

WSR 24-01-046
RULES OF COURT
STATE SUPREME COURT
[December 7, 2023]

IN THE MATTER OF THE ) ORDER
SUGGESTED AMENDMENTS TO ) NO. 25700-A-1554
APR 11—MANDATORY )
CONTINUING LEGAL EDUCATION )
(MCLE) )

The Mandatory Continuing Legal Education Board, having recommended the suggested amendments to APR 11—Mandatory Continuing Legal Education (MCLE), and the Court having approved the suggested amendments for publication;

Now, therefore, it is hereby

ORDERED:

(a) That pursuant to the provisions of GR 9(g), the suggested amendments as shown below are to be published for comment in the Washington Reports, Washington Register, Washington State Bar Association and Administrative Office of the Court's websites in January 2024.

(b) The purpose statement as required by GR 9(e) is published solely for the information of the Bench, Bar and other interested parties.

(c) Comments are to be submitted to the Clerk of the Supreme Court by either U.S. Mail or Internet E-Mail by no later than April 30, 2024. Comments may be sent to the following addresses: P.O. Box 40929, Olympia, Washington 98504-0929, or supreme@courts.wa.gov. Comments submitted by e-mail message must be limited to 1500 words.

DATED at Olympia, Washington this 7th day of December, 2023.

For the Court

Gonzalez, C.J.

CHIEF JUSTICE

GR 9 COVER SHEET

Suggested Amendments

ADMISSION AND PRACTICE RULE (APR) 11

Mandatory Continuing Legal Education

Submitted by the Mandatory Continuing Legal Education Board

A. Name of Proponent:

Mandatory Continuing Legal Education (MCLE) Board
Staff Liaison/Contact:
Bobby Henry, Associate Director for Regulatory Services
Washington State Bar Association (WSBA)
1325 Fourth Avenue, Suite 600
Seattle, WA 98101-2539
roberth@wsba.org
206-727-8227

B. Spokesperson:

Efrem Krisher, Chair
MCLE Board
c/o Washington State Bar Association (WSBA)
1325 Fourth Avenue, Suite 600
Seattle, WA 98101-2539

**C. Purpose:**

The Mandatory Continuing Legal Education (MCLE) Board is suggesting amendments to rule 11 of the Admission and Practice Rules (APR). The purposes of the suggested amendments to APR 11 are to:

- require licensed legal professionals to earn one credit per MCLE reporting period (every three years) in the subject of mental health;
- require licensed legal professionals to earn one credit per MCLE reporting period (every three years) in the subject of technology security;
- create a separate category for the already required subject of "equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law" (hereinafter referred to as "equity");
- allow for additional credits earned beyond the required amount for any given reporting period in the subjects of mental health, technology security, and "equity" to carry over as "Other" credits.

The suggested amendments do NOT increase the total number of credits required for a reporting period. Nor do they dilute the ethics and professional responsibility ("ethics") or law and legal procedure requirements.

The suggested amendments reduce the ethics requirement to five credits, because the one credit requirement for "equity" will become its own category as opposed to a subcategory of ethics as currently provided for in APR 11. Although "equity" will be a separate category for credit count and compliance, the definition of "equity" remains unchanged. Creating a separate "equity" category will make it easier for licensed legal professionals and WSBA staff both to understand that there is a one credit "equity" requirement each reporting period and to track compliance with the "equity" requirement. Therefore, although the suggested amendments will technically reduce the ethics requirement to five credits, there remain essentially six ethics credits required because "equity" will still be a required credit category.

The MCLE Board puts forth these suggested amendments to ensure each lawyer, limited license legal technician (LLLT), and limited practice officer (LPO) focuses on mental health and technology security topics (in addition to "equity" topics) at least once every three years. These are serious topics that can greatly impact a licensed legal professional's competency and ability to practice law and, if ignored, could result in serious consequences to the licensed legal professional, the client, the administration of justice, and the integrity of the legal profession. The proposed requirements, therefore, are primarily directed toward the protection of clients and the public, improving the competency of licensed legal professionals, and, ultimately, improving and preserving the integrity of the legal community as a whole.

**I. Background**

One of the duties of the MCLE Board is to review and suggest amendments to APR 11 as necessary to fulfill the purpose of MCLE and for the efficient administration of these rules. APR 11 (d)(2)(i). Accordingly, in the Autumn of 2022, the MCLE Board appointed a committee to study and make recommendations regarding any subject areas that should be required learning for licensed legal professionals in Washington state. Following months of meetings, discussion, and research,

the committee recommended two subject areas—mental health ethics and technology security ethics. Notably, the committee initially recommended the subject areas be focused on ethical considerations related to the two subjects.

In the Spring of 2023, the MCLE Board sought public comment on its proposal. Nearly 1,000 WSBA members responded to the survey with approximately 670 comments. Approximately 2/3 of members responding to the survey were opposed to the amendments and 1/3 were in support. Amongst the many reasons given for opposing the amendments were three in particular that the MCLE Board addressed:

(1) it would be too difficult to find presenters qualified to talk about both the proposed subject matters and the related ethical considerations which would likely result in a very limited number of qualifying topics and course offerings;

(2) it would be difficult for licensed legal professionals to find ethics CLEs specifically on the two proposed subjects noting that ethics credits are already the most difficult to complete; and

(3) it would be complicated and difficult for licensed legal professionals to track compliance with several subcategories of ethics in addition to the other requirements in APR 11.

In light of these comments, at its meeting on June 16, 2023, the MCLE Board decided to untie those proposed subjects from professional ethics. In addition, the MCLE Board decided to create separate credit categories for the subjects to increase the breadth of discussion of those important topics and availability of course offerings while making it easier for licensed legal professionals to track their compliance. The MCLE Board, at a special meeting on June 14, 2023, approved the final language for the suggested amendments.

The MCLE Board then sought support from the WSBA Board of Governors which added the topic to its agenda for the WSBA Board of Governors meeting on August 11, 2023. Following a presentation by the MCLE Board and a discussion among governors, the WSBA Board of Governors voted on each of the two new subjects individually. In a vote of 6-5, the Board of Governors voted to support the stand-alone mental health requirement. However, in a vote of 4-6-1, the Board of Governors voted against supporting the stand-alone technology security requirement. The MCLE Board met on August 13, 2023, and decided to submit the suggested amendments to the Court without further changes.

## **II. Considerations in Support of the Technology Security Credit Requirement**

The MCLE Board presents the following as important factors in support of the suggested amendment for a new requirement for all licensed legal professionals to complete one credit each reporting period in technology security for the protection of electronic data and communication.

Legal professionals have an ethical and common law duty to take competent and reasonable measures to safeguard client information. They also have contractual and regulatory duties to protect confidential information. Rules 1.1, 1.3, and 1.4 of the Rules of Professional Conduct (RPC) address lawyers' core ethical duties of competence, diligence, and communication with their clients. Possessing technological knowledge to safeguard client information as a fundamental requirement is explained in comment eight to RPC 1.1 which states that in order for legal professionals to, "[m]aintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practices, including the benefits and **risks associated with relevant**

**technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." (Emphasis added.) With the advent of the global pandemic and an increasing number of legal professionals practicing "virtually," it is imperative that lawyers, and all legal professionals, stay cognizant of their ethical responsibilities.<sup>1</sup>

<sup>1</sup> ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 498 (2021) (issuing cautionary ethics guidance on virtual law practices), [https://www.americanbar.org/content/dam/aba/administrative/professional\\_responsibility/aba-formal-opinion-498.pdf](https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf)

**A Technology Security Credit Should be Mandatory Because Lack of Knowledge Can Result in Significant Consequences to Legal Professionals and Their Clients.**

With each passing year, cybercrimes become more rampant and cyber insecurity results in increasingly costly and catastrophic events. "The rate of global weekly cyberattacks rose by 7% in the first financial quarter of 2023 compared with the same period in 2022" with an average 1,248 attacks per week and one of out of every 40 of those targeting a law firm or insurance provider.<sup>2</sup> "More than a quarter of law firms in a 2022 American Bar Association survey said they had experienced a data breach, up 2% from the previous year."<sup>3</sup> Electronic security breaches today are now so prevalent, that the question is not if, but when, it will happen. The Federal Bureau of Investigation Internet Crime Complaint Center ("IC3") received 847,376 complaints relating to extortion, identity theft, and personal data breaches representing potential losses exceeding \$6.9 billion in 2021.<sup>4</sup> The IC3 receives an average of over 2,300 cybercrime complaints each day, with over 6.5 million complaints since the IC3's inception in 2000.<sup>5</sup> Washington state is ranked as the 9th highest state where internet crime victims reside.<sup>6</sup> Washington state victims reported losing \$157,454,331 in 2021 as a result of internet crimes.<sup>7</sup>

<sup>2</sup> Bloomberg Law, *Law Firm Cyberattacks Grow, Putting Operations in Legal Peril*, (2023), <https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril?source=newsletter&item=body-link&region=text-section>

<sup>3</sup> *Id.*

<sup>4</sup> Internet Crime Complaint Center, *2021 Internet Crime Report*, at 3 (2022), [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

<sup>5</sup> *Id.* at 18 n.16.

<sup>6</sup> *Id.* at 26.

<sup>7</sup> *Id.* at 27.

In 2021, the IC3 received 19,954 compromised business email complaints resulting in adjusted losses at nearly \$2.4 billion.<sup>8</sup> The cybercrimes involved sophisticated scams targeting businesses, including law firms, and individuals, such as law firm clients, performing monetary transfers. Criminals will hack emails and spoof business representatives' credentials to initiate fraudulent wire transfers.

<sup>8</sup> *Id.* at 3.

Law firms are being specifically targeted. Such targeted attacks have become so frequent that the State Bar of Texas maintains an updated list on their blog notifying attorneys of recent scams.<sup>9</sup>

<sup>9</sup> See Joanna Herzik, *Scams Continue to Target Texas Attorneys*, State Bar of Texas Blog (June 28, 2022), <https://blog.texasbar.com/2022/12/articles/law-firms-and-legal-departments/scams-continue-to-target-texas-attorneys/>.

Additionally, back in October of 2018 the American Bar Association warned,

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting tar-

gets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.<sup>10</sup>

<sup>10</sup> ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018) (discussing lawyers' obligations after an electronic data breach or cyberattack), [https://www.americanbar.org/content/dam/aba/images/news/formal\\_op\\_483.pdf](https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf).

The IC3 report details a complaint filed by a victim law office in June 2021 regarding a wire transfer of more than \$198,000 to a fraudulent U.S. domestic account.<sup>11</sup> However, other law firms have reported bigger breaches with higher stakes at risk. In May of 2020, law firm hackers behind a ransomware attack on a New York celebrity law firm threatened to publish compromising information on former U.S. President Donald Trump if they did not receive their \$42 million demand.<sup>12</sup> As proof, the hackers gained access to sensitive client information and published legal contracts related to the law firm's client, Madonna.<sup>13</sup> The hackers also released 2.4 GB of legal data related to client Lady Gaga.<sup>14</sup>

<sup>11</sup> Internet Crime Complaint Center, *supra* note 2 at 11.

<sup>12</sup> Alex Scroxton, *Law Firm Hackers Threaten to Release Dirt on Trump*, ComputerWeekly.com (May 15, 2020, 10:19 AM), <https://www.computerweekly.com/news/252483193/Law-firm-hackers-threaten-to-release-dirt-on-Trump>.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

One in four law firms that participated in the ABA's 2021 Legal Technology Survey reported their firms experienced a data breach at some time.<sup>15</sup> A breach includes incidents like a lost/stolen computer or smartphone, hacker, break-in, or website exploit.<sup>16</sup> The actual number of victim firms could be higher as the firm may have experienced a security breach and never detected it.<sup>17</sup> The survey revealed that only 53% of law firms have a policy to manage the retention of information/data held by the firm, and only 36% of respondents have an incident response plan.<sup>18</sup>

<sup>15</sup> David G. Ries, *2021 Cybersecurity*, American Bar Association, [https://www.americanbar.org/groups/law\\_practice/publications/techreport/2021/cybersecurity/](https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/) (last visited Dec. 4, 2022).

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

Law firms are not the only legal targets. In May of 2020, a ransomware attack hit Texas courts and took down the courts' websites and case management systems for the state's appellate and high courts.<sup>19</sup> While there is no evidence that hackers accessed sensitive or personnel information, the hack left Texas' top civil and criminal courts without a working case management system or internet in their offices which forced staff to put out rulings over Twitter.<sup>20</sup>

<sup>19</sup> Jake Bleiberg, *Texas High Courts Hit By Ransomware Attack, Refuse to Pay*, APNEWS.com (May 12, 2020), <https://apnews.com/article/hacking-tx-state-wire-technology-us-news-courts-474453285863aebab0a2fe239f493548>.

<sup>20</sup> *Id.*

The fact is, anyone with a computer connected to the Internet is susceptible to a cyberattack from computer hackers who use phishing scams, spam email, instant messages and bogus websites to deliver dangerous malware to the computer.<sup>21</sup> Once the malware program is installed on the computer, it may quietly transmit the user's private and financial information without their knowledge.<sup>22</sup> During the period of March 2021 to February 2022, 153 million new malware programs, includ-

ing ransomware programs, were discovered.<sup>23</sup> This is a 5% increase from the previous year.<sup>24</sup>

<sup>21</sup> *The Dangers of Hacking and What a Hacker Can Do to Your Computer*, Webroot, <https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers> (last visited Nov. 30, 2022).

<sup>22</sup> Id.

<sup>23</sup> Andra Zaharia, *300+ Terrifying Cybercrime and Cybersecurity Statistics (2023 Edition)*, Comparitech (last updated Feb. 8, 2023). <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/>.

<sup>24</sup> Id.

Unfortunately, the learning curve is steep for users who find their computers infected.<sup>25</sup> <sup>26</sup> Continuing education in this field is necessary given the pace of technology development. Cyberattacks that will occur in a few years' time are not conceivable today.

<sup>25</sup> Id.

<sup>26</sup> Webroot BrightCloud, *2021 Threat Report Mid-Year Addendum*, 2021, at 8.

***A Technology Security Credit Should be Mandatory Because Lack of Knowledge Can Result in Significant Professional Dilemmas.***

The following are only a few examples of technology scenarios that lead to professional pitfalls for legal professionals. CLEs on these topics can give members critical guidance that prevent negative outcomes for legal professionals and their clients.

After A Cyber Breach

Do firms have an ethical duty to notify their clients if a breach occurs? If so, there is a significant ethical issue not being addressed by lawyers given only 24% of the law firms nationwide that reported a breach in the ABA 2021 Legal Technology Survey notified their clients of the data breach.<sup>27</sup>

<sup>27</sup> Ries, *supra*.

Public Wi-fi

It has become commonplace for lawyers to connect to public wi-fi when working in coffee shops or hotels.<sup>28</sup> However, by doing so, the lawyer can expose confidential and privileged client information because the "packets" or pieces of information they send or receive from their devices can be intercepted and decoded.<sup>29</sup> Additionally, lawyers may be tricked into logging on to a fake wi-fi network set up by cyber criminals to look like the legitimate public wi-fi network.<sup>30</sup> And unknowingly, offer up their clients' information to criminals on a platform.

<sup>28</sup> Alison Austin, *Public Wi-fi: Lawyers Beware of Coffeehouse Practice*, American Bar Association (May 20, 2017), <https://www.americanbar.org/groups/litigation/committees/trial-practice/practice/2017/beware-of-public-wifi/>.

<sup>29</sup> Id.

<sup>30</sup> *What Is An Evil Twin Attack?*, Panda Security (Dec. 13, 2021), <https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/>.

Chatbots

Law firms are increasingly using Artificial Intelligence such as "chatbots" to deliver legal services and communicate with clients about their legal needs.<sup>31</sup> As such, do legal professionals have an ethical duty to train and supervise bots?<sup>32</sup> Can a legal professional or law firm be disciplined for the conduct of a chatbot? Chatbots have access to a person's personally identifiable information and other sensitive financial and medical data. Thus, are law firms in the United States that service international corporate clients subject to the requirements of the General Data Protection Regulation enacted in the European Union?

<sup>31</sup> Lisa Dimyadi, *Chatbots for Lawyers*, Clio, <https://www.clio.com/blog/chatbots-for-lawyers/> (last visited Dec. 4, 2022).

<sup>32</sup> See e.g., Wash. Rules of Prof'l Conduct R. 5.1, 5.3 (2022).

Texting

Legal professionals use text messages to contact prospective clients.<sup>33</sup> Legal professionals also use texting to communicate with existing clients.<sup>34</sup> The use of text messages raises concerns whether and how confidentiality can be maintained in these communications and what steps a legal professional should take to ensure client information is protected. At a minimum, is the legal professional aware that others may have access to the client's mobile device? Additionally, text messages are not kept by the cellular provider indefinitely for future reference. Therefore, do legal professionals need to transfer and backup text messages from their mobile phones to their computers?

<sup>33</sup> *Text Message Marketing for Lawyers*, CosmoLex, <https://www.cosmolex.com/text-message-marketing-for-lawyers-the-next-big-thing/> (last visited Dec. 4, 2022).

<sup>34</sup> Mark C. Palmer, *Ethical Considerations for Lawyers When Texting Clients*, 2Civility (Jan. 6, 2022), <https://www.2civility.org/ethical-considerations-for-lawyers-when-texting-clients/>

Use of Unencrypted Email

The use of unencrypted email to communicate with clients is generally accepted.<sup>35</sup> However, the American Bar Association warns, ... cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, legal professionals must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.<sup>36</sup>

<sup>35</sup> 3ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) (discussing securing communication of protected client information), [https://www.americanbar.org/content/dam/aba/administrative/professional\\_responsibility/aba\\_formal\\_opinion\\_477.pdf](https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf).

<sup>36</sup> Id. (referring to Model Rules of Prof'l Conduct R. 1.6 cmt. 18 (2016)).

***A Technology Security Credit Should be Mandatory to Ensure Members Are Fulfilling Their Responsibilities of Competence and Diligence.***

Despite the duty to keep abreast of the risks associated with relevant technology and that legal professionals increasingly use technology in their practice, most legal professionals lack training and experience in technology security to recognize and prevent a cyber-attack. These days, dangerous emails look like legitimate communications from your bank, Amazon, shipping carrier, or even your friend. With phishing, vishing, smishing, pharming, and spoofing tactics continually evolving and becoming more sophisticated and harder to detect, legal professionals not keeping up with the trends are at serious risk of jeopardizing client information and funds. The following statistics are troubling:

- More than 70% of phishing emails, socially engineered fraudulent messages designed to trick a person into revealing sensitive information or deploy malicious software, are opened by their targets.<sup>37</sup>
- More than 59.4 million Americans fell victim to voice phishing, also known as "vishing" in 2021.<sup>38</sup>
- Less than 35% of the United States population can correctly define smishing, phishing scams operating through text or short message service messages.<sup>39</sup>
- Millions in the US, Europe, and the Asia-Pacific region fell victim to a sophisticated pharming scam where the attackers directed bank customers to a fake website which downloaded malware to col-

lect banking credentials before being redirected to their bank's real website.<sup>40</sup>

- During the first half of 2021, 62.6% of all identity deception-based attacks, or "spoofing" attacks, leveraged display name deception that impersonated a trusted individual or brand.<sup>41</sup>

37 Nikolina Cveticanin, *Phishing Statistics & How To Avoid Taking the Bait*, DataProt (Nov. 16, 2022), <https://dataprot.net/statistics/phishing-statistics/>.

38 Trevor Cooke, *Vishing Statistics 2022: Costs of Voice Phishing Attacks*, EarthWeb (Nov. 12, 2022), <https://earthweb.com/vishing-statistics>.

39 Ben Martens, *11 Facts + Stats on Smishing (SMS Phishing) in 2022*, <https://www.safetynetdetectives.com/blog/what-is-smishing-sms-phishing-facts/> (last visited Dec. 4, 2022).

40 *What Is Pharming and How To Protect Against It*, Avast.com, <https://www.avast.com/c-pharming> (last visited Dec. 4, 2022).

41 Zaharia, *supra*.

Keeping clients' information safe is no longer just about keeping hard paper copies secure. The rise of technology in the practice of law creates several risks and raises several ethical questions. The monetary and ethical risks of failing to keep up with the benefits and risks associated with technology are significant and therefore mandating continuing legal education in this area is necessary.

#### **Technology Security Education is Effective**

Technology Security education prevents cybercrime. The following statistics demonstrate the beneficial impact of technology security training:

- Security awareness training improves overall password security by an estimated 30-50%.
- Security awareness training reduces the cost of phishing by more than 50%.
- Even a modest investment in security awareness and training has a 72% chance of significantly reducing the business impact of a cyberattack.
- Companies that engage in regular security awareness training have 70% fewer security incidents.
- Security awareness training improves phishing awareness by an estimated 40%.
- Security-related risks are reduced by 70% when businesses invest in cybersecurity awareness training.
- Trained users are 30% less likely to click on a phishing link.<sup>42</sup>

42 *10 Facts About the Benefits of Security Awareness Training*, IDAgent.com, <https://www.idagent.com/blog/10-facts-about-the-benefits-of-security-awareness-training/> (last visited Oct. 3, 2023).

#### **Other Jurisdictions with Mandatory Technology Related Credits**

By adding a required credit in technology security, Washington will join other states that recognize the necessity and value of this type of education to the legal profession. In 2023, Florida, New York, North Carolina and the U.S. Virgin Islands require or will require credits related to technology including topics related to cybersecurity.

### **III. Considerations in Support of the Mental Health Credit Requirement**

The MCLE Board presents the following as important factors in support of the suggested amendment for a new requirement for all licensed legal professionals to complete one credit each reporting period in mental health.

#### **A Mental Health Credit Requirement Should be Mandatory Because of the Prevalence of Mental Health Issues Among Legal Professionals**

Several recent studies concluded: Attorneys are prone to mental health issues, including substance abuse and addiction, depression, anxiety, and stress, more so than the general population. A nationwide



study published in the Journal of Addiction Medicine in 2016 (the "ABA Study")<sup>43</sup>, supported by the American Bar Association, studying licensed attorneys currently employed in the legal profession, who voluntarily completed surveys sent by their respective bar associations. The study found:

- 20.6% of respondents screened positive for hazardous, harmful, and potentially alcohol-dependent drinking, as compared with 6.4% of the general US population;
- 28% experienced symptoms of depression;
- 19% experienced symptoms of anxiety;
- 23% experienced symptoms of stress.

<sup>43</sup> Patrick R. Krill, Ryan Johnson & Linda Albert, The Prevalence of Substance Use and Other Mental Health Concerns Among American Attorneys, *Journal of Addiction Medicine*, pp. 46-52, 10(1) Jan/Feb 2016 [https://journals.lww.com/journaladdictionmedicine/Fulltext/2016/02000/The\\_Prevalence\\_of\\_Substance\\_Use\\_and\\_Other\\_Mental.8.aspx](https://journals.lww.com/journaladdictionmedicine/Fulltext/2016/02000/The_Prevalence_of_Substance_Use_and_Other_Mental.8.aspx)

The study concluded, "attorneys experience problematic drinking that is hazardous, harmful, or otherwise consistent with alcohol use disorders at a higher rate than other professional populations." Attorneys under 30 years old were found to be at the higher level of 32%. Further, the study found that the data underscore the need for resources devoted to address the issues of mental health and substance abuse within the legal profession, through prevention, as well as lawyers' assistance programs and, where necessary, treatment intervention. That 2016 study cited data from a 1990 study, specific to Washington State lawyers, which found that 18% of lawyers in Washington, at that time, were "problem drinkers," compared with an estimated 10% among American adults in the general population. The 1990 study found that 19% of Washington lawyers suffered from statistically significant elevated levels of depression, contrasted with estimated levels of depression in Western industrialized countries in the range of 3% - 9%.

Similarly, a recent survey conducted by ALM Intelligence and Law.com ("ALM Study")<sup>44</sup> found:

- 74% of respondents feel the legal profession has had a "negative impact" on their mental health;
- 44% use alcohol to deal with stress;
- 10% self-identify as having a problem with alcohol;
- 4% use illegal drugs or abuse prescription drugs to deal with stress;
- 64% feel they suffer from anxiety;
- 31% self-identify as depressed;
- 74% feel their work environment contributes negatively to their own or colleagues' well-being;
- 18% have contemplated suicide at some point in their careers.

<sup>44</sup> ALM's Mental Health and Substance Abuse Survey (2020), reported and summarized by Leigh Jones, Lawyers Reveal the Truth Depth of Mental Health Struggles, ALM's Mental Health and Substance Abuse Survey, <https://www.law.com/international-edition/2020/02/19/lawyers-reveal-true-depth-of-the-mental-health-struggles-378-134739/> (February 19, 2020); see also, By the Numbers: The State of Mental Health in the Legal Industry, <https://www.law.com/2020/02/19/by-the-numbers-the-state-of-mental-health-in-the-legal-industry/> (February 19, 2019)

Beyond self-assessment by respondents, the ALM Study also found that 62% of respondents know a colleague who is depressed, and 50% know a colleague with an alcohol problem.

Moreover, actual and perceived stigma is a contributing factor to mental health and addiction issues in lawyers. The ALM Study found that 65% of respondents felt they could not take extended leave to tend to mental health issues, and 77% were fearful of what their employer would think if they sought treatment through an extended leave.

***Continuing Legal Education Can Assist in Ameliorating Mental Health Issues, and Therefore the Competence of Practitioners.***

The need to address these issues, and to do so as early as possible, relates directly to competence and fitness to practice law. The proposal to require one hour of MCLE credit every three years is a crucial link in addressing this problem. While other elements are necessary to address the problem, including lawyers' assistance programs, available treatment, etc., the MCLE requirement is an entry point to provide a broad base of legal professionals with the knowledge they need for self-assessment, creating avenues of community care to reduce mental health stigma in the legal profession, and knowledge and understanding of available tools and programs, including new developments.

A typical course may include current legal requirements and standards concerning competence and mental health issues, whether in oneself or colleagues; available resources, including lawyers' assistance programs; data concerning the prevalence of mental health issues in the profession; deeper understanding of the nature of mental health issues; tools for self-assessment; common warning signs in colleagues, and deeper understanding of causes and treatments.

The courses accredited to fulfill this requirement should not be designed nor viewed as a substitute for treatment. Nonetheless, requiring every legal professional to devote one hour every three years to education concerning these crucial issues will elevate the profession, improve the overall quality of legal services, and, ultimately, encourage greater public confidence in the integrity of the profession. Moreover, this requirement may encourage members to seek the help they need, and others to be supportive of their colleagues, while maintaining standards of excellence in the practice of law.

***Other Jurisdictions with Mandatory Mental Health CLE Requirements***

In 2017 the ABA adopted the Model Rule for Minimum Continuing Legal Education and Comments ("ABA Model Rule")<sup>45</sup>, the first such promulgation since 1988. In addition to the inclusion of a diversity and inclusion requirement, one of the main highlights was the addition of a model mental health MCLE requirement. As the ABA stated:

<sup>45</sup> See ABA Model Rule for Minimum Continuing Legal Education, American Bar Association (February 6, 2017), [https://www.americanbar.org/content/dam/aba/directories/policy/midyear-2017/2017\\_hod\\_midyear\\_106.pdf](https://www.americanbar.org/content/dam/aba/directories/policy/midyear-2017/2017_hod_midyear_106.pdf).

The Mental Health and Substance Use Disorder Credit recognizes that requiring all lawyers to receive education about these disorders can benefit both individual lawyers and the profession. This requirement is in part a response to the 2016 landmark study conducted by the Hazelden Betty Ford Foundation and the American Bar Association Commission on Lawyer Assistance Programs, entitled, "The Prevalence of Substance Use and Other Mental Health Concerns Among American Attorneys."<sup>46</sup>

<sup>46</sup> ABA Model Rule Implementation Resources, American Bar Association (February 2017), <https://www.americanbar.org/events-cle/mcle/modelrule/>.

At the time, only five states had any form of mental health MCLE requirement. At present, at least eight states (as well as the U.S. Virgin Islands) have adopted some form of this requirement.

The clear trend is toward states and other jurisdictions adopting some form of a mandatory mental health CLE, whether as a separate requirement, or couched in terms of a "professional competence" requirement. This trend suggests the importance and value of a mandatory mental health CLE. The CLE requirement elevates the importance of mental health and self-care for legal professionals. Introducing this requirement can destigmatize mental health and promote awareness and

self-care. By adding a required credit in Mental Health, Washington will join other states who recognize the necessity and value of this type of education to the legal profession.

#### IV. Suggested Effective Date

The MCLE Board recommends that this suggested amendment become effective July 1, 2025, and apply to MCLE reporting periods beginning with the 2025-2027 reporting period and all reporting periods thereafter. This would allow for sufficient time for the WSBA to implement the necessary changes to the MCLE software and provide notice to licensed legal professionals and CLE sponsors.

**I. Hearing:** A hearing is not requested.

**J. Expedited Consideration:** Expedited consideration is not requested.

#### K. Supporting Material:

1. Suggested Amendments to APR 11 - Redline
2. Suggested Amendments to APR 11 - Clean

**SUGGESTED AMENDMENTS TO ADMISSION AND PRACTICE RULES  
ADMISSION AND PRACTICE RULES (APR)  
RULE 11. MANDATORY CONTINUING LEGAL EDUCATION (MCLE)**

**(a) - (b)** [Unchanged.]

#### **(c) Education Requirements**

(1) *Minimum Requirement.* Each lawyer must complete 45 credits and each LLLT and LPO must complete 30 credits of approved continuing legal education by December 31 of the last year of the reporting period with the following requirements:

(i) at least 15 credits must be from attending approved courses in the subject of law and legal procedure, as defined in subsection (f) (1); and

(ii) at least ~~six~~ five credits must be in ethics and professional responsibility, as defined in subsection (f) (2); ~~with at least one credit in equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law.~~

(iii) at least one credit must be in equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law;

(iv) at least one credit must be in the subject of technology security, as defined in subsection (f) (9); and

(v) at least one credit must be in the subject of mental health as defined in subsection (f) (10).

(2) - (6) [Unchanged.]

(7) *Carryover Credits.* If a lawyer, LLLT or LPO completes more than the required number of credits for any one reporting period, up to 15 of the excess credits, ~~two of which may be ethics and professional responsibility credits,~~ may be carried forward to the next reporting period subject to the following limitations:

(A) Only two of the 15 allowed carryover credits can be in the subject of ethics and professional responsibility;

(B) Credit requirements for the subjects of mental health; technology security; and equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law cannot be fulfilled in whole or in part with carryover credit from a prior reporting period;

(C) Excess credits from subsections (c) (1) (iii), equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law; (c) (1) (iv), technology securi-

ty; and (c)(1)(v), mental health, carry over as "Other" credits as defined in subsection (j)(1).

(d)-(e) [Unchanged.]

(f) **Approved Course Subjects.** Only the following subjects for courses will be approved:

(1) [Unchanged.]

(2) Ethics and professional responsibility, defined as topics relating to the general subject of professional responsibility and conduct standards for lawyers, LLLTs, LPOs, and judges, including equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law, and the risks to ethical practice associated with diagnosable mental health conditions, addictive behavior, and stress;

(3)-(7) [Unchanged.]

(8) Equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law;

(9) Technology security, defined as subjects that educate and inform lawyers, LLLTs, or LPOs about cybersecurity in the legal profession and the practice of law including protection of confidential, privileged, and proprietary information; client counseling and consent; storage protection policies and protocols; risk and privacy implications; protection of escrow funds; inadvertent and unauthorized electronic disclosure of confidential information, including through social media, data breaches and cyber-attacks; and supervision of employees, vendors, and third parties; and

(10) Mental health, defined as subjects that educate and inform lawyers, LLLTs, or LPOs about, but not treatment for, mental health issues in the legal profession and the practice of law including substance abuse, addictive behaviors, anxiety disorders, bipolar disorder, depression, schizophrenia, stress management, suicide prevention, and work-life balance.

(g)-(i) [Unchanged.]

(j) **Sponsor Duties.** All sponsors must comply with the following the duties unless waived by the Bar for good cause shown:

(1) The sponsor must not advertise course credit until the course is approved by the Bar but may advertise that the course credits are pending approval by the Bar after an application has been submitted. The sponsor shall communicate to the lawyer, LLLT, or LPO the number of credits and denominate whether the credits are: "law and legal procedure" as defined under subsection (f)(1); "ethics and professional responsibility" as defined under subsection (f)(2); "equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law" as defined under subsection (f)(8); "technology security" as defined under subsection (f)(9); "mental health" as defined under subsection (f)(10); or "other," meaning any of the other subjects identified in subsections (f)(3)-(7).

(2)-(7) [Unchanged.]

(k) [Unchanged.]

**Reviser's note:** The typographical errors in the above material occurred in the copy filed by the state supreme court and appear in the Register pursuant to the requirements of RCW 34.08.040.