

TO: WSBA Board of Governors
CC: Terra Nevitt, Executive Director
FROM: Todd Alberstone, Chair, MCLE Board
Bobby Henry, Associate Director for Regulatory Services
DATE: July 24, 2023
RE: MCLE Board's Suggested Amendments to APR 11

ACTION: The MCLE Board asks the Board of Governors to support its suggested amendments to APR 11 which would create and require one MCLE credit each reporting period in the subject matters of mental health and technology security.

EXECUTIVE SUMMARY

The Mandatory Continuing Legal Education (MCLE) Board is recommending amendments to rule 11 of the Admission and Practice Rules (APR). The MCLE Board's suggested amendments to APR 11 would:

- require legal professionals to earn one credit per reporting period in the subject of mental health;
- require legal professionals to earn one credit per reporting period in the subject of technology security;
- separate the already required credit in the subject of "*equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law*" from ethics and professional responsibility;
- reduce the number of required ethics and professional responsibility credits from six to five;
- allow for additional credits earned beyond the required amount for any given reporting period in the subject of "*equity, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law*" to count as ethics and professional responsibility credits;
- allow for additional credits earned beyond the required amount for any given reporting period in the subject of mental health to count as "other" credits under the subject of personal development and mental health; and
- allow for additional credits earned beyond the required amount for any given reporting period in the subject of technology security to count as "other" credits under the subject of office management.

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, inclusion, and the mitigation of both implicit and explicit bias in the legal profession and the practice of law" ("equity") would become its own category as opposed to a subcategory of ethics as it currently is. Creating a separate equity category will make it easier for members and staff to track compliance with the equity requirement.

The suggested amendments will not place a financial burden on licensed legal professionals. In 2019, the WSBA Board of Governors passed a motion directing WSBA CLE to offer free CLEs in the topics of mental health, technology security, and equity. The WSBA Board of Governors directed that the CLEs be offered in-person and on-demand for free, addressing the concern that this requirement would pose barriers to access or a financial burden for licensed legal professionals. In addition, several CLE sponsors regularly provide courses on these topics.

These suggested amendments would ensure lawyers, LLLTs, and LPOs focus 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 to practice law and, if ignored, could result in serious consequences. The proposed requirements, therefore, are directed toward the protection of clients and the public, improving legal professional competency and integrity, and, ultimately, improving the legal community as a whole. In addition, having separate categories will make it easy for members to keep track of their requirements and which ones have been met.

PROCESS

In the Fall of 2022, the MCLE Board appointed a committee to study and make recommendations regarding any subject areas that should be required learning for all legal professionals. Following months of meetings, discussion, and research, the committee recommended two subject areas—mental health ethics and technology security ethics. Notably, the committee recommended that 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 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. One, it would be too difficult to find presenters qualified to talk about the proposed subject matters and the related ethical considerations; two, it would be difficult for member to find ethics CLEs specifically on the two proposed subjects noting that ethics credits are already the most difficult to complete; and three, that it would be complicated and difficult to track compliance for the members. In light of these comments, at its June 16, 2023 meeting, the MCLE Board decided to remove the ethics component for both proposed subjects. In addition, the proposal creates separate credit categories for the subjects to make it easier for members to track their compliance. The MCLE Board, at that same meeting, decided to seek approval from the Board of Governors on its suggested amendments.

BACKGROUND

Equity Credit

The suggested amendments remove the subject of equity from the ethics subject and define equity as its own subject while maintaining the current requirement for legal professionals to earn one equity credit per reporting period. Additionally, the suggested amendments clarify that the equity requirement needs to be met each reporting period and cannot be satisfied with carryover credit. However, additional equity credits within one reporting period will count as ethics credits and may be carried over to the next reporting period as ethics credits. Finally, as discussed above, creating a separate equity category will make it easier for members and staff to track compliance with the equity requirement.

Technology Security Credit

The suggested amendments include 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.¹

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. 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 2021.² 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. ³ Washington state is ranked as the 9th highest state where internet crime victims reside.⁴ Washington state victims reported losing \$157,454,331 in 2021 as a result of internet crimes.⁵

In 2021, the IC3 received 19,954 compromised business email complaints resulting in adjusted losses at nearly \$2.4 billion.⁶ 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.

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.⁷

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 targets 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.⁸

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.⁹ 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

¹ 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

² Internet Crime Complaint Center, *2021 Internet Crime Report*, at 3 (2022), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

³ *Id.* at 18 n.16.

⁴ *Id.* at 26.

⁵ *Id.* at 27.

⁶ *Id.* at 3.

⁷ 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/>.

⁸ 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.

⁹ Internet Crime Complaint Center, *supra* note 2 at 11.

threatened to publish compromising information on former U.S. President Donald Trump if they did not receive their \$42 million demand.¹⁰ As proof, the hackers gained access to sensitive client information and published legal contracts related to the law firm's client, Madonna.¹¹ The hackers also released 2.4 GB of legal data related to client Lady Gaga.¹²

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.¹³ A breach includes incidents like a lost/stolen computer or smartphone, hacker, break-in, or website exploit.¹⁴ The actual number of victim firms could be higher as the firm may have experienced a security breach and never detected it.¹⁵ 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.¹⁶

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.¹⁷ 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.¹⁸

Cybercriminals attacked our own Washington State Bar Association ("WSBA") website, malicious code was introduced to the website targeting credit card numbers entered into the website.¹⁹ The myWSBA.org portal was taken offline in mid-November 2020, causing a major disruption for members who wanted to log into their Fastcase and Casemaker accounts, purchase a Continuing Legal Education ("CLE") product, pay their license fee, and report Mandatory Continuing Legal Education credits.²⁰ As a precaution, the WSBA asked members who purchased a CLE product or paid their license fee at myWSBA.org during the previous year to monitor their credit card for potential fraudulent activity.²¹

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.²² Once the malware program is installed on the computer, it may quietly transmit the user's private and financial information without their knowledge.²³ During the period of March 2021 to February 2022, 153 million new

¹⁰ Alex Scroton, *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>.

¹¹ *Id.*

¹² *Id.*

¹³ David G. Ries, *2021 Cybersecurity*, American Bar Association, https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/ (last visited Dec. 4, 2022).

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ 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>.

¹⁸ *Id.*

¹⁹ E-mail from Terra Nevitt, Interim Executive Director, Wash. St. B. Ass'n, to WSBA Members (Nov. 13, 2020, 13:32 PST) (email available for records request).

²⁰ *Id.*

²¹ *Id.*

²² *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).

²³ *Id.*

malware programs, including ransomware programs, were discovered.²⁴ This is a 5% increase from the previous year.²⁵

Unfortunately, the learning curve is steep for users who find their computers infected.^{26 27} 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.

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 reported a breach in the ABA 2021 Legal Technology Survey notified their clients of the data breach.²⁸

Public Wi-fi

It has become commonplace for lawyers to connect to public wi-fi when working in coffee shops or hotels.²⁹ 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.³⁰ 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.³¹ And unknowingly, offer up their clients' information to criminals on a platter.

Chatbots

Law firms are increasingly using Artificial Intelligence such as “chatbots” to deliver legal services and communicate with clients about their legal needs.³² As such, do legal professionals have an ethical duty to train and supervise bots?³³ 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?

²⁴ 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/>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ Webroot BrightCloud, *2021 Threat Report Mid-Year Addendum*, 2021, at 8.

²⁸ Ries, *supra*.

²⁹ 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/>.

³⁰ *Id.*

³¹ *What Is An Evil Twin Attack?*, Panda Security (Dec. 13, 2021), <https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/>.

³² Lisa Dimyadi, *Chatbots for Lawyers*, Clio, <https://www.clio.com/blog/chatbots-for-lawyers/> (last visited Dec. 4, 2022).

³³ 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.³⁴ If RPC 7.3 prohibits lawyers from directly soliciting prospective clients using real-time electronic contact, do text messages constitute real-time electronic contact?³⁵ If not, must the texts follow Rule 7.2, which requires communications to include the name and office address of at least one lawyer responsible for its content?³⁶

Legal professionals also use texting to communicate with existing clients.³⁷ 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?

Use of Unencrypted Email

The use of unencrypted email to communicate with clients is generally accepted.³⁸ 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.³⁹

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. Long gone are the days of the clearly dodgy email from a Nigerian prince in need, now the 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:

³⁴ *Text Message Marketing for Lawyers*, CosmoLex, <https://www.cosmolex.com/text-message-marketing-for-lawyers-the-next-big-thing/> (last visited Dec. 4, 2022).

³⁵ See Wash. Rules of Prof'l Conduct R. 7.3 (2022).

³⁶ See Wash. Rules of Prof'l Conduct R. 7.2 (2022).

³⁷ 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/>

³⁸ ABA 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.

³⁹ *Id.* (referring to Model Rules of Prof'l Conduct R. 1.6 cmt. 18 (2016)).

- 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.⁴⁰
- More than 59.4 million Americans fell victim to voice phishing, also known as “vishing” in 2021.⁴¹
- Less than 35% of the United States population can correctly define smishing, phishing scams operating through text or short message service messages.⁴²
- 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 collect banking credentials before being redirected to their bank’s real website.⁴³
- 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.⁴⁴

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.

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.

Mental Health Credit

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

The suggested amendments include a new requirement for all licensed legal professionals to complete one credit each reporting period in mental health.

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”)⁴⁵, 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;

⁴⁰Nikolina Cveticanin, *Phishing Statistics & How To Avoid Taking the Bait*, DataProt (Nov. 16, 2022), <https://dataprot.net/statistics/phishing-statistics/>.

⁴¹ Trevor Cooke, *Vishing Statistics 2022: Costs of Voice Phishing Attacks*, EarthWeb (Nov. 12, 2022), <https://earthweb.com/vishing-statistics>.

⁴² Ben Martens, *11 Facts + Stats on Smishing (SMS Phishing) in 2022*, <https://www.safetymartens.com/blog/what-is-smishing-sms-phishing-facts/> (last visited Dec. 4, 2022).

⁴³ *What Is Pharming and How To Protect Against It*, Avast.com, <https://www.avast.com/c-pharming> (last visited Dec. 4, 2022).

⁴⁴ Zaharia, *supra*.

⁴⁵ 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

- 23% experienced symptoms of stress.

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”)⁴⁶ 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.

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, recognizing issues in colleagues, destigmatizing the need for help, 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

⁴⁶ALM’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)

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”)⁴⁷, 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:

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.”⁴⁸

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.

CONCLUSION

Based on the above discussion detailing the importance of the subjects required in the potential suggested amendments, the MCLE Board recommends amending APR 11 to include a one credit requirement every three years for mental health and technology security. It is the belief of the Board that these requirements increase the protection of clients and the public and improve legal professional competency and integrity.

WSBA RISK ANALYSIS: *This section is to be completed by the Office of General Counsel, with input from the proposing entity or individual.*

WSBA FISCAL ANALYSIS: *This section is to be completed by the Finance Department, with input from the proposing entity or individual.*

⁴⁷ 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.

⁴⁸ ABA Model Rule Implementation Resources, American Bar Association (February 2017), <https://www.americanbar.org/events-cle/mcle/modelrule/>.

WSBA EQUITY ANALYSIS: *This section is to be completed by the Equity and Justice Team, with input from the proposing entity or individual.*

Attachments

- MCLE Board's Suggested Amendments to APR 11 – redline
- MCLE Board's Suggested Amendments to APR 11 – clean