

What Does Ethical Competence Mean in the Digital Era?



February 28, 2016

University of Richmond School of Law

Presenters: Sharon D. Nelson, Esq. and John W. Simek
President and Vice President, Sensei Enterprises, Inc.

703-359-0700 www.senseient.com

snelson@senseient.com; jsimek@senseient.com

Note to Virginia Lawyers: The Virginia Supreme Court has amended Rule 1.1 (Competence) and Rule 1.6 (Confidentiality), effective March 1, 2016. The new rules may be found at the end of these written materials.

Why Do Lawyers Resist Ethical Rules Requiring Competence with Technology? Practical Tips to Shore Up Your Data Security!

By Sharon D. Nelson, Esq. and John W. Simek

© 2015 Sensei Enterprises, Inc.

Recently, the Virginia State Bar Council voted to adopt changes to the Model Rules of Professional Conduct. The changes were based on the American Bar Association's modifications to the Comments of Rule 1.1 respecting Competence ("...a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with technology...**") and Rule 1.6 respecting Confidentiality ("(c) A lawyer shall make **reasonable efforts** to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client.")

What's reasonable? The Comments go on to list relevant factors:

1. the sensitivity of the information
2. the likelihood of disclosure if additional safeguards are not employed
3. the cost of employing additional safeguards
4. the difficulty of implementing the safeguards
5. adverse effect on the lawyer's ability to represent clients

The Comments also make it clear that the client can demand more security or, with informed consent, accept lesser measures. This was not adopted by the VSB Council, but many states have adopted it.

As to the remainder of the changes, which were adopted and have been sent to the Supreme Court of Virginia for its blessing before becoming final, there was quite a firestorm prior to the final vote adopting the proposed rules.

Even before the Council met, there had been comments received on the proposals, saying things like “I believe it is unreasonable to expect a lawyer to become an IT professional in addition to all of our other responsibilities.” This was echoed at the Council meeting.

This is a misunderstanding of the requirement. The change does not require a lawyer to become an IT professional – indeed, for most lawyers, dabbling in IT would be dangerous. They need outside or inside IT help in most cases – the small firms generally contract IT work to an outside IT service company. But all lawyers should be aware of the benefits and risks of technology to be a competent lawyer in the digital era. Hence, the change to Rule 1.1 makes good sense.

Another comment made the point that technology is the only form of competence specifically referenced in the proposed rule.

We are all accustomed to taking CLE each year to maintain our competence as attorneys in the fields of law in which we practice. However, it is uncontroverted that the most disruptive force we have ever seen in the practice of law is technology. It is pervasive – and becomes more so with each successive generation of lawyers. We have reached the point in time where a lawyer cannot effectively practice law without technology – which makes it an imperative that lawyers know something about the technology they use.

We live in a “breach-a-day” world which suggests even more strongly that we need to pay attention to sensitive client data. According to a 2013 Mandiant Threat Report, law firms and consultants constitute 7% of the targets of advanced attackers. This has come to mean that we are the easy route to getting the data of our clients. Cybercriminals and state-sponsored hackers alike have attacked law firms, large and small – and they are all too often successful because employees are not trained in safe computing, security patches and updates are not installed, out-of-support software (receiving no security updates) continues to be used, and they do not employ encryption.

All of this can be addressed by a competent IT professional. Are there costs? Yes, certainly, but they are a matter of scale. The costs will be far greater for a large firm than for a solo or small firm practitioner. The measurement of “acting reasonably” is obviously different depending on the size of the firm.

In spite of all the rhetoric about “small firms can’t afford this requirement” the truth is that many reasonable precautions cost nothing. Installing security patches is free – yet it is frequently not done. It costs nothing to encrypt a Word or PDF attachment with a password before sending it. Encryption is already a built-in feature of modern computers and smartphones – it may need to be enabled, but it is there.

You can encrypt e-mail easily these days with inexpensive products like ZixCorp, to name just one. A lawyer doesn’t need to understand the mathematics of encryption – only how to use the products. And they are fast and easy to learn. You don’t need to use encryption all the time, but when you are sending sensitive data, you probably should. You know what you have to learn? How to hit the “Encrypt and Send” button. That’s it.

Using the cloud to hold data is fine, so long as you understand the security precautions. Chiefly, if you encrypt the data before sending it to the cloud, your data is safe because only you hold the decryption key. Holding the encryption key yourself means the cloud provider has “zero knowledge” of the decryption key – and that’s the kind of cloud provider you want. There is no additional cost to this – you just have pick the right provider. As an example, SpiderOak is a “zero knowledge” file synching cloud whereas Dropbox holds a master decryption key and will, if given the proper paperwork, turn over your data to the authorities. We like SpiderOak and others that are moving in the “zero knowledge” direction, a far better solution for lawyers.

There is no cost to forbidding employees by policy from connecting to the law firm network with personal devices. Who knows what malware may exist on those devices? Large firms may choose to use sophisticated techniques to manage personal devices, but smaller firms are better off simply forbidding them to connect to the network.

There is a long list of free or reasonably priced safeguards for data, but that's why attorneys should go to CLEs – to learn them and see that they are implemented by their IT provider. How about making sure lawyers use strong passwords (and not same password everywhere) and change them (especially their network credentials) regularly?

The changes to the Model Rules require only reasonable safeguards and give a host of factors to be considered in determining what is reasonable. In some cases, where lawyers hold HIPAA data or data containing personally identifiable information, they may be governed by state or federal law beyond the scope of the proposed rules, which is noted in the new comments to Rule 1.6.

So why all the hoo-ha at the Council meeting? Largely, we believe that there are fundamental misunderstandings about the changes and what they mean. There is also a mentality – so common in the legal profession – that “we’ve always done it this way.” One person actually said that lawyers shouldn’t be required to do more to protect data in the digital world than they were in the paper world? Say what? It defies belief that this sentiment has such a strong hold on so many lawyers, but it does. Perhaps the speaker didn’t realize that over 93% of documents are created electronically and that more than 50% of them are never printed.

One young lawyer took the microphone to point out that the digital world is a new one – and requires us to adapt. We might add “or face extinction.” By the way, as of the time this article was written, 16 states had adopted the ABA rules, some (like Virginia) with minor variations.

Taken as a whole, what we cannot do is turn a blind eye to the impact of technology on our profession. There was a time when protecting client data involved locked file cabinets in a locked office. Today, we must still “lock” the data – digitally. The new modifications to Rule 1.1 and 1.6 are a measured and technology-agnostic step toward applying old rules to the 21st century.

Here are some practical questions to ask: If you find your answers aren’t measuring up, then you need to meet with your IT provider – or cybersecurity consultant - and shore up your firm security:

- Do you have written security policies and have they been reviewed and signed by all employees?
- Do you have onboarding/out-processing documents/checklists for hiring and terminating employees?
- Do you have a disaster recovery plan?
- Do you have a computer software and hardware asset inventory list and network diagram?
- Are there industry standards for which your firm must be compliant, such as PCI, HIPAA, HITECH or Sarbanes-Oxley?
- Do you have a list of third-party vendors that your business is using, including infrastructure access and contact information?
- Do your employees receive annual training on information security and safe computing practices?
- Do you have a Bring Your Own Device (BYOD) policy?
- Do you have a Bring Your Own Network (BYON) policy?
- Do you have an Incident Response Plan in the event of a data breach or a disaster?
- Are your systems protected by enterprise grade security software?
- Is the security software up-to-date, license current, and actively scanning on a regular basis?
- Are all of the Windows-based firewalls enabled?
- Is your e-mail being filtered to protect users from spam, viruses and phishing attempts?

- Is a password policy in place requiring strong, 14-character or longer passwords? Are passwords, especially network log-in passwords, required to be changed every 30 days? Is password reuse prohibited via technology for 12 months or longer?
- Are computer systems up-to-date with security patches?
- Is software being updated on a regular basis and with updates from the manufacturer?
- Have you upgraded all software that is no longer supported?
- Is your data getting backed up on a regular basis? Are you performing test restorations of backups?
- Is your backup engineered so that it cannot be encrypted by ransomware?
- Is data on mobile devices encrypted (smartphones, laptops, tablets)?
- Do you require passphrases/PINs on mobile devices that connect to your network?
- Are your mobile devices protected with security software?
- Is your wireless network using WPA2 encryption?
- Do you have a guest wireless network so you can restrict access to your business data?
- Have the default usernames and passwords for your computers, equipment and software been changed?
- Are your computers running Microsoft Windows 7 or newer, servers Microsoft Server 2008 or newer?

- Do you have a redundant/backup Internet connection, in the event your business loses connectivity?
- Can you remotely wipe data from mobile devices if they are lost or stolen?

For most of you, we're guessing it's time to roll up your sleeves and get to work!

*The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA.
703-359-0700 (phone) www.senseient.com*

VIRGINIA:

In the Supreme Court of Virginia held at the Supreme Court Building in the City of Richmond on Thursday the 17th day of December, 2015.

On March 16, 2015 came the Virginia State Bar, by Kevin E. Martingayle, its President, and Karen A. Gould, its Executive Director and Chief Operating Officer, and presented to the Court a petition, approved by the Council of the Virginia State Bar, praying that Section II, of the Rules of Integration of the Virginia State Bar, Part Six of the Rules of Court, be amended to read as follows:

Amend the Comments to Part Six, Section II, Rule 1.1 to read as follows:

Rule 1.1. Competence.

*

*

*

COMMENT

*

*

*

Maintaining Competence

[6] To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education in the areas of practice in which the lawyer is engaged. Attention should be paid to the benefits and risks associated with relevant technology. The Mandatory Continuing Legal Education requirements of the Rules of the Supreme Court of Virginia set the minimum standard for continuing study and education which a lawyer licensed and practicing in Virginia must satisfy. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances.

*

*

*

Amend Part Six, Section II, Rule 1.6 to read as follows:

Rule 1.6. Confidentiality of Information.

* * *

(d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information protected under this Rule.

COMMENT

* * *

Former Client

[18] The duty of confidentiality continues after the client-lawyer relationship has terminated.

Acting Reasonably to Preserve Confidentiality

[19] Paragraph (d) requires a lawyer to act reasonably to safeguard information protected under this Rule against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of this Rule if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the employment or engagement of persons competent with technology, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of

software excessively difficult to use).

19[a] Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other laws, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of this Rule.

[20] Paragraph (d) makes clear that a lawyer is not subject to discipline under this Rule if the lawyer has made reasonable efforts to protect electronic data, even if there is a data breach, cyber-attack or other incident resulting in the loss, destruction, misdelivery or theft of confidential client information. Perfect online security and data protection is not attainable. Even large businesses and government organizations with sophisticated data security systems have suffered data breaches. Nevertheless, security and data breaches have become so prevalent that some security measures must be reasonably expected of all businesses, including lawyers and law firms. Lawyers have an ethical obligation to implement reasonable information security practices to protect the confidentiality of client data. What is "reasonable" will be determined in part by the size of the firm. *See* Rules 5.1(a)-(b) and 5.3(a)-(b). The sheer amount of personal, medical and financial information of clients kept by lawyers and law firms requires reasonable care in the communication and storage of such information. A lawyer or law firm complies with paragraph (d) if they have acted reasonably to safeguard client information by employing appropriate data protection measures for any devices used to communicate or store client confidential information.

To comply with this Rule, a lawyer does not need to have all the required technology competencies. The lawyer can and more likely must turn to the expertise of staff or an outside technology professional. Because threats and technology both change, lawyers should periodically review both and enhance their security as needed; steps that are reasonable measures when adopted may become outdated as well.

[21] Because of evolving technology, and associated evolving risks, law firms should keep abreast on an ongoing basis of reasonable methods for protecting client confidential information, addressing such practices as:

- (a) Periodic staff security training and evaluation programs, including precautions and procedures regarding data security;

(b) Policies to address departing employee's future access to confidential firm data and return of electronically stored confidential data;

(c) Procedures addressing security measures for access of third parties to stored information;

(d) Procedures for both the backup and storage of firm data and steps to securely erase or wipe electronic data from computing devices before they are transferred, sold, or reused;

(e) The use of strong passwords or other authentication measures to log on to their network, and the security of password and authentication measures; and

(f) The use of hardware and/or software measures to prevent, detect and respond to malicious software and activity.

Virginia Code Comparison

Rule 1.6 retains the two-part definition of information subject to the lawyer's ethical duty of confidentiality. EC 4-4 added that the duty differed from the evidentiary privilege in that it existed "without regard to the nature or source of information or the fact that others share the knowledge." However, the definition of "client information" as set forth in the ABA Model Rules, which includes all information "relating to" the representation, was rejected as too broad.

Paragraph (a) permits a lawyer to disclose information where impliedly authorized to do so in order to carry out the representation. Under DR 4-101(B) and (C), a lawyer was not permitted to reveal "confidences" unless the client first consented after disclosure.

Paragraph (b)(1) is substantially the same as DR 4-101(C)(2).

Paragraph (b)(2) is substantially similar to DR 4-101(C)(4) which authorized disclosure by a lawyer of "[c]onfidences or secrets necessary to establish the reasonableness of his fee or to defend himself or his employees or associates against an accusation of wrongful conduct."

Paragraph (b)(3) is substantially the same as DR 4-101(C)(3).

Paragraph (b)(4) had no counterpart in the Virginia Code.

Paragraphs (c)(1) and (c)(2) are substantially the same as DR 4-101(D).

Paragraph (c)(3) had no counterpart in the Virginia Code.

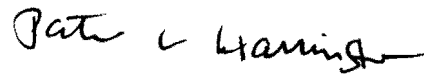
Committee Commentary

The Committee added language to this Rule from DR 4-101 to make the disclosure provisions more consistent with current Virginia policy. The Committee specifically concluded that the provisions of DR 4-101(D) of the Virginia Code, which required broader disclosure than the ABA Model Rule even permitted, should be added as paragraph (c). Additionally, to promote the integrity of the legal profession, the Committee adopted new language as paragraph (c)(3) setting forth the circumstances under which a lawyer must report the misconduct of another lawyer when such a report may require disclosure of privileged information.

Upon consideration whereof, it is ordered that the Rules for Integration of the Virginia State Bar, Part Six of the Rules of Court, be and the same hereby are amended in accordance with the prayer of the petition aforesaid, effective March 1, 2016.

A Copy,

Teste:

A handwritten signature in black ink, appearing to read "Patricia C. Hanning", with a stylized flourish at the end.

Clerk