ETHICS: COMPETENCE AND CANDOR

FEDERAL PRACTICE INSTITUTE

NOVEMBER 2014

Materials by:

Richard Y. Uchida, Esq.
Hinckley, Allen & Snyder
11 South Main Street, Ste. 400
Concord, NH 03301

Richard Guerriero, Esq.
Lothstein Guerriero
7 Main Street, Ste. 5
Keene, NH 03431

1. COMPETENCE

Hypothetical …….....1

The Ethics of Competence in the Age of Technology, by Richard Y. Uchida…... 2

1. GENERAL GUIDANCE ON THE USE OF CLOUD COMPUTING AND 3RD PARTY VENDORS TO STORE CLIENT DATA……..…… 6

NHRPC Rule 1.2 - Communication ……..... 6
NHRPC Rule 1.6 - Confidentiality of Information (Proposed) …… 6
NHRPC Rule 1.15 - Safeguarding Client Property ……... 6
NHRPC Rule 1.16 - Terminating Representation …….…… 6
NHRPC Rule 5.3 - Responsibilities Regarding Non-Lawyer Assistance .. 6

2. WHOOPSIES: INADVERTENT DISCLOSURE OF CONFIDENTIAL INFORMATION …….. 8

3. BRIEF SUMMARY OF NEW HAMPSHIRE AND MASSACHUSETTS DATA PROTECTION LAWS ……..…….. 11

New Hampshire Data Breach Law: N.H. Rev. Stat. § 359-C:19, *et seq.* .. 12
Massachusetts Data Breach Law: Mass. Gen. Laws 93H § 1 *et seq*. 12

4. ETHICS AND DATA BREACHES ……..... 15

5. SOCIAL MEDIA AND THE ETHICS OF CLIENT CONFIDENTIALITY …. 18

2. CANDOR

Hypothetical…… 20

Candor to the Tribunal: Statements by Counsel, by Richard Guerriero…… 21

THE STANDARDS FOR PROFESSIONAL CONDUCT ARE THE NEW HAMPSHIRE RULES OF PROFESSIONAL CONDUCT ……... 21

Local Rules 83.1 and 83.5 ……..…….. 21

THE IMPORTANCE THE NEW HAMPSHIRE SUPREME COURT PLACES ON CANDOR ……21

RULES REGARDING ATTORNEY CANDOR TO THE TRIBUNAL …….….. 22

Knowledge of Falsity…….. 23
The Obligation to Take Remedial Measures ……..... 24
Materiality and Confidentiality …….. 24
Omissions …… 24

1. Competence - Hypothetical

GEO-TAGGING HYPOTHETICAL

Your client, Marc, is a divorce attorney who is very successful and is well-known in the local community. He is contacted by a prominent politician, Anne, who tells him that she intends to file for divorce, which she expects will be a surprise to her spouse.

Marc agrees to meet with Anne to discuss her case. Because of her high-profile stature, Anne cautions Marc not to disclose their meeting, lest her plans be revealed. Marc suggests an out-of-the-way restaurant where they are not likely to be recognized. The meeting goes well and Anne retains Marc to represent her.

On his way back to his car, Marc tweets, "Had a great meeting with new client. Life is good." Marc has recently started to use Twitter as a business-development tool and already has several hundred followers. Because he has enabled the "Tweet Your Location" feature in his Twitter account, his update includes his exact coordinates at the time of his post.

As luck would have it, a waiter from the restaurant takes a break after Marc and Anne leave and has logged into Twitter from his iPhone. The waiter, who makes it a point to follow local businesspeople, including Marc, on Twitter, sees Marc's tweet about meeting his "new client". The tweet, which is geotagged, appears with an address one block away from the restaurant. The waiter quickly figures out that the "new client" is Anne, and posts to his several thousand Twitter followers: "Just waited on Marc who lunched with Anne – does this mean Anne is soon to be an ex and back on the dating scene??"

To make matters worse, Anne's son calls during lunch. He has come home from college for a surprise visit but has forgotten his key. After explaining to Marc that her son will believe she is at lunch with a constituent, Anne tells her son to stop by to pick up the key. The son is at the restaurant for a moment but being a devoted Facebook user, he uses his mobile phone to "check in" to the restaurant. (Facebook Places enables users to "check in" to a location, and to "tag" their friends and check them in, as well.) He also "checks in" with his mother. All of the son's Facebook friends now know about the lunch.

QUESTIONS:

1. Did Marc violate his <u>ethical</u> duties to his client, Anne, and if so, what ethical duties did he violate and why?

2. Should Marc, in fulfilling his <u>ethical</u> duties and upon learning Anne's son was poised to stop by, have warned Anne about the use of Facebook Places and similar tagging programs?

The Ethics of Competence in the Age of Technology

By Richard Y. Uchida
Partner
Hinckley, Allen & Snyder, LLP

"A computer lets you make more mistakes faster than any invention in human history – with the possible exceptions of handguns and tequila." - United States v. Carelock, 459 F.3d. 437, 443 (3d Cir. 2006).

The professional conduct rule on competence is one of those rules most practitioners take for granted. It is a simple rule: "A lawyer shall provide competent representation to a client." New Hampshire Rule of Professional Conduct (NHRPC) 1.1(a). The rule then notes that at a minimum, legal competence requires:

- Specific knowledge about the fields of law in which the lawyer practices.
- Performance of the techniques of practice with skill.
- Identification of areas beyond the lawyer's competence and bringing those areas to the client's attention.
- Proper preparation; and
- Attention to details and schedules necessary to assure the matter undertaken is completed with no avoidable harm to the client's interest.

NHRPC 1.1(b).

It is intuitive that a practitioner must be competent. But with the growth of technology in the practice of law, the challenges to be competent have grown geometrically. Thus, if legal competence means the "performance of the techniques of practice with skill" and identifying for clients those "areas beyond the lawyer's competence", how can a lawyer be (or remain) competent with the technological advances that seem to happen with lightning speed? The ABA

comments to Rule 1.1, which have not been fully imported into the New Hampshire Rule comments, note that:

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

While staying abreast of technology implicates such issues as marketing and advertising, as well as the use of technology in litigation, nowhere is this challenge more apparent than in the area of confidentiality. Gone are the days when a locked briefcase, a locked file drawer, and a locked office made up the safeguards one needed to protect information. Use of the internet, cloud storage, e-mail, e-filing, the practice of attorneys to engage in "blawging", micro-blogging, and the use of Twitter, LinkedIn, Facebook, Skype and similar applications, together with geo-tagging applications like FourSquare, and the use of public wi-fi hot spots, make the protection of confidential information a much more difficult task for lawyers and law firms. As noted in a report to ABA Commission on Ethics Resolution to Amend the ABA Model Rules of Professional Conduct (August 2012):

> "Technology can increase the quality of legal services, reduce the cost of legal services to existing clients, and enable lawyers to represent clients who might not otherwise have been able to afford those services. Lawyers, however, need to understand that technology can pose certain risks to clients' confidential information and that reasonable safeguards are ethically required.
>
> "The Commission's proposals are designed to help lawyers understand these risks so that they can take appropriate and reasonable measures when taking advantage of technology's many benefits. The proposals also update the language of the Model Rules so that it reflects the way that law is practiced in the 21st century."

As a result, the ABA recommended, among other things, amending the opening professional conduct rule (Model Rule 1.1) because:

> "The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology

> and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document.
>
> "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase "including the benefits and risks associated with relevant technology," would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

With this as a backdrop, a few reminders are in order in the context of confidentiality and technology. First, recall that under the Rules of Professional Conduct, all information received in connection with the representation of a client is presumed to be confidential. *See* New Hampshire Rules of Professional Conduct (NHRPC) Rule 1.6(a). Note that the rule states that "a lawyer shall not reveal information related to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b)." Paragraph (b) sets forth some limited exceptions dealing with reasonably certain death, substantial bodily harm, a criminal act that is likely to result in substantial injury to the financial interest or property of another, securing of legal advice about compliance with the rule, establishing a defense or claim, or complying with a law or court order. *See* NHRPC 1.6(b)(1)-(4).

Second, note that because of the way the rule is worded, confidential information need not come from the client, but can come from any source. It need only be "information related to the representation of a client." NHRPC 1.6(a). Third, recall that in order for a client to give informed consent to the release of confidential information, a person must agree "to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of

conduct." NHRPC 1.0(e). *See also* NHRPC 1.4(b) (requiring a lawyer to explain the legal and practical aspects of a matter and alternative courses of action to permit the client to make informed decisions.)

Raising these points reminds lawyers that the universe of confidential information a lawyer receives, and must therefore safeguard, is large, indeed. As a result, the ABA has proposed a new Model Rule 1.6(c), a form of which is under consideration by the New Hampshire Supreme Court. It provides that "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Factors which determine what might constitute reasonable efforts include (i) the sensitivity of the information, (ii) the likelihood of disclosure if additional safeguards are not employed, (iii) the cost of such additional safeguards, (iv) the difficulty of implementing the safeguards, and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients. *See* Comment 18 to ABA Model Rule 1.6.

These materials explore several aspects of protecting client confidentiality in the age of technology. Those areas include:

(1) Use of third party vendors to store client information, including the storage of information in the "cloud".

(2) Whoopsies: Dealing with the inadvertent transmission of confidential information.

(3) Data protection laws (which admittedly go beyond the world of ethics.)

(4) The evolving world of a lawyer's ethical and legal responsibilities in the wake of a data breach.

(5) A brief view into how social media can unintentionally result in the revelation of confidential information.

1.

GENERAL GUIDANCE ON THE USE OF
CLOUD COMPUTING AND 3RD PARTY VENDORS TO STORE CLIENT DATA

The ABA Model Rules do not specifically address cloud computing, but use of these services implicates principles found in several rules, in addition to the comment to ABA Model Rule 1.1, set forth above:

NHRPC Rule 1.4 – Communication

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

NHRPC Rule 1.6 – Confidentiality of Information (proposed)

- A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client

NHRPC Rule 1.15 – Safeguarding Client Property

- Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of six years after termination of the representation.

NHRPC Rule 1.16 – Terminating Representation

- Upon termination of representation, a lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred. The lawyer may retain papers relating to the client to the extent permitted by other law.

NHRPC Rule 5.3 – Responsibilities Regarding Non-Lawyer Assistance

- Comment 3: A lawyer may use non-lawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, ***and using an Internet-based service to store client information***. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations.

Worth reviewing is New Hampshire Bar Association Ethics Opinion 2012-13/4 on cloud computing. Of note is that it states:

- Cloud computing is permissible so long as the attorney takes “reasonable steps” to protect client data.

- A lawyer must be competent in understanding how and where data is stored and what the service agreement says.

- An attorney must consider the following issues before using or selecting a cloud computing service:

    - Is the provider of cloud computing services a reputable organization?
    - Does the provider offer robust security measures?
    - Is the data stored in a format that renders it retrievable as well as secure? Is it stored in a proprietary format and is it promptly and reasonably retrievable by the lawyer in a format acceptable to the client?
    - Does the provider commingle data belonging to different clients and/or different practitioners such that retrieval may result in inadvertent disclosure?
    - Do the terms of service state that the provider merely holds a license to the stored data, as, for example, Google's do?
    - Does the provider have an enforceable obligation to keep the data confidential?
    - Where are the provider's servers located and what are the privacy laws in effect at that location regarding unauthorized access, retrieval, and destruction of compromised data?
    - Will the provider retain the data – and, if so, for how long?
    - Do the terms of service obligate the provider to warn the lawyer if information is being subpoenaed by a third party, where the law permits such notice?
    - What is the provider's disaster recovery plan with respect stored data? Is a copy of the digital data stored on-site?

Several different articles about cloud computing note other safeguards and questions to ask in order for lawyers to take advantage of these resources and comply with these rules regarding technology, including:

- Selecting the right vendor/cloud service:

    - Evaluate the vendor’s practices, reputation and history.
    - Evaluate the vendor’s measures for safeguarding the security and confidentiality of stored data and ensure they are *at least* as good as your own standards.
    - Consider whether the lawyer will have the ability to encrypt data using higher level encryption tools.
    - Consider where the vendor will store the data and whether another state’s or country’s laws might apply.
    - Consider the vendor’s financial health and the impact on your data if they go out of business.

- Determine if, and how, your client's data will be segregated from other clients' data.

- Negotiating Protections into Your Contract

  - Require third party vendor to agree preserve the confidentiality and security of the materials.
  - Require the vendor to notify you if its storage server, or any other system is breached.
  - Provider should explicitly agree that it has no ownership or security interest in the data and the agreement should clearly state that the attorney owns the data.
  - Assert the right to audit the provider's security procedures and to obtain copies of any security audits performed by others.
  - Ensure vendor retains the data for the appropriate amount of time and will return or destroy the data when necessary.

- Monitoring the vendor during your relationship

  - Periodically review the vendor's system to ensure system remains in compliance with evolving technology and legal requirements.
  - Create plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data
  - Consider backing up data to allow the firm to restore data that has been lost, corrupted or accidentally deleted.
  - Engage in periodic education about ever changing security risks presented by the Internet.

- Taking appropriate steps when that relationship ends

  - Ensure all client data is returned to you, preserved if necessary, and destroyed only when appropriate.

2.

WHOOPSIES: INADVERTENT DISCLOSURE OF CONFIDENTIAL INFORMATION

There are few feelings worse than hitting the "send" button on your computer and sending information or material to someone who was never intended to receive it. Apart from the embarrassment and humiliation of the event, a lawyer may very well have handicapped or substantially harmed the case of the lawyer's client.

The current New Hampshire rule (NHRPC 4.4(b)) tries to provide solace to lawyers who commit such a *faux pas*, by providing that:

> (b) A lawyer who receives materials relating to the representation of the lawyer's client and knows that the material was inadvertently sent shall promptly notify the sender and shall not examine the materials. The receiving lawyer shall abide by the sender's instructions or seek determination by a tribunal.

The New Hampshire Bar Association Ethics Committee has also issued an opinion relating to NHRPC 4.4(b) in the context of inadvertent disclosure, review and use of metadata in electronic materials. *See* NH ECOP #2008-2009/4: Disclosure, Review and Use of Metadata in Electronic Materials. It notes that lawyers sending electronic materials to opposing counsel are ethically required to take reasonable care to avoid improper disclosure of confidential information contained in metadata. That care might include appropriate training and education on reasonable measures that can be taken to reduce the likelihood of improper disclosure of confidential information through transmission of metadata. The opinion notes that there is no *per se* rule on what constitutes reasonable care in transmission of metadata, as the facts and circumstances of each case dictate the reasonableness of protective measures taken by sending lawyers.

In recent changes to the comments of Model Rule 4.4(b), the ABA has noted that:

> "Paragraph (b) recognizes that lawyers sometimes receive a documents or electronically stored information that was mistakenly sent or produced by opposing parties or their lawyers. A document or electronically stored information is inadvertently sent when it is accidentally transmitted, such as when an email or letter is misaddressed or a document or electronically stored information is accidentally included with information that was intentionally transmitted. If a lawyer knows or reasonably should know that such a document or electronically stored information was sent inadvertently, then this Rule requires the lawyer to promptly notify the sender in order to permit that person to take protective measures. Whether the lawyer is required to take additional steps, such as returning or deleting the document or electronically stored information, is a matter of law beyond the scope of these Rules, as is the question of whether the privileged status of a document or electronically stored information has been waived. Similarly, this Rule does not address the legal

> duties of a lawyer who receives a document or electronically stored information that the lawyer knows or reasonably should know may have been inappropriately obtained by the sending person.[1] For purposes of this Rule, ''document or electronically stored information'' includes, in addition to paper documents, email and other forms of electronically stored information, including embedded data (commonly referred to as "metadata"), that is subject to being read or put into readable form. Metadata in electronic documents creates an obligation under this Rule only if the receiving lawyer knows or reasonably should know that the metadata was inadvertently sent to the receiving lawyer.
>
> In its report supporting the amendment of Rule 4.4(b), the ABA noted that:
>
> "Technology has increased the risk that confidential information will be inadvertently disclosed, and Model Rule 4.4(b) addresses one particular ethics issue associated with this risk. Namely, it provides that, if lawyers receive documents that they know or reasonably should know were inadvertently sent to them, they must notify the sender.

To alleviate the risk of unintended harm through inadvertent disclosure and in the context of transactional law (as opposed to litigation), one might use the principles in NHRPC 4.4(b) to negotiate a "clawback agreement". The agreement should state that inadvertent disclosure of a document, metadata or information does not constitute a waiver of privilege. It should establish a procedure and time frame for returning and/or destroying inadvertently produced information and materials. It should also require an attorney who receives inadvertently produced material to secure the return of any such material from third parties who may have received it. Finally, it should contain restrictions on the use or disclosure of inadvertently produced information or materials, and should describe the standard for determining whether there was a waiver of such clawback protections if a court is required to rule on whether confidential materials were produced inadvertently.

The Federal Rules of Evidence also allow a party to protect itself before an inadvertent disclosure occurs. Parties may enter into an agreement, or a federal court may issue an order, to prevent a privilege waiver when a document is inadvertently disclosed, regardless of the care a

[1] However, New Hampshire's rule DOES outline duties of the receiving attorney, as noted above.

party uses to prevent the disclosure of privileged information. *See* Fed. R. Evid. 502(d), 502(e). A court order issued pursuant to Fed. R. Evid. 502(d) is binding not only on the parties to the case, but on third parties as well. However, contrary to the plain language of 502(d) and (e), some courts have read a reasonableness requirement into those provisions. Therefore, practitioners should still employ reasonable measures to prevent disclosure of privileged documents. But, a protective order or agreement between the parties may provide another layer of protection against a privilege waiver by inadvertent disclosure. For a comprehensive discussion and suggestions on how to limit the risk of privilege waiver, *see* Paul W. Grimm, Lisa Yurwit Bergstrom, Matthew P. Kraeuter, Federal Rule of Evidence 502: Has It Lived Up to Its Potential?, 17 Rich. J.L. & Tech. 8 (2011).

Keep in mind that New Hampshire's rule NHRPC 4.4(b) governs the conduct of New Hampshire lawyers or lawyers practicing in New Hampshire. Several ethics opinions in other jurisdictions, including ABA Formal Opinion 06-442, have concluded that Rule 4.4 does not prohibit a lawyer from reviewing metadata inadvertently sent. Finally, there are court rules on the inadvertent disclosure of *privileged information,* which is a subset of confidential information. However, the reach of those court rules is beyond the scope of this presentation.

3.

BRIEF SUMMARY OF NEW HAMPSHIRE AND MASSACHUSETTS DATA PROTECTION LAWS

Although slightly beyond the scope of one's *ethical* responsibilities to safeguard a client's confidential information, it is worth taking a small diversion to note the data protection laws in New Hampshire. I have also included a summary of the laws in Massachusetts because so many of us do business with Massachusetts clients, and the prevailing wisdom is that the

Massachusetts law will become the standard for data protection (and thus, the standard of care) in the future.

New Hampshire Data Breach Law: N.H. Rev. Stat. § 359-C:19 *et seq*.

Personal Information Definition:

- "Personal information" means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

  (A) Social security number;
  (B) Driver's license number or other government identification number;
  (C) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

- "Personal information" shall not include information that is lawfully made available to the general public from federal, state, or local government records.

Security Breach Definition:

- Unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Application:

- Any person doing business in this state who owns or licenses computerized data that includes personal information;
- Any person engaged in trade or commerce that is subject to RSA 358-A:3, I;
- Any person or business that maintains computerized data that includes personal information that the person or business does not own.

Massachusetts Data Breach Law: Mass. Gen. Laws 93H § 1 *et seq*.

Personal Information Definition:

- A resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relates to such resident:

  - Social Security Number;

- Driver license or MA identification card number; or
- Financial account number, or credit card number, with or without any required security code, access code, personal ID number or password, that would permit access to a resident's financial account.

- Such information does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Security Breach Definition:

- The unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.

- A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Application:

- A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the Commonwealth, <u>or</u> a person or agency that owns or licenses data that includes personal information about a resident of the Commonwealth.

Notification Obligation:

- An entity that <u>owns the data</u> shall provide notice to the affected residents, as soon as practicable and without unreasonable delay, when such person or agency:

  (1) knows or has reason to know of a breach of security;

  (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, <u>to the attorney general, the director of consumer affairs and business regulation and to such resident</u>, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Third Party Notification Obligation:

- An entity that maintains, but does not own the data shall provide notice to the affected residents, as soon as practicable and without unreasonable delay, when such person or agency:

  (1) knows or has reason to know of a breach of security;

  (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter.

- Any such entity shall cooperate with the owner or licensor of such information. Cooperation shall include, but not be limited to, informing the owner or licensor of the breach, of the date or approximate date and nature of the breach, and any steps already taken or planned. Such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.

Contents of Notification:

- The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

Methods of Notification:

Any notice to a resident, owner or licensee required by the provisions of this section may be provided by one of the following methods:

- If total cost of notification under $250,000:

  (1) written notice;
  (2) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC § 7001(c); and chapter 110G; or
  (3) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

- If total cost of notification over $250,000, substitute notice permissible by:

(1) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;
(2) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and
(3) publication in or broadcast through media or medium that provides notice throughout the commonwealth.

Notice Exception for Criminal Investigations:

- Notice may be delayed if a law enforcement agency determines that it may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination.
- Notice is required as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as above.
- The entity shall cooperate with law enforcement in its investigation, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.

Additional Relevant Provisions:

- Failure to Comply: The Attorney General may bring a 93A or other action against any entity that fails to comply.
- Detailed requirements for written information security programs and computer system security programs, including encryption of transmitted records and files containing personal information that will travel across public networks and encryption of all personal information data to be transmitted wirelessly, as well as encryption of personal information stored on laptops and other portable devices.
- Secure user authentication, secure access control, reasonable monitoring to detect unauthorized access, up-to-date firewall protection, up-to-date security software (including patches and virus definitions) and education and training of employees.

4.

ETHICS AND DATA BREACHES

Most data breaches involving law firms and lawyers fall into three main categories: (1) careless disposal of confidential information, (2) theft of mobile devices, and (3) misuse of internal security protocols. The professional conduct rules governing a lawyer's ethical responsibilities pertaining to data breaches are rules we have previously examined – NHRPC

Rule 1.1 related to competence and NHRPC Rule 1.6, including the proposed NHRPC 1.6(c) related to protecting confidential information pertaining to the representation of a client.

But what do these rules mean in practice? Put differently, what are our responsibilities to a client regarding the protection of their confidential information from data breaches. A bevy of articles and materials suggest that competence and reasonable efforts at protection could come to mean OR already do mean the following:

Generally – Client Advice

□ Attorneys will be treated as the "quarterback" in advising clients about breaches – both to prevent them and to address them when they occur. They will need to assess all risks emanating from a breach by that lawyer's particular client including financial, reputational, criminal, regulatory, and civil liability risks, and to plan (in advance of a breach) and to react (following a breach) accordingly.

□ Lawyers will need to advise clients about "business espionage" as well as media espionage (i.e. – The Murdoch/*News of the World* scandal), and "spear fishing" (An e-mail that contains malware if opened, with taglines such as "Check this out – you're quoted" or "Referring a Case to You").

□ Lawyers should insist that clients who possess confidential information have:

- Passwords on mobile devices
- Encrypted back-up data
- Encrypted e-mail
- Timely installation of security patches
- Monitoring of USB ports
- Control/prohibition of file-sharing applications such as DropBox.
- Longer passwords (8 characters can be deciphered in 2 hours, 4 characters in 15 minutes and 12 characters in 17 years.)
- Policies to wipe computers and mobile devices when disposing of them
- Remote wiping programs
- Policies on wireless connection use: What one can and cannot work on or access while on a public wireless connection
- Secure destruction policies: Redaction, burning, shredding and pulverizing
- Compliance oversight when court rules or statutes require redaction of information in filed/submitted materials.
- Policies about when and how confidential information may be removed from the workplace, whether on mobile devices, in paper form or otherwise.
- Data breach reporting and incident response protocols.

Inside Your Law Firm

In addition applying some of the same points above to your firm:

- □ In-house lawyers should have (and understand) network diagrams, and review maintenance of computer logs. They should oversee enforcement and monitoring of security policies. They should understand that breaches can occur due to conduct from those inside the company, as well as outside of the company and design policies and practices around such potential breaches.

- □ If limited security information is supplied to outside vendors, contractual arrangements will need to be made to protect that information, as well as regulation of conduct when vendors are in areas (physically and/or electronically) containing confidential information.

- □ Lawyers must stay abreast of technology and/or engage someone who can ensure that lawyer's competence in areas of technology.

- □ Lawyers may need to enter into agreements with opposing counsel to ensure that if confidential information is produced in discovery, the opposing lawyer and his/her firm has adequate security procedures and protections.

- □ Routine encryption of e-mail.

- □ Lawyers will need to acknowledge (to clients) and understand client security protection measures in fee agreements and guarantee compliance by the lawyer and the lawyer's firm.

Post-Breach

- □ Confidentiality agreements should be reached between clients and information security vendors who investigate data breaches, and such investigations should occur under the auspices of an attorney to try to protect those investigations on grounds of privilege or work product.

- □ Clients with in-house counsel should be advised that use of in-house counsel to investigate data breaches may not protect such investigations from disclosure. That is, the investigation reports may not be privileged or confidential if in-house counsel was acting in a business versus legal capacity.

- □ Lawyers must ensure preservation of evidence about what was happening within systems containing confidential information at the time of breach: Avoiding spoliation through use of a computer forensics expert.

□ Lawyers must also ensure satisfaction of notification requirements to third parties set forth in relevant statutes in jurisdictions having such requirements. These jurisdictions are likely to be those where a client does business and a breach occurs.

In addition, some of the system and security requirements in the data protection statutes, summarized in Section 3, above, could become the basis for common law or ethical duties related to reasonable confidential information protection.

5.

SOCIAL MEDIA AND THE ETHICS OF CLIENT CONFIDENTIALITY

It is noteworthy that there are a number of articles which note that use of social media may be necessary for diligent client representation. This is because NHRPC Rule 1.3, comment A, provides that "a lawyer must also act with commitment and dedication to the interests of the client and with zeal in advocacy upon the client's behalf." Thus:

* Lawyers may, in some circumstances, have an ethical duty to actually use social media to obtain private (and perhaps even confidential) information related to representation of a client. Ignorance of social media may be punishable as ignoring an important client representation tool, causing the lawyer to run the risk of missing evidence, locating witnesses, and exposing potential biases or improprieties (example: 66 percent of divorce attorneys use Facebook as their primary source for online evidence).

* Social media requests to a potential client, and the ability to reach that prospective client's private and possibly confidential information, may be useful in screening potential clients, who may not be forthcoming with facts in the initial intake interview.

* A lawyer may have (likely has) a duty to warn the client about posting potentially damaging content, including private and confidential information, to social media during the course of litigation, as an opposing counsel is likely to search online for damaging information.

* This standard may be read to require the lawyer to monitor social media for information that may be damaging about the opposing party, potential and actual jurors, witnesses and even judges.

* Lawyers should also run conflict checks before posting materials about pending legal matters to ensure their firm does not represent a party involved in the matter.

In using social media, one must be careful not to disclose confidential client information. Attorneys have disclosed confidential client information via blog posts, Twitter posts, Facebook posts, etc. Even if the post does not refer to the client by name, the lawyer may not use information that would make clients easily identifiable. Social media services that use "geotagging" to post the geographic location of the poster (i.e. Facebook, Foursquare, Twitter) have gotten lawyers in trouble as they may add evidence that leads to the potential identification of a client or the revelation of confidential information. Such disclosures are a clear violation of NHRPC 1.6.

52697622 v1

2. Candor - Hypothetical

CANDOR TO THE TRIBUNAL:
STATEMENTS BY COUNSEL – HYPOTHETICAL

On the morning of her client's sentencing hearing, defense counsel arrives and notices that the defendant is not present. She calls the defendant on his cell phone. The defendant answers. The defendant says that he was worried that he would be sent to prison and that "he just can't do prison." Defense counsel asks the client where he is. The defendant says, "I'm sorry but I had to leave." The defendant then hangs up.

Defense counsel appears in court. The Assistant United States Attorney is also present. The defendant does not appear. The court asks defense counsel whether the defendant was aware of the date and time of the hearing. Counsel says yes, she discussed the date and time with the defendant. Advocating for her client, counsel then adds that the defendant appeared for a prior hearing in this case, that the defendant has no history of failing to appear for other court dates, and that the defendant has no prior criminal record. Those statements are all true.

The judge remarks that under the circumstances it is possible that there is an innocent explanation for the failure to appear. The judge states that, as long as there is no objection, the hearing will be rescheduled to the following week. The prosecutor says he has no objection.

Has defense counsel violated Rule 3.3? What is defense counsel's obligation? Note that the court did not ask her a direct question about what she knew about why her client had failed to appear.

CANDOR TO THE TRIBUNAL:
STATEMENTS BY COUNSEL - MATERIALS

"The confidence of judges to rely with certainty upon the word of attorneys forms the very bedrock of our judicial system. . . . The privilege of practicing law does not come without the concomitant responsibilities of truth, candor and honesty. Lawyering involves a public trust and requires an unswerving allegiance to honesty and integrity."[1]

THE STANDARDS FOR PROFESSIONAL CONDUCT ARE THE NEW HAMPSHIRE RULES OF PROFESSIONAL CONDUCT

Local Rules 83.1 and 83.5

Rule 83.1: Any active member in good standing of the bar of the Supreme Court of New Hampshire is eligible for admission to the bar of this court.

Rule 83.5: The Standards for Professional Conduct adopted by this court are the Rules of Professional Conduct as adopted by the New Hampshire Supreme Court, as the same may from time to time be amended by that court, and any standards of conduct set forth in these rules. Attorneys who are admitted or permitted to practice before this court shall comply with the Standards for Professional Conduct, and the court expects attorneys to be thoroughly familiar with such standards before appearing in any matter. Attorneys prosecuting criminal cases are also held to the standards of conduct established by law for prosecutors.

THE IMPORTANCE THE NEW HAMPSHIRE SUPREME COURT PLACES ON CANDOR

Under New Hampshire RSA 311:6, every attorney admitted to practice in New Hampshire has answered "yes" when asked to give the following oath:

> You solemnly swear or affirm that <u>you will do no falsehood, nor consent that any be done in the court, and if you know of any, that you will give knowledge thereof to the justices of the court, or some of them, that it may be reformed</u>; that you will not wittingly or willingly promote, sue or procure to be sued any false or unlawful suit, nor consent to the same; that you will delay no person for lucre or malice, and will act in the office of an attorney within the court according to the best of your learning and discretion, and with all good fidelity as well to the court as to your client. <u>So help you God or under the pains and penalty of perjury</u>.

(Emphasis added.) The oath is not just a formality. The New Hampshire Supreme Court has stated, when quoting the oath, that "no single transgression reflects more negatively

[1] *In re Morse*, 160 N.H. 538, 548-49 (2010)(quotations and citations omitted).

on the legal profession than a lie." *Nardi's Case*, 142 N.H. 603, 606 (1998). The court has also stressed its longstanding recognition of the duty of candor.

> We have long recognized that a license to practice law imposes upon a practitioner certain moral obligations. In 1890, Chief Justice Charles Doe observed that attorneys are a class of individuals "to whose diligence, integrity, ability, and honor much is necessarily confided" and, therefore, whose "honesty, probity, and good demeanor" is ensured by oath. *Ricker's Petition*, 66 N.H. 207, 237, 240, 29 A. 559 (1890). He further commented that it is, therefore, an attorney's duty to avoid "any ill practice attended with fraud or corruption, and committed against the obvious rules of justice and honesty." Id. at 212, 29 A. 559.

In re Kalil's Case, 146 N.H. 466, 467, 773 A.2d 647, 648 (2001); *see also In re Morse*, 160 N.H. 538, 548-49 (2010)(quoted above).

<u>RULES REGARDING ATTORNEY CANDOR TO THE TRIBUNAL</u>

The attorney's duty of candor to the court is set forth in N.H.R. Prof. Conduct 3.3, specifically in part 3.3(a)(1). For ease of reference, the entire rule is set forth below:

> (a) A lawyer shall not knowingly:
>
> (1) <u>make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer</u>;
>
> (2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or
>
> (3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and comes to know if its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.
>
> (b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.
>
> (c) In an *ex parte* proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

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

(Emphasis added.).

This rule contains the same language as the ABA Model Rule[2]. For that reason and because the New Hampshire Supreme Court has looked to the Model Rules for guidance, the comments to the Model Rules are included in the discussion below.

Knowledge of Falsity

Rule 3.3 is applied most strictly when the lawyer personally makes a statement to the court. Comment 3 to ABA Model Rule 3.3 states that: "[A]n assertion purporting to be on the lawyer's own knowledge, as in an affidavit by the lawyer or in a statement in open court, may properly be made only when the lawyer knows the assertion is true or believes it to be true on the basis of a reasonably diligent inquiry." (Emphasis added.). This duty of "reasonably diligent inquiry" requires that a lawyer "inform himself of the facts of his client's case and only press non-frivolous claims." *Mortgage Specialists, Inc. v. New Hampshire Banking Dep't*, 13-CV-00156-JL, 2013 WL 1953536 (D.N.H. May 10, 2013).

A lawyer may have "knowledge" of falsity in violation of the rule even if the lawyer does not have a specific intent to deceive. *See Carpenito's Case*, 139 N.H. 168, 173 (1994)(distinguishing a failure to correct a misrepresentation [as under Rule 3.3 or 4.1] from conduct involving dishonesty, fraud, deceit, or misrepresentation under Rule 8.4(c). Furthermore, under N.H.R. Prof. Conduct 1.0(f), a lawyer's knowledge of falsity may be "inferred from circumstances." *In re Young*, 154 N.H. 359, 366-67 (2007) (finding that awareness of circumstances establishing falsity constituted knowledge of falsity).

Note that a lawyer's knowledge of the truth of his or her own statements to the court is treated separately, in 3.3(a)(1), from the lawyer's knowledge of the falsity of the statements of a witness or the client. Most importantly, the lawyer's knowledge of the falsity of a criminal defendant's testimony is treated differently because of the constitutional rights implicated. In recognition of the presumption of innocence and a criminal defendant's constitutional right to testify, courts have set a high standard for when a criminal defense lawyer is charged with knowing that his or her client is making a false statement. *See generally State v. Chambers*, 296 Conn. 397, 416, n. 13 (Conn. 2010); *Commonwealth v. Mitchell*, 438 Mass. 535, 545-46, 781 N.E.2d 1237, cert. denied, 539 U.S. 907, 123 S. Ct. 2253, 156 L. Ed. 2d 118 (2003); *People v. Calhoun*, 815 N.E. 2d 492, 502 (4th Dist., Ill. 2004) (describing five different tests used by state and federal courts). Nonetheless, counsel must bear in mind that a criminal defendant has no constitutional right to commit perjury and, if counsel truly has knowledge of the falsity, as defined by the case law, then Rule 3.3 is not limited by the criminal defendant's

[2] The New Hampshire rule changes the order of (c) and (d) but the language in the two rules is the same.

constitutional rights. *Nix v. Whiteside*, 475 U.S. 157, 166 (1985). More to the point here, a lawyer should distinguish the leeway given regarding the lawyer's assessment of the veracity of a criminal defendant's testimony from the duty of candor regarding the lawyer's own statements to the court.

The Obligation to Take Remedial Measures

When counsel makes a statement he or she believes to be true, only to discover later that the statement was not true, the lawyer must act to correct the misstatement. The lawyer has a duty, under 3.3(a)(1) to correct false statements of material fact or law, if the discovery of falsity is made prior to the conclusion of the proceeding, as stated by 3.3(d).[3]

Materiality and Confidentiality

When a lawyer is addressing the court, the obligation of candor is not limited to statements of "material" fact. Rule 3.3(a)(1), provides that a lawyer shall not knowingly "make a false statement of fact or law to a tribunal . . . ," and that a lawyer shall not knowingly "fail to correct a false statement of <u>material</u> fact . . . ." (Emphasis added.) Thus, materiality becomes an issue when the lawyer later learns that a statement he made to the court was false, although he did not know it at the time. In the first instance, however, a lawyer's duty of candor applies to every statement, not just those which deal with "material" facts. *See, e.g.*, *In re Clark's Case*, 163 N.H. 184, 190 (2012)(Where a lawyer argued that his false statements in a bankruptcy pleading would not have been considered by the court, the New Hampshire Supreme Court stated, "Whether and how the court could consider [the false statements] has no bearing on whether the respondent knowingly made a false statement of fact to the court."). Similarly, a lawyer may not argue that the opposing party was not prejudiced by the false statement. *See Feld's Case*, 149 N.H. 19, 24 (2002)("We have never held that lack of prejudice to an opposing party is a defense to a violation involving deceit upon the court or an opposing party.")

Nor is there any limitation regarding confidentiality. Rather, Rule 3.3(d) expressly states that the duty of candor trumps any limitations which might otherwise arise from the duty of confidentiality under N.H. Rule of Prof. Conduct 1.6: "The duties stated in paragraphs (a) and (b) . . . apply even if compliance requires disclosure of information otherwise protected by Rule 1.6."

Omissions

Rule 3.3(a)(1) provides: "A lawyer shall not knowingly . . . make a false statement of fact or law to a tribunal," but does not expressly address a lawyer's knowing failure to disclose facts where the omission might mislead the court. For example, counsel might make a statement which is true, standing alone, but is nevertheless misleading because counsel has omitted relevant facts. The question is

[3] The N.H. Bar Ethics Committee has provided some guidance regarding the related problem of correcting a false statement by a client or witness. N.H. Bar Ethics Committee Advisory Opinion # 2008-09/3, "Remedial Measures Under Rule 3.3."

whether the knowing omission in such circumstances is, in effect, a false statement in violation of the rule.

One could argue that knowing omissions of fact do not violate Rule 3.3(a)(1) because when the New Hampshire Supreme Court has wanted to bar such conduct, it expressly did so. For example, in Rule 4.1, regarding fairness to third parties, the court provided that lawyers may not "fail to disclose a material fact to a third person" in certain situations. Similarly, in part (a)(2) of 3.3, the court addressed a failure to disclose controlling legal authority. Thus, the argument is that the New Hampshire Supreme Court is aware of the difference between an affirmatively false statement as opposed to a failure to disclose or a misleading omission. If the court had also intended in Rule 3.3(a)(1) to require attorneys to disclose facts to avoid misleading a court, it would have used the "failure to disclose" language in that part of the rule.

I do not believe this argument would prevail. Admittedly, the case law could be more developed on this point. Nevertheless, it appears very likely that the New Hampshire Supreme Court will hold that knowing omissions which may mislead a court do fall within the scope of Rule 3.3(a)(1). There are three reasons to believe this.

First, in dealing with the prior version of Rule 3.3, which also prohibited knowing false statements to a tribunal, the New Hampshire Supreme Court twice referred to omissions, in both instances apparently regarding the rule as applicable. In *In re Bruzga's Case*, 145 N.H. 62, 69-70 (2000), the court stated the lawyer violated 3.3 when he "knowingly exaggerated facts and omitted material detail regarding the events underlying his allegations to a point of perverting the truth." In a later case, *In re Wolterbeek*, 152 N.H. 710, 716 (2005), the parties stipulated to a violation of 3.3(a)(1) which the court described as a failure "to disclose material facts and provide complete answers to questions" in a bankruptcy petition. Thus, while the issue here was not expressly addressed, the court clearly assumed that omissions were within the scope of the rule.

Second, the ABA Model Rule comments to Rule 3.3 provide the following guidance: ". . . There are circumstances where failure to make a disclosure is the equivalent of an affirmative misrepresentation. . . ." N.H. Rule Prof. Conduct, 3.3, ABA Model Rule cmt. 3. This commentary is important because there is precedent that indicates the court will borrow from the ABA comments to construe candor rules broadly. In *Carpenito's Case*, the Court held that an attorney violated Rule 4.1 by failing to correct a statement that he believed to be true at the time he made it but subsequently learned was not true. 139 N.H. at 174-74. Notably, Rule 4.1 does not contain a requirement that a lawyer subsequently correct the record — as is contained in Rule 3.3. The Court in *Carpenito's Case* made short shrift of the plain language, narrow construction, argument, noting that: "Although the text of each rule is authoritative, the comments are intended as guides to interpretation." *Id*. at 173. Although Rule 4.1 did not contain any language suggesting there is a duty to correct the record, the Court found such a duty in the ABA Model Code Comments to the rule. *Id*. at 174.

Finally, as noted above, the New Hampshire Supreme Court has repeatedly emphasized the great importance it places on lawyers' obligations of candor. For this reason, there is very little chance of the court adopting a narrow reading of 3.3(a)(1) to allow a lawyer to make superficially true statements while knowingly omitting relevant facts such that tribunal is left with a false impression.

In short, although Rule 3.3(a)(1) speaks in terms of your obligation not to make affirmative false statements, you should heed the language in the comments (both New Hampshire and ABA) that broaden the scope of Rule 3.3(a)(1), and operate on the assumption that your omissions of fact may also give rise to a "false statement" as contemplated by the rule.