only two types of retainers. The first, a general retainer (also described as a "true," "engagement," or "classic" retainer) is paid by a client to the lawyer in order to ensure the lawyer's availability during a specific period of time or for a specific matter. This type of retainer is earned when paid and immediately becomes property of the lawyer, regardless of whether the lawyer ever actually performs any services for the client. The second, a "security" retainer, secures payment for future services and expenses, and must be deposited in a client trust account pursuant to Rule 1.15B(b). Funds in a security retainer remain the property of the client until applied for services rendered or expenses incurred. Any unapplied funds are refunded to the client. Any written retainer agreement should clearly define the kind of retainer being paid. If the parties agree that the client will pay a security retainer, that term should be used in any written agreement, which should also provide that the funds remain the property of the client until applied for services rendered or expenses incurred and that the funds will be deposited in a client trust account. If the parties' intent is not evident, an agreement for a retainer will be construed as providing for a security retainer.

[6] A special purpose retainer, identified in *Dowling* as an advance payment retainer, is a present payment to the lawyer in exchange for the commitment to provide legal services in the future. Ownership of this retainer passes to the lawyer immediately upon payment; and the retainer may not be deposited into a client trust account because a lawyer may not commingle property of a client with the lawyer's own property. However, any portion of a special purpose retainer that is not earned must be refunded to the client. A special purpose retainer should be used sparingly, only when necessary to accomplish a purpose for the client that cannot be accomplished by using a security retainer. A special purpose retainer agreement must be in a written agreement signed by the client that contains the elements listed in paragraph (d)(5). A special purpose retainer is distinguished from a fixed fee (also described as a "flat" or "lump-sum" fee), where the lawyer agrees to provide a specific service (*e.g.,* defense of a criminal charge, a real estate closing, or preparation of a will or trust) for a fixed amount. Unlike a special purpose retainer, a fixed fee is generally not subject to the obligation to refund any portion to the client, although a fixed fee is subject, like all fees, to the requirement of Rule 1.5(a) that a lawyer may not charge or collect an unreasonable fee.

[7] The type of retainer that is appropriate will depend on the circumstances of each case, and any written retainer agreement should clearly define the kind of retainer being paid. The guiding principle in the choice of the type of retainer is protection of the client's interests. In the vast majority of cases, this will dictate that funds paid to retain a lawyer will be considered a security retainer and placed in a client trust account, and if the parties' intent is not evident, an agreement for a retainer will be construed as providing for a security retainer. Any unapplied funds of a security retainer are refunded to the client under Rule 1.16(d).

Terms of Payment

[8] A lawyer may accept property in payment for services, such as an ownership interest in an enterprise, providing this does not involve acquisition of a proprietary interest in the cause of action or subject matter of the litigation contrary to Rule 1.8 (i). However, a fee paid in property instead of money may be subject to the requirements of Rule 1.8(a) because such fees often have the essential qualities of a business transaction with the client.

[8A] Rule 1.5 allows fee agreements that are not on an hourly rate, for example, fixed fee arrangements, so long as the fee charged or collected is reasonable for the services performed as allowed under Rule 1.5. Where appropriate, lawyers should consider alternative arrangements to deliver affordable representation. In structuring any fee agreement, lawyers should strive to make the cost of legal services transparent and predictable, with the goal of reducing misunderstandings and avoiding fee disputes with clients.

[9] An agreement may not be made whose terms might induce the lawyer improperly to curtail services for the client or perform them in a way contrary to the client's interest. For example, a lawyer should not enter into an agreement whereby services are to be provided only up to a stated amount when it is foreseeable that more extensive services probably will be required, unless the situation is adequately explained to the client. Otherwise, the client might have to bargain for further assistance in the midst of a proceeding or transaction. However, it is proper to define the extent of services in light of the client's ability to pay. A lawyer should not exploit a fee arrangement based primarily on hourly charges by using wasteful procedures.

Prohibited Contingent Fees

[10] Paragraph (e) prohibits a lawyer from charging a contingent fee in a domestic relations matter when payment is contingent upon the securing of a divorce or upon the amount of alimony or support or property settlement to be obtained. This provision does not preclude a contract for a contingent fee for legal representation in connection with the recovery of postjudgment balances due under support, alimony or other financial orders because such contracts do not implicate the same policy concerns.

Division of Fee

[11] A division of fee is a single billing to a client covering the fee of two or more lawyers who are not in the same firm. A division of fee facilitates association of more than one lawyer in a matter in which neither alone could serve the client as well, or referral of a matter where appropriate, and often is used when the fee is contingent and the division is between a referring lawyer and a trial specialist. Paragraph (e) permits the lawyers to divide a fee either on the basis of the proportion of services they render or, where the primary service performed by one lawyer is the referral of the client to another lawyer, if each lawyer assumes financial responsibility for

the representation as a whole. In addition, the client must agree to the arrangement, including the share that each lawyer is to receive, and the agreement must be confirmed in writing. Contingent fee agreements must be in a writing signed by the client and must otherwise comply with paragraph (d)(2) of this Rule. Joint financial responsibility for the representation entails financial responsibility for the representation as if the lawyers were associated in a general partnership. See *In re Storment*, 203 Ill. 2d 378 (2002). A lawyer should only refer a matter to a lawyer whom the referring lawyer reasonably believes is competent to handle the matter. See Rule 1.1.

[12] Paragraph (f) does not prohibit or regulate division of fees to be received in the future for work done when lawyers were previously associated in a law firm, or payments made pursuant to a separation or retirement agreement.

Disputes over Fees

[13] If a procedure has been established for resolution of fee disputes, such as an arbitration or mediation procedure established by law or rule, the lawyer must comply with the procedure when it is mandatory, and, even when it is voluntary, the lawyer should conscientiously consider submitting to it. Law may prescribe a procedure for determining a lawyer's fee, for example, in representation of an executor or administrator, a class or a person entitled to a reasonable fee as part of the measure of damages. The lawyer entitled to such a fee and a lawyer representing another party concerned with the fee should comply with the prescribed procedure.

Adopted July 1, 2009, effective January 1, 2010; amended Dec. 22, 2022; amended Mar. 1, 2023, eff. July 1, 2023.

RULE 1.8: CONFLICT OF INTEREST: CURRENT CLIENTS: SPECIFIC RULES

(a) A lawyer shall not enter into a business transaction with a client or knowingly acquire an ownership, possessory, security or other pecuniary interest adverse to a client unless:

(1) the transaction and terms on which the lawyer acquires the interest are fair and reasonable to the client and are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;

(2) the client is informed in writing that the client may seek the advice of independent legal counsel on the transaction, and is given a reasonable opportunity to do so; and

(3) the client gives informed consent, in a writing signed by the client, to the essential terms of the transaction and the lawyer's role in the transaction, including whether the lawyer is representing the client in the transaction.

(b) A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these Rules.

(c) A lawyer shall not solicit any substantial gift from a client, including a testamentary gift, or prepare on behalf of a client an instrument giving the lawyer or a person related to the lawyer any substantial gift unless the lawyer or other recipient of the gift is related to the client. For purposes of this paragraph, related persons include a spouse, child, grandchild, parent, grandparent or other relative or individual with whom the lawyer or the client maintains a close, familial relationship.

(d) Prior to the conclusion of representation of a client, a lawyer shall not make or negotiate an agreement giving the lawyer literary or media rights to a portrayal or account based in substantial part on information relating to the representation.

(e) A lawyer shall not provide financial assistance to a client in connection with pending or contemplated litigation, except that:

(1) a lawyer may advance court costs and expenses of litigation, the repayment of which may be contingent on the outcome of the matter; and

(2) a lawyer representing an indigent client may pay court costs and expenses of litigation on behalf of the client.

(f) A lawyer shall not accept compensation for representing a client from one other than the client unless:

(1) the client gives informed consent;

(2) there is no interference with the lawyer's independence of professional judgment or with the client-lawyer relationship; and

(3) information relating to representation of a client is protected as required by Rule 1.6.

(g) A lawyer who represents two or more clients shall not participate in making an aggregate settlement of the claims of or against the clients, or in a criminal case an aggregated agreement as to guilty or *nolo contendere* pleas, unless each client gives informed consent, in a writing signed by the client. The lawyer's disclosure shall include the existence and nature of all the claims or pleas involved and of the participation of each person in the settlement.

(h) A lawyer shall not:

(1) make an agreement prospectively limiting the lawyer's liability to a client for malpractice unless the client is independently represented in making the agreement; or

(2) settle a claim or potential claim for such liability with an unrepresented client or former client unless that person is advised in writing of the desirability of seeking and is given a reasonable opportunity to seek the advice of independent legal counsel in connection therewith.

(i) A lawyer shall not acquire a proprietary interest in the cause of action or subject matter of litigation the lawyer is conducting for a client, except that the lawyer may:

(1) acquire a lien authorized by law to secure the lawyer's fee or expenses;

and

(2) contract with a client for a reasonable contingent fee in a civil case.

(j) A lawyer shall not have sexual relations with a client unless a consensual sexual relationship existed between them when the client-lawyer relationship commenced.

(k) While lawyers are associated in a firm, a prohibition in the foregoing paragraphs (a) through (i) that applies to any one of them shall apply to all of them.

Adopted July 1, 2009, effective January 1, 2010.

Comment

Business Transactions Between Client and Lawyer

[1] A lawyer's legal skill and training, together with the relationship of trust and confidence between lawyer and client, create the possibility of overreaching when the lawyer participates in a business, property or financial transaction with a client, for example, a loan or sales transaction or a lawyer investment on behalf of a client. The requirements of paragraph (a) must be met even when the transaction is not closely related to the subject matter of the representation, as when a lawyer drafting a will for a client learns that the client needs money for unrelated expenses and offers to make a loan to the client. The Rule applies to lawyers engaged in the sale of goods or services related to the practice of law, for example, the sale of title insurance or investment services to existing clients of the lawyer's legal practice. It also applies to lawyers purchasing property from estates they represent. It does not apply to ordinary fee arrangements between client and lawyer, which are governed by Rule 1.5, although its requirements must be met when the lawyer accepts an interest in the client's business or other nonmonetary property as payment of all or part of a fee. In addition, the Rule does not apply to standard commercial transactions between the lawyer and the client for products or services that the client generally markets to others, for example, banking or brokerage services, medical services, products manufactured or distributed by the client, and utilities' services. In such transactions, the lawyer has no advantage in dealing with the client, and the restrictions in paragraph (a) are unnecessary and impracticable.

[2] Paragraph (a)(1) requires that the transaction itself be fair to the client and that its essential terms be communicated to the client, in writing, in a manner that can be reasonably understood.

Paragraph (a)(2) requires that the lawyer inform the client in writing that the client may seek the advice of independent legal counsel and provide a reasonable opportunity for the client to do so. Paragraph (a)(3) requires that the lawyer obtain the client's informed consent, in a writing signed by the client, both to the essential terms of the transaction and to the lawyer's role. When necessary, the lawyer should discuss both the material risks of the proposed transaction, including any risk presented by the lawyer's involvement, and the existence of reasonably available alternatives and should explain why the advice of independent legal counsel is desirable. See Rule 1.0(e) (definition of informed consent). The common law regarding business transactions between lawyer and client may impose additional requirements, such as encouraging the client to seek independent legal counsel, in lawyer liability and other nondisciplinary contexts.

[3] The risk to a client is greatest when the client expects the lawyer to represent the client in the transaction itself or when the lawyer's financial interest otherwise poses a significant risk that the lawyer's representation of the client will be materially limited by the lawyer's financial interest in the transaction. Here the lawyer's role requires that the lawyer must comply, not only with the requirements of paragraph (a), but also with the requirements of Rule 1.7. Under that Rule, the lawyer must disclose the risks associated with the lawyer's dual role as both legal adviser and participant in the transaction, such as the risk that the lawyer will structure the transaction or give legal advice in a way that favors the lawyer's interests at the expense of the client. Moreover, the lawyer must obtain the client's informed consent. In some cases, the lawyer's interest may be such that Rule 1.7 will preclude the lawyer from seeking the client's consent to the transaction.

[4] If the client is independently represented in the transaction, paragraph (a)(2) of this Rule is inapplicable, and the paragraph (a)(1) requirement for full disclosure is satisfied either by a written disclosure by the lawyer involved in the transaction or by the client's independent counsel. The fact that the client was independently represented in the transaction is relevant in determining whether the agreement was fair and reasonable to the client as paragraph (a)(1) further requires.

Use of Information Related to Representation

[5] Use of information relating to the representation to the disadvantage of the client violates the lawyer's duty of loyalty. Paragraph (b) applies when the information is used to benefit either the lawyer or a third person, such as another client or business associate of the lawyer. For example, if a lawyer learns that a client intends to purchase and develop several parcels of land, the lawyer may not use that information to purchase one of the parcels in competition with the client or to recommend that another client make such a purchase. The Rule does not prohibit uses that do not disadvantage the client. For example, a lawyer who learns a government agency's interpretation of trade legislation during the representation of one client may properly use that information to benefit other clients. Paragraph (b) prohibits disadvantageous use of client information unless the client gives informed consent, except as permitted or required by these Rules. See Rules 1.2(d), 1.6, 1.9(c), 3.3, 4.1(b), 8.1 and 8.3.

Gifts to Lawyers

[6] A lawyer may accept a gift from a client, if the transaction meets general standards of fairness. For example, a simple gift such as a present given at a holiday or as a token of appreciation is permitted. If a client offers the lawyer a more substantial gift, paragraph (c) does not prohibit the lawyer from accepting it, although such a gift may be voidable by the client under the doctrine of undue influence, which treats client gifts as presumptively fraudulent. In any event, due to concerns about overreaching and imposition on clients, a lawyer may not suggest that a substantial gift be made to the lawyer or for the lawyer's benefit, except where the lawyer is related to the client as set forth in paragraph (c).

[7] If effectuation of a substantial gift requires preparing a legal instrument such as a will or conveyance the client should have the detached advice that another lawyer can provide. The sole exception to this Rule is where the client is a relative of the donee.

[8] This Rule does not prohibit a lawyer from seeking to have the lawyer or a partner or associate of the lawyer named as executor of the client's estate or to another potentially lucrative fiduciary position. Nevertheless, such appointments will be subject to the general conflict of interest provision in Rule 1.7 when there is a significant risk that the lawyer's interest in obtaining the appointment will materially limit the lawyer's independent professional judgment in advising the client concerning the choice of an executor or other fiduciary. In obtaining the client's informed consent to the conflict, the lawyer should advise the client concerning the nature and extent of the lawyer's financial interest in the appointment, as well as the availability of alternative candidates for the position.

Literary Rights

[9] An agreement by which a lawyer acquires literary or media rights concerning the conduct of the representation creates a conflict between the interests of the client and the personal interests of the lawyer. Measures suitable in the representation of the client may detract from the publication value of an account of the representation. Paragraph (d) does not prohibit a lawyer representing a client in a transaction concerning literary property from agreeing that the lawyer's fee shall consist of a share in ownership in the property, if the arrangement conforms to Rule 1.5 and paragraphs (a) and (i).

Financial Assistance

[10] Lawyers may not subsidize lawsuits or administrative proceedings brought on behalf of their clients, including making or guaranteeing loans to their clients for living expenses, because to do so would encourage clients to pursue lawsuits that might not otherwise be brought and because such assistance gives lawyers too great a financial stake in the litigation. These dangers do not warrant a prohibition on a lawyer lending a client court costs and litigation expenses, including the expenses of medical examination and the costs of obtaining and presenting evidence, because these advances are virtually indistinguishable from contingent fees and help ensure access to the courts. Similarly, an exception allowing lawyers representing indigent clients to pay court costs and litigation expenses regardless of whether these funds will be repaid is warranted.

Person Paying for a Lawyer's Services

[11] Lawyers are frequently asked to represent a client under circumstances in which a third person will compensate the lawyer, in whole or in part. The third person might be a relative or friend, an indemnitor (such as a liability insurance company) or a co-client (such as a corporation sued along with one or more of its employees). Because third-party payers frequently have interests that differ from those of the client, including interests in minimizing the amount spent on the representation and in learning how the representation is progressing, lawyers are prohibited from accepting or continuing such representations unless the lawyer determines that there will be no interference with the lawyer's independent professional judgment and there is informed consent from the client. See also Rule 5.4(c) (prohibiting interference with a lawyer's professional judgment by one who recommends, employs or pays the lawyer to render legal services for another).

[12] Sometimes, it will be sufficient for the lawyer to obtain the client's informed consent regarding the fact of the payment and the identity of the third-party payer. If, however, the fee arrangement creates a conflict of interest for the lawyer, then the lawyer must comply with Rule. 1.7. The lawyer must also conform to the requirements of Rule 1.6 concerning confidentiality. Under Rule 1.7(a), a conflict of interest exists if there is significant risk that the lawyer's representation of the client will be materially limited by the lawyer's own interest in the fee arrangement or by the lawyer's responsibilities to the third-party payer (for example, when the third-party payer is a co-client). Under Rule 1.7(b), the lawyer may accept or continue the representation with the informed consent of each affected client, unless the conflict is nonconsentable under that paragraph.

Aggregate Settlements

[13] Differences in willingness to make or accept an offer of settlement are among the risks of common representation of multiple clients by a single lawyer. Under Rule 1.7, this is one of the risks that should be discussed before undertaking the representation, as part of the process of obtaining the clients' informed consent. In addition, Rule 1.2(a) protects each client's right to have the final say in deciding whether to accept or reject an offer of settlement and in deciding whether to enter a guilty or *nolo contendere* plea in a criminal case. The rule stated in this paragraph is a corollary of both these Rules and provides that, before any settlement offer or plea bargain is made or accepted on behalf of multiple clients, the lawyer must inform each of them about all the material terms of the settlement, including what the other clients will receive or pay if the settlement or plea offer is accepted. See also Rule 1.0(e) (definition of informed consent). Lawyers representing a class of plaintiffs or defendants, or those proceeding derivatively, may not have a full client-lawyer relationship with each member of the class; nevertheless, such lawyers must comply with applicable rules regulating notification of class members and other procedural requirements designed to ensure adequate protection of the entire class.

Limiting Liability and Settling Malpractice Claims

[14] Agreements prospectively limiting a lawyer's liability for malpractice are prohibited unless the client is independently represented in making the agreement because they are likely to undermine competent and diligent representation. Also, many clients are unable to evaluate the desirability of making such an agreement before a dispute has arisen, particularly if they are then represented by the lawyer seeking the agreement. This paragraph does not, however, prohibit a lawyer from entering into an agreement with the client to arbitrate legal malpractice claims, provided such agreements are enforceable and the client is fully informed of the scope and effect of the agreement. Nor does this paragraph limit the ability of lawyers to practice in the form of a limited-liability entity, where permitted by law, provided that each lawyer remains personally liable to the client for his or her own conduct and the firm complies with any conditions required by law, such as provisions requiring client notification or maintenance of adequate liability insurance. Nor does it prohibit an agreement in accordance with Rule 1.2 that defines the scope of the representation, although a definition of scope that makes the obligations of representation illusory will amount to an attempt to limit liability.

[15] Agreements settling a claim or a potential claim for malpractice are not prohibited by this Rule. Nevertheless, in view of the danger that a lawyer will take unfair advantage of an unrepresented client or former client, the lawyer must first advise such a person in writing of the appropriateness of independent representation in connection with such a settlement. In addition, the lawyer must give the client or former client a reasonable opportunity to find and consult independent counsel.

Acquiring Proprietary Interest in Litigation

[16] Paragraph (i) states the traditional general rule that lawyers are prohibited from acquiring a proprietary interest in litigation. Like paragraph (e), the general rule has its basis in common law champerty and maintenance and is designed to avoid giving the lawyer too great an interest in the representation. In addition, when the lawyer acquires an ownership interest in the subject of the representation, it will be more difficult for a client to discharge the lawyer if the client so desires. The Rule is subject to specific exceptions developed in decisional law and continued in these Rules. The exception for certain advances of the costs of litigation is set forth in paragraph (e). In addition, paragraph (i) sets forth exceptions for liens authorized by law to secure the lawyer's fees or expenses and contracts for reasonable contingent fees. The law of each jurisdiction determines which liens are authorized by law. These may include liens granted by statute, liens originating in common law and liens acquired by contract with the client. When a lawyer acquires by contract a security interest in property other than that recovered through the lawyer's efforts in the litigation, such an acquisition is a business or financial transaction with a client and is governed by the requirements of paragraph (a). Contracts for contingent fees in civil cases are governed by Rule 1.5.

Client-Lawyer Sexual Relationships

[17] The relationship between lawyer and client is a fiduciary one in which the lawyer occupies the highest position of trust and confidence. The relationship is almost always unequal; thus, a sexual relationship between lawyer and client can involve unfair exploitation of the lawyer's fiduciary role, in violation of the lawyer's basic ethical obligation not to use the trust of the client to the client's disadvantage. In addition, such a relationship presents a significant danger that, because of the lawyer's emotional involvement, the lawyer will be unable to represent the client without impairment of the exercise of independent professional judgment. Moreover, a blurred line between the professional and personal relationships may make it difficult to predict to what extent client confidences will be protected by the attorney-client evidentiary privilege, since client confidences are protected by privilege only when they are imparted in the context of the client-lawyer relationship. Because of the significant danger of harm to client interests and because the client's own emotional involvement renders it unlikely that the client could give adequate informed consent, this Rule prohibits the lawyer from having sexual relations with a client regardless of whether the relationship is consensual and regardless of the absence of prejudice to the client.

[18] Sexual relationships that predate the client-lawyer relationship are not prohibited. Issues relating to the exploitation of the fiduciary relationship and client dependency are diminished when the sexual relationship existed prior to the commencement of the client-lawyer relationship. However, before proceeding with the representation in these circumstances, the lawyer should consider whether the lawyer's ability to represent the client will be materially limited by the relationship. See Rule 1.7(a)(2).

[19] When the client is an organization, paragraph (j) of this Rule prohibits a lawyer for the organization (whether inside counsel or outside counsel) from having a sexual relationship with a constituent of the organization who supervises, directs or regularly consults with that lawyer concerning the organization's legal matters.

Imputation of Prohibitions

[20] Under paragraph (k), a prohibition on conduct by an individual lawyer in paragraphs (a) through (i) also applies to all lawyers associated in a firm with the personally prohibited lawyer. For example, one lawyer in a firm may not enter into a business transaction with a client of another member of the firm without complying with paragraph (a), even if the first lawyer is not personally involved in the representation of the client. The prohibition set forth in paragraph (j) is personal and is not applied to associated lawyers.

Adopted July 1, 2009, effective January 1, 2010.

RULE 8.4: MISCONDUCT

It is professional misconduct for a lawyer to:

(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another.

(b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness, or fitness as a lawyer in other respects.

(c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.

(d) engage in conduct that is prejudicial to the administration of justice.

(e) state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law.

(f) knowingly assist a judge or judicial officer in conduct that is a violation of applicable rules of judicial conduct or other law. Nor shall a lawyer give or lend anything of value to a judge, official, or employee of a tribunal, except those gifts or loans that a judge or a member of the judge's family may receive under Canon 3, Rule 3.13, of the Illinois Code of Judicial Conduct of 2023. Permissible campaign contributions to a judge or candidate for judicial office may be made only by check, draft, or other instrument payable to or to the order of an entity that the lawyer reasonably believes to be a political committee supporting such judge or candidate. Provision of volunteer services by a lawyer to a political committee shall not be deemed to violate this paragraph.

(g) present, participate in presenting, or threaten to present criminal or professional disciplinary charges to obtain an advantage in a civil matter.

(h) enter into an agreement with a client or former client limiting or purporting to limit the right of the client or former client to file or pursue any complaint before the Illinois Attorney Registration and Disciplinary Commission.

(i) avoid in bad faith the repayment of an education loan guaranteed by the Illinois Student Assistance Commission or other governmental entity. The lawful discharge of an education loan in a bankruptcy proceeding shall not constitute bad faith under this paragraph, but the discharge shall not preclude a review of the lawyer's conduct to determine if it constitutes bad faith.

(j) engage in conduct in the practice of law that the lawyer knows or reasonably should know is harassment or discrimination on the basis of race, color, ancestry, sex, religion, national origin, ethnicity, disability, age, sexual orientation, gender identity, gender expression, marital status, military or veteran status, pregnancy, or socioeconomic status. This paragraph does not limit the ability of a lawyer to accept, decline, or, in accordance with Rule 1.16, withdraw from a representation. This paragraph does not preclude or limit the giving of advice, assistance, or advocacy consistent with these Rules.

(k) if the lawyer holds public office:

(1) use that office to obtain, or attempt to obtain, a special advantage in a legislative matter for a client under circumstances where the lawyer knows or reasonably should know that such action is not in the public interest;

(2) use that office to influence, or attempt to influence, a tribunal to act in favor of a client;

or

(3) represent any client, including a municipal corporation or other public body, in the promotion or defeat of legislative or other proposals pending before the public body of which such lawyer is a member or by which such lawyer is employed.

Adopted July 1, 2009, effective January 1, 2010; amended May 25, 2022, eff. immediately; amended Dec. 30, 2022, eff. Jan. 1, 2023; amended May 30, 2024, eff. July 1, 2024.

Comment

[1] Lawyers are subject to discipline when they violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so or do so through the acts of another, as when they request or instruct an agent to do so on the lawyer's behalf. Paragraph (a), however, does not prohibit a lawyer from advising a client concerning action the client is legally entitled to take.

[2] Many kinds of illegal conduct reflect adversely on fitness to practice law, such as offenses involving fraud and the offense of willful failure to file an income tax return. However, some kinds of offenses carry no such implication. Traditionally, the distinction was drawn in terms of offenses involving "moral turpitude." That concept can be construed to include offenses concerning some matters of personal morality, such as adultery and comparable offenses, that have no specific connection to fitness for the practice of law. Although a lawyer is personally answerable to the entire criminal law, a lawyer should be professionally answerable only for offenses that indicate lack of those characteristics relevant to law practice. Offenses involving violence, dishonesty, breach of trust, or serious interference with the administration of justice are in that category. A pattern of repeated offenses, even ones of minor significance when considered separately, can indicate indifference to legal obligation.

[3] Discrimination and harassment by lawyers in the practice of law in violation of paragraph (j) undermines confidence in the legal profession and the legal system. Conduct in the practice of law includes representing clients; interacting with witnesses, coworkers, court personnel, lawyers, and others when representing clients; operating or managing a law firm or law practice; and participating in law-related professional activities or events, including law firm or bar association educational or social events. Conduct protected by the Constitutions of the United States or the State of Illinois, including a lawyer's expression of views on matters of public concern in the context of teaching, public speaking, or other forms of public advocacy, does not violate this paragraph.

[3A] The Rules of Professional Conduct are rules of reason, and whether conduct violates paragraph (j) must be judged in context and from an objectively reasonable perspective. See Scope, paragraph [14]. Discrimination means harmful verbal or physical conduct directed at another person or group that manifests bias or prejudice on the basis of any characteristics identified in paragraph (j). Harassment includes conduct directed at another person or group that is invasive, pressuring, or intimidating in relation to any characteristic identified in paragraph (j). It includes

sexual harassment and derogatory or demeaning verbal or physical conduct. Sexual harassment includes unwelcome sexual advances, requests for sexual favors, and other unwelcome verbal or physical conduct of a sexual nature. The substantive law of antidiscrimination and antiharassment statutes and caselaw may guide the application of paragraph (j) and the evaluation of whether specific conduct constitutes discrimination or harassment. In addition, any judicial or administrative tribunal findings involving the same conduct may be considered in assessing whether a lawyer has violated paragraph (j). A trial judge's finding that preemptory challenges were exercised on a discriminatory basis does not alone establish a violation of paragraph (j).

[3B] Lawyers may engage in conduct undertaken to promote diversity and inclusion without violating paragraph (j) by, for example, implementing initiatives to encourage recruiting, hiring, retaining, and advancing diverse employees or sponsoring diverse law student organizations. A lawyer does not violate paragraph (j) by limiting the scope or subject matter of the lawyer's practice or by limiting the lawyer's practice to members of underserved populations in accordance with these Rules and other law. A lawyer may charge and collect reasonable fees and expenses for a representation. See Rule 1.5(a). Lawyers should be mindful of their obligation under Rule 6.2 not to avoid appointments from a tribunal except for good cause. A lawyer's representation of a client does not constitute an endorsement by the lawyer of the client's views or activities. See Rule 1.2(b).

[4] A lawyer may refuse to comply with an obligation imposed by law upon a good-faith belief that no valid obligation exists. The provisions of Rule 1.2(d) concerning a good-faith challenge to the validity, scope, meaning or application of the law apply to challenges of legal regulation of the practice of law.

[5] Lawyers holding public office assume legal responsibilities going beyond those of other citizens. A lawyer's abuse of public office can suggest an inability to fulfill the professional role of lawyers. The same is true of abuse of positions of private trust such as trustee, executor, administrator, guardian, agent and officer, director or manager of a corporation or other organization.

Adopted July 1, 2009, effective January 1, 2010; amended May 30, 2024, eff. July 1, 2024.

Law Bulletin
SEMINARS

Knowledge for Success