NEW HAMPSHIRE BAR ASSOCIATION

Ethics Committee Advisory Opinion #2018-19/1

Border Law and Confidential Client Information: Practical Considerations and Ethical Obligations

ABSTRACT

Lawyers traveling to foreign countries remain subject to the Rules of Professional Conduct. Among a lawyer's responsibilities under the Rules are the duty to provide competent representation, which includes an obligation to remain current on developments in technology, and the duty to maintain the confidentiality of client information. Given the possibility that a lawyer's electronic devices may be subject to search without reasonable suspicion both at the U.S. border and within foreign countries, lawyers traveling abroad may need to take special precautions to ensure that the confidentiality of client information is not compromised.

ANNOTATIONS

A lawyer's ethical obligations under the Rules of Professional Conduct transcend state and international boundaries.

Lawyers traveling outside the United States must remain aware of their ethical duties with respect to the confidentiality of client information and take all steps necessary to protect that confidentiality.

A lawyer's duty under Rule 1.1 to provide competent representation to clients includes an obligation to remain current on developments in technology.

A lawyer has a general duty under Rule 1.6 to maintain a client's confidential information.

Under Rule 1.6(b)(4), a lawyer may reveal information relating to the representation of a client to the extent necessary to comply with other law or a court order.

Upon receipt of a demand for confidential client information from a court or government entity, a lawyer first must notify or attempt to notify the client, whether current or former, of the demand.

Rule 1.6(a) permits a lawyer to disclose confidential client information with the client's informed consent.

When consulting with a client regarding a demand for confidential client information from a court or government entity, the lawyer should explain the

protections afforded by Rule 1.6; the extent to which the attorney-client privilege, work product doctrine, or other privileges or immunities apply; whether the demand is valid; any grounds for challenging the demand; and the extent to which disclosure of confidential client information may raise potential criminal liability for the client.

If a client wishes to challenge a demand for confidential client information from a court or government entity, the lawyer should take steps consistent with the client's wishes and challenge the demand on any reasonable grounds.

If a challenge to a demand for confidential client information from a court or government entity is unsuccessful, the lawyer must consult with the client about the possibility of appeal.

If a challenge to a demand for confidential client information from a court or government entity is unsuccessful, the disclosure should be no greater than the lawyer reasonably believes necessary to accomplish the purpose.

If a lawyer is unable to consult with the client regarding a demand for confidential client information from a government entity, the lawyer should assert all non-frivolous claims and objections on behalf of the client.

A lawyer is obligated to be aware of how confidential client information will be handled when that lawyer is travelling internationally.

A lawyer should understand how the electronic devices with which the lawyer is traveling access and store information, and should take all reasonable steps to prevent others from accessing confidential information through that device.

INTRODUCTION

A lawyer's ethical obligations under the New Hampshire Rules of Professional Conduct (NH RPC) remain in place regardless of whether that lawyer is physically within the confines of New Hampshire or even the United States.[1] Accordingly, a lawyer crossing international borders should always be mindful of these ethical obligations. In light of recent policy pronouncements by U.S. Customs and Border

[1] NH RPC 8.5(a) ("A lawyer admitted to practice in this jurisdiction is subject to the disciplinary authority of this jurisdiction, regardless of where the lawyer's conduct occurs.").

Protection concerning the potential search of electronic devices, it is particularly important that attorneys traveling outside the United States remain aware of their ethical duties with respect to the confidentiality of client information and take all steps necessary to protect that confidentiality. While this piece will primarily focus on the ethical duties of a lawyer entering or leaving the United States, similar issues should be considered when crossing any international border.

I. BACKGROUND ON BORDER SEARCHES

A. What kind of U.S. border searches of electronic devices can be expected?

There is limited case law on border searches of electronic devices. As a general matter, searches of entrants to the United States at its borders "are not subject to any requirement of reasonable suspicion, probable cause, or warrant." [2] As the U.S. Supreme Court has explained, "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." [3]

It is less clear, however, whether this same blanket rule applies to searches of electronic devices at the border. The U.S. Court of Appeals for the 9th Circuit has held that a forensic search of a laptop required reasonable suspicion, even though that search occurred at the border.[4] The court observed that, while international travelers expect their property to be searched at the border:

---

[2] United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

[3] United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004) (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

[4] U.S. v. Cotterman, 709 F.3d 952 (9th Cir. 2013).

> "what they do not expected is that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property for days (or perhaps weeks or even months, depending upon how long the search takes.)… Such a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity. We therefore hold that the forensic examination of [the defendant's] computer required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment." [5]

Courts categorize border searches as either "routine" or "non-routine." Properly empowered officials have the statutory authority to conduct "routine" searches of persons and their personal belongings at the border without reasonable suspicion, probable cause, or a warrant.[6] A "routine" search may consist of a limited search for contraband or weapons by means of:

i. A pat-down; [7]
ii. The removal of outer garments such as jackers, hats, shoes, and the emptying of pockets, wallets, or purses; [8]
iii. The use of drug-sniffing dogs; [9]
iv. The examination of outbound materials; [10] and
v. The inspection of luggage.[11]

There is no established test to determine whether a particular search procedure is "routine" versus "non-routine". Typically, the court looks at the degree of

---

[5] Id. at 967-68.

[6] 8 U.S.C. §1357; 19 U.S.C. §1496; 19 U.S.C. §1582; see also U.S. v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

[7] U.S. v. Johnson, 991 F.2d 1287, 1291 (7th Cir. 1993).

[8] U.S. v. Beras, 183 F.2d 22, 24 (1st Cir. 1999)

[9] U.S. v. Kelly, 302 F.3d 291, 294-95 (5th Cir. 2002)

[10] U.S. v. Kolawole Odutayo, 406 F.3d 386, 392 (5th Cir. 2005)

[11] U.S. v. Okafor, 285 F.3d 842 (9th Cir. 2002).

intrusiveness associated with the particular technique. The First Circuit has identified 6 factors to be considered:[12]

i. Whether the search required the traveler to disrobe or expose intimate body parts;
ii. Whether there was physical contact with the traveler;
iii. Whether force was used;
iv. Whether the type of search exposed the traveler to pain or danger;
v. The overall manner in which the search was conducted; and
vi. Whether the traveler's reasonable expectation of privacy, if any, was invaded by the search.

The Braks Court found that only strip searches and body cavity searches are consistently "non-routine." At a minimum, courts require the presence of reasonable suspicion of criminal activity to justify a "non-routine" border search.[13]

The Fourth, Fifth, and Eleventh Circuit Courts of Appeals have also examined border searches of electronic devices within the context of the "routine" versus "nonroutine" framework.[14] Both Kolsuz and Vergara held that a "non-routine" border search of an electronic devices did not require a warrant.[15] Molina-Isidoro held that a "routine" border search of an electronic device did not require a warrant, but the Court did not reach the level of proof necessary because the search was supported by probable cause.[16]

---

[12] U.S. v. Braks, 842 F.2d 509, 511-12 (1st Cir. 1988).

[13] Montoya de Hernandez, 473 U.S. at 541.

[14] U.S. v. Kolsuz, 2018 U.S. App. LEXIS 12147 (4th Cir. 2018); U.S. v. Vergara, 884 F.3d 1309 (11th Cir. 2018); U.S. v. Molina-Isidoro, 884 F.3rd 287 (5th Cir. 2018).

[15] Kolsuz, 2018 U.S. App. LEXIS 12147 at 30-31 (holding "it was reasonable for the CBP officers who conducted the forensic analysis of Kolsuz's phone to rely on the established and uniform body of precedent allowing warrantless border searches of digital devices that are based on at least reasonable suspicion"); Vergara, 884 F.3d at 1312-13 (holding that border searches are excepted from warrant and probable cause requirements).

[16] 884 F.3d at 292-93.

Recently, U.S. Customs and Border Protection (CBP) has issued a new directive providing guidance on the border searches of electronic devices the agency believes it is authorized to conduct.[17] The directive states:[18]

> Border searches of electronic devices may include searches of the information stored on the device when it is presented for inspection or during its detention by CBP for an inbound or outbound border inspection. The border search will include an examination of only the information that is resident upon the device and accessible through the device's operating system or through other software, tools, or applications. Officers may not intentionally use the device to access information that is solely stored remotely. To avoid retrieving or accessing information stored remotely and not otherwise present on the device, Officers will either request that the traveler disable connectivity to any network (e.g., by placing the device in airplane mode), or, where warranted by national security, law enforcement, officer safety, or other operational considerations, Officers will themselves disable network connectivity. Officers should also take care to ensure, throughout the course of a border search, that they do not take actions that would make any changes to the contents of the device.

This policy goes on to create two categories of searches of electronic devices: (1) advanced searches and (2) basic searches. An advanced search is defined as "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." [19] With respect to such searches, the policy explains, the following rules govern:[20]

> In instances in which there is reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval at the

[17] CBP Directive No. 3340-049A, dated January 4, 2018,

[18] CBP Directive No. 3340-049A at Para. 5.1.2.

[19] Id. at Para. 5.1.4.

[20] Id. at Para. 5.1.4.

> Grade 14 level or higher (or a manager with comparable responsibilities), an Officer may perform an advanced search of an electronic device. Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.

A basic search is defined as "[a]ny border search of an electronic device that is not an advanced search." [21] "In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law." An advanced search, by contrast, permits the CBP agent to "review, copy, and/or analyze" the device's contents.[22]

In effect, then, CBP has self-imposed a policy quite similar to the rule imposed by the 9th Circuit in Cotterman: where CBP wishes to (in the words of that court) "mine every last piece of data" on a device, reasonable suspicion is required; less intrusive searches, however, are not subject to such a requirement.[23] The policy is also consistent with the Fourth, Fifth, and Eleventh Circuits decisions (discussed supra), which were all argued before, but decided after, the policy's issuance. Additionally, it suggests that the CBP views basic searches as analogous to "routine" searches while advanced searches are analogous to "non-routine" searches.

The Policy also addresses how CBP agents should review and handle information that they identify as, or that is asserted to be, protected by the attorney-

---

[21] Id. at Para. 5.1.3.
[22] Id. (emphasis added).
[23] 709 F.3d at 965.

client privilege or attorney work product doctrine. Upon the discovery or notification of such information, the CBP agent should seek written clarification of the materials over which the privilege or doctrine is being asserted.[24] Prior to conducting any border search of those materials, the CBP will contact CBP Associate/Assistant Chief Counsel's office. Those materials will be segregated from other information examined during the border search to ensure that any privileged materials are handled appropriately. Unless there are any materials identified that indicate an imminent threat to home security, copies of materials maintained by CBP and determined to be privileged will be destroyed, excluding a copy to be maintained by CBP Associate/Assistant Chief Counsel's office for the purposes of complying with a litigation hold or other requirements of law.[25]

B. What can be expected by a non-U.S. border search?

As may be expected, many different countries have differing border search policies and practices. A lawyer who anticipates travelling to a foreign jurisdiction with client information in tow—either physically or stored on an electronic device—would be prudent to become familiar with the policies and practices of any destination countries and any countries through which the lawyer may be travelling. The lawyer should be sure to take into account not only those policies and practices concerning border searches, but also those that concern the authorities' ability to search electronic devices anywhere within those countries.

---

[24] CBP Directive No. 3340-049A at Para. 5.2.1.1.

[25] CBP Directive No. 3340-049A at Para. 5.2.1.3.

A lawyer should not expect that other countries will have a search policy similar to that currently practiced by CBP, but should realize that different countries have different values and priorities regarding the attorney-client relationship, confidentiality, and the appropriateness of searching electronic devices. The lawyer should be prepared for the possibility that in certain countries, the lawyer may be detained until and unless access is provided to clients' confidential information. A lawyer would be wise to contemplate these considerations regardless of where the lawyer may be travelling and what borders may be crossed.

II. ETHICS RULES OVERVIEW

Having discussed the current U.S. jurisprudence surrounding border searches (and in particular border searches of electronic devices), it is worthwhile to briefly review the New Hampshire Rules of Professional Conduct (NH RPC) most pertinent to this area.

A. A lawyer's ethical obligation to maintain competence includes a duty to remain up to date on technological developments.

A lawyer has a duty, under NH RPC 1.1, to provide competent representation to clients. This duty includes an obligation to remain current on developments in technology. As the Ethics Committee has previously explained, to comply with NH RPC 1.1 a "lawyer should keep reasonably abreast of readily determinable benefits and risks associated with applications of technology used by the lawyer, and benefits and risks of technology lawyers similarly situated are using." [26] This admonition

[26] N.H. Ethics Committee Comment to NH RPC 1.1.

extends to all areas of technology, including best practices for maintaining information security.

B. A lawyer has a general duty to maintain a client's confidential information.

A client's confidential information is sacrosanct. Under NH RPC 1.6(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 falls within certain limited circumstances elucidated by the rule. Similarly, under NH RPC 1.6(c), a lawyer is obliged to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

The maintenance of such confidentiality is "[a] fundamental principle in the client-lawyer relationship," [27] and the Ethics Committee has previously cautioned that "[t]he disclosure of client confidences is an extreme and irrevocable act," [28] Importantly, "[a] lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure," [29]— and, as just discussed, competence requires at least some savviness in current technology.

For the present topic, most of the exceptions enumerated in NH RPC 1.6 are not specifically relevant to attorneys traveling abroad. However, the Rule does

---

[27] ABA Model Rule 1.6, comment (cmt.) [2],

[28] N.H. Ethics Committee Comment to NH RPC 1.6.

[29] ABA Model Rule 1.6, cmt. [16]

provide that a lawyer may reveal information relating to the representation to a client to the extent the lawyer believes it is necessary "to comply with other law or a court order." [30] What qualifies as an "other law or court order" is ill-defined, but the ABA commentary to the Model Rules suggests that the term encompasses an order from "a court or by another tribunal or government entity claiming authority pursuant to other law to compel" disclosure of otherwise confidential client information.[31]

i. Upon receiving a demand for confidential client information from a court or governmental entity claiming authority pursuant to other law, a lawyer must notify or attempt to notify the client.

Upon receipt of a demand for confidential client information from a court or government entity, a lawyer first must notify or attempt to notify the client, whether current or former, of the demand. [32] The lawyer's obligation does differ depending upon whether the client is available for consultation. NH RPC 1.6(a) permits the lawyer to disclose confidential client information with the client's informed consent. Therefore, when the client is available, NH RPC 1.4 governing client communications guides this portion of the analysis.

When the client is available, the lawyer must "promptly inform the client of any decision or circumstance with respect to which the client's informed consent is required" and "explain the legal and practical aspects of a matter and alternative courses of action to the extent that such an explanation is reasonably necessary to

---

[30] NH RPC 1.6(b)(4).

[31] ABA Model Rule 1.6, cmt. [15].

[32] See generally ABA Formal Opinion 473, Obligations Upon Receiving a Subpoena or Other Compulsory Process for Client Documents or Information (Feb. 17, 2016).

permit the client to make informed decisions regarding the representation." [33] The consultation with the client should include:[34]

1. A description of the protections afforded by Rule 1.6;
2. Whether and to what extent the attorney-client privilege, work product doctrine, or other privileges or immunities apply;
3. Whether the demand is valid;
4. Grounds for challenging the demand; and
5. The extent to which disclosure of confidential client information may raise potential criminal liability for the client.

If the client wishes to challenge the demand, the lawyer should take steps consistent with the client's wishes and challenge the demand on any reasonable grounds. If the challenge is unsuccessful, the lawyer must consult with the client about the possibility of appeal.[35] If the challenge is ultimately unsuccessful, "a disclosure adverse to the client's interests should be no greater than the lawyer reasonably believes necessary to accomplish the purpose." [36]

ii. If a lawyer is unable to consult with the client, the lawyer should assert all non-frivolous claims and objections on behalf of the client.

When the lawyer is unable to consult with the client on how to respond to the demand for confidential client information, the lawyer is obliged to raise all non-frivolous claims and objections on the client's behalf.[37] The lawyer should be sure to

---

[33] NH RPC 1.4.

[34] ABA Formal Opinion 473.

[35] See ABA Model Rule 1.6, cmt. [15] ("In the event of an adverse ruling [requiring the production of confidential information], the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4.").

[36] ABA Model Rule 1.6, cmt. [16].

[37] See ABA Model Rule 1.6, cmt. [15] ("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."); see also Bd.

document all efforts made to attempt to notify the client before making a response to the demand.

When a client is unavailable for consultation, the ABA has taken a position that a lawyer is not ethically obligated to pursue an appeal of an adverse ruling.[38] There is no formal ruling on this issue in New Hampshire.

III. PRACTICAL DISCUSSION: ETHICS ON THE BORDER

Given the very real possibilities of border searches and searches without even reasonable suspicion within foreign countries, the safest alternative will always be for the lawyer to avoid traveling with any electronic devices containing confidential information. Practically speaking, of course, that is not always an option—indeed, a lawyer may need to travel abroad to meet with a client or for other work-related purposes that require the lawyer to travel with a laptop, cellular telephone, or other electronic device. When bringing an electronic device abroad is unavoidable, there are a number of considerations of which the lawyer should be aware.

Suppose the following hypothetical: a criminal defense lawyer is leaving New Hampshire to travel to the Philippines for two weeks. The lawyer plans to bring a laptop and cellular telephone along to facilitate working from the beach and maintaining access to work email.

The lawyer is obligated to be aware of how confidential client information will be handled when that lawyer is travelling. Any lawyer travelling out of the United

---

Of Prof'l. Responsibility of the Supreme Ct. of Tenn. Formal Op. 2014-F-158 (2014); D.C. Bar Op. 288 (1999); D.C. Bar Op. 14 (1976).

[38] See ABA Formal Op. 473.

States and planning on returning can reasonably anticipate how electronic devices will be handled by CBP. The lawyer can reasonably expect that a CBP agent will review and analyze the contents of the devices. The lawyer also can reasonably expect that the CBP will not seek to access any information that is not stored locally on the devices. Finally, the lawyer can reasonably expect that a CBP agent will not seek to access information the lawyer identifies as protected by attorney-client privilege or the work-product doctrine.

It may not be possible, however, for the lawyer to reasonably anticipate how authorities in other countries will handle clients' confidential information stored on the electronic devices. Some countries may provide protections similar to those in place in the United States, whereas others may have no protection in place at all and allow unfettered access to the contents of such devices — and even to documents and information that can be accessed remotely through an electronic device. As noted above, it thus is incumbent upon the lawyer traveling to the Philippines with a laptop and cellular telephone to understand how that country, and any other country through which the lawyer may travel, could treat the devices.

In addition to general awareness of the risks involved with travelling abroad with electronic devices, an attorney should also take the following matters into account.

A. The lawyer should understand how the electronic devices with which the lawyer is traveling access and store information, and should take all reasonable steps to prevent others from accessing confidential information through that device.

As mentioned at the outset of the article, under NH RPC 1.6 a lawyer is obliged not only to personally maintain the confidentiality of client information but also to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." When traveling with an electronic device, a lawyer can take several steps to help maintain the security of client information.

One way to minimize the risks of disclosing confidential client information when traveling abroad is to minimize the confidential client information the lawyer must take along. If the lawyer has sufficient resources available, in lieu of bringing the lawyer's normal laptop and cellular phone the lawyer may wish to bring stripped-down devices that have no information stored locally but are able to access information remotely through a remote desktop or cloud program. Where that is not an option, a risk-averse lawyer should nonetheless carefully review the electronic devices with which the lawyer will be traveling for confidential client information and remove unnecessary information to prevent it from being accessed later. The lawyer should also be aware that, in many cases, simply deleting the information will not actually remove that information from the device. Additional steps specific to the device must be taken to ensure the information has been permanently deleted.

Yet another way to minimize the risk of disclosing confidential client information is to electronically "lock" all devices so they cannot be opened without the

correct "key." At minimum, this includes password-protecting all devices (a wise step even for a lawyer who is not contemplating international travel). It may also include using a device that employs fingerprint- or facial recognition software. Combining biometric and alphanumeric (password) security measures may provide the greatest practical security to a lawyer's electronic devices. In this way, the lawyer can ensure that the lawyer's devices will not easily be accessed without the lawyer's presence and/or consent.

The lawyer also should consider what information and networks are accessible by the lawyer's electronic devices and whether other electronic devices are able to access those devices with which the lawyer is traveling. The lawyer should examine email, email settings, hard drive, network drive, and backup settings to understand how the electronic devices are storing information and where that information is being stored. Some commonly-used email programs such as Microsoft Outlook save information locally, and those programs can be opened, and messages contained within them viewed, even when a device is offline. A lawyer should avoid locally storing confidential client information on any transportable electronic devices to the greatest degree possible when traveling internationally. This minimizes the risk of the disclosure of confidential client information.

The lawyer should be extremely careful when using USB plugs and physically connecting an electronic device to other devices. For instance, some airports provide charging stations that permit a person to charge devices using only a USB cord, rather than a USB cord and plug. The prudent lawyer should avoid using such

locations. While the charging station is charging the connected device, it could also be using the USB cord to surreptitiously access and copy information from that device. The best course of action is for the lawyer to carry appropriate cords and plugs and to only charge devices directly from an outlet or trusted device. Finally, when a lawyer must travel with confidential client information, the lawyer should be able to identify any specific files, file types, folders, categories of files, names, email addresses, phone numbers, or other information that may assist in identifying the protected information. A lawyer may consider organizing the confidential client information in a discrete folder and therefore segregating it from the other information that may more properly be the subject of a basic search. Additionally, a lawyer may consider taking additional steps to protect electronic devices, including obtaining additional and more sophisticated encryption.

B. The lawyer must be prepared to notify or attempt to notify a client if authorities seek to review, copy, and/or analyze any client's confidential information.

As discussed *supra*, the lawyer has an ethical obligation to notify or attempt to notify the client if a CBP agent, or an agent of another country or agency, seeks to review any client's confidential information. If the lawyer is unable to notify the client, the lawyer must make all non-frivolous objections and claims to protect the client's information. While the circumstances surrounding the search are reasonably considered in this obligation, the lawyer should be reasonably prepared to make the attempt to contact the client and to document the steps taken to do so. Absent clear direction from the client, the lawyer should notify the CBP or foreign agent of the existence of the confidential client information on the lawyer's electronic devices,

provide any non-frivolous objections and claims to shield it from review, and provide the information necessary to identify the confidential client information. Once a privilege has been asserted over the confidential client information, the lawyer should continue attempts to notify the client and protect the client's interests until the client is reached and can provide guidance to the lawyer.

CONCLUSION

Technological advances permit an attorney to carry and access clients' most precious confidential information using a single handheld device while traveling a world away from the office. Similar advances permit a border agent to extract and copy any files on that device in moments. An attorney crossing international borders must carefully consider what devices should be brought along, what information is stored on those devices, what information is accessible from those devices, and the security of those devices. Sometimes, the best way to protect clients' information may be to leave it at the office.

NH RULES OF PROFESSIONAL CONDUCT:

Rule 1.1

Rule 1.4

Rule 1.6

Rule 8.5

SUBJECTS:

Client Communications

Competence

Confidentiality

Confidentiality of Information

By the NHBA Ethics Committee

This opinion was submitted for publication to the NHBA Board of Governors at its January 7, 2019 Meeting.