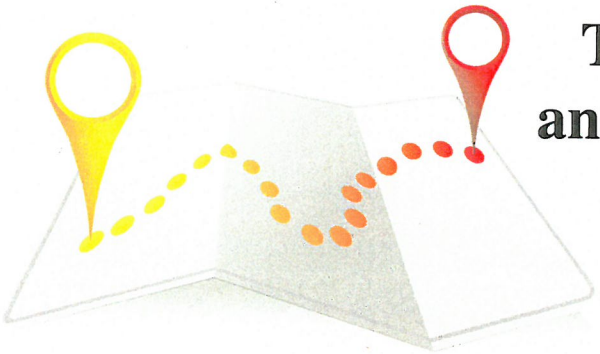
Professionalism as a Moving Target:

The Blurry Line Between "Best" and "Required" Practices, Part II



By Tom C. Vincent II

In the first part of this article we considered the changing pursuit of "professionalism" – i.e., adopting practices "above and beyond the minimum" – in light of higher and higher standards required as that "minimum." These higher and higher standards are particularly evident with respect to client confidentiality, where the ever-increasing ways to collect, store, and communicate can result in correspondingly numerous ways that the confidentiality of that information can be violated. As discussed in Part I, recent guidance with respect to confidentiality regarding client information was provided by the American Bar Association in its Formal Opinion 477R (the "**Opinion**"). While in some instances such guidance may be considered "above and beyond," it serves to remind attorneys of the minimums that may be implicated – and required – with particular types of client information.

As provided in Part I, The Opinion outlines seven considerations for lawyers when communicating (and storing) electronic client information:

1) Understand the Nature of the Threat;
2) Understand How Client Confidential Information is Transmitted and Where It Is Stored;
3) Understand and Use Reasonable Electronic Security Measures;
4) Determine How Electronic Communications About Clients Matters Should Be Protected;
5) Label Client Confidential Information;
6) Train Lawyers and Nonlawyer Assistants in Technology and Information Security;and
7) Conduct Due Diligence on Vendors Providing Communications Technology.

While each of the considerations is generally discrete, they do have common elements that can and should be both understood and implemented together (as described below).

Understanding

All of the considerations speak to what an attorney and their staff need to **know** about cybersecurity before **doing** anything. Put another way, an attorney should understand three important issues **before** anything happens – their process, their risks, and their controls – and make sure that others in the firm or company understand them as well:

a) **Process** refers to the lifecycle of confidential information in the firm: i) how it's identified as confidential, ii) how it enters and exits the firm, and iii) where it stays while it's in there. This also includes who has access to the information – internally and externally - and how they protect it.

b) The **Risks** to information include not only how it may be exposed by third parties – for example, vendors – but how third parties may work to get the attorney or staff to expose it for them.

c) Finally, to address those risks the firm should have particular **Controls** in place that are designed to prevent, detect, or mitigate the effects of those risks. These include firm policies, limitations on access, encryption requirements for sensitive information, and required clauses in vendor agreements.

Because of the interplay of these three elements, it is difficult to fully understand one without having a similar understanding of the others. For example, if the attorney is unaware that part of the firm's process

involves client exchange of information with assistants via e-mail, she may not realize that a significant risk to that process is a Spearphishing or spoofing[1] attack designed to elicit client information from that assistant. Similarly, without an understanding of how information may be communicated/stored, any electronic security measures identified may not be fully responsive to those risks. [2]

Beyond those elements listed above, it's also important for the attorney and staff to understand the specific **type** of information communicated and/or stored, as that will inform and direct **all** of these considerations. If the information falls into the category of "protected health information[3]," then the determination of "reasonable electronic security measures" may include an analysis of the firm's safeguards for such information as required under the Health Insurance Portability and Accountability Act ("**HIPAA**") and the Health Information Technology for Economic and Clinical Health Act ("**HITECH**")[4]. Similarly, if the firm is communicating and/or storing information that falls into the category of personal information covered by one or more state statutes, then those measures may need to include other proactive measures.[5]

Implementing

After the processes and risks are identified by the firm, and the necessary controls determined, those controls should be implemented, and not just "on paper" – not only to prevent the identified risks from resulting in breaches of client confidentiality, but also to reduce the risk of financial penalties resulting from the breach.[6] Everyone at the firm who may have access to confidential information – and certainly everyone who has e-mail – should understand these controls and be regularly reminded of their responsibilities. As technology changes, processes may change as well – controls should similarly be updated to reflect both the new processes and the resulting risks.

Just as with professionalism generally, maintaining client confidentiality is less a destination than a journey. – not a single accomplishment but a continuous effort. While the primary focus may be on **surpassing** client expectations, simply **meeting** legal and regulatory requirements must be a consideration as well.

---

1 Spearphishing typically refers to an e-mail request sent to an individual, using information particular to that individual, designed to create a false sense of authority or familiarity resulting in the fulfillment of the request (which is often for information or fuds which should not be provided). Spoofing refers to the use of a website or e-mail address that is similar to an expected website/address often with the same objective as Spearphishing.

2 Note that, in addition to the tactics listed, certain e-mail providers may collect data from information on their systems – attorneys should review the terms of use for their provider(s) to determine if such collection is performed and what obligations may result.

3 See 45 CFR 1690.103 for a full definition.

4 Should the firm utilize protected health information in its representation of a client, it may be considered a "business associate" under HIPAA – if so, the firm will be required to identify and implement appropriate administrative, physical, and technical safeguards for that information.

5 See e.g. 201 CMR 17.04 (requirements for a computer system that electronically stores or transmits information about a Massachusetts resident).

6 For example, in 2016 a business associate which failed to conduct an assessment of the risks to protected health information in its possession, and to implement corresponding security measures, was fined $650,000.00 by the Department of Health and Human Services.

Tom C. Vincent II is an attorney with Gable Gotwals