ALPS Practice Management Pointers

Maintaining Confidentiality Should Never Be an Afterthought

Mark Bassingthwaighte, Esq.
Risk Manager

How much time do you really spend thinking about your ethical obligation to maintain client confidences? I suspect not much. We all understand that what we learn at the office is to stay at the office. That's a good start, mind you, but is this understanding enough? How far does it really go? I believe it goes further than most of us realize because maintaining client confidences is about more than just keeping our mouths shut.

Allow me to share an example to demonstrate the point. In office share settings or executive office space it isn't uncommon to find that files are left lying about, office doors left open, file cabinets left unlocked, and even computers left on overnight. Sometimes this is reportedly due to the necessity of allowing janitorial staff access so that the space may be cleaned. When asked about confidentiality concerns in these settings, I often am told that I needn't worry because no one on the cleaning staff speaks English. I don't know about you, but that response makes me nervous. After hearing that kind of response, I would so love to take a look at any computer in that firm that was left on overnight. Call me a pessimist if you must, but I don't buy that the computers are never touched or file drawers never opened. Years ago I managed a cleaning service/skills training program and I can assure you that what can go on in your office after hours would be upsetting to many.

We need to get past thinking about our confidentiality rule as just requiring that we keep secrets by keeping quiet. With this in mind, I thought I would share some additional thoughts you might want to keep in mind.

At a minimum all tech must be password protected. This is particularly import with jump drives, external hard drives, smart phones, and tablets as these items can be easily lost and sometimes are stolen. Laptop and smartphone theft is rampant and such thefts do not occur just at the airport. You would be surprised at how many disappear from offices. Don't make it easy. What would you do if you learned that information about a client has been posted on Facebook; then

upon further inquiry discovered that several days prior an attorney at the firm lost his iPhone and the posted material was on that device. Ouch.

If anyone at the firm wishes to access the firm's network using a wireless connection, this should always occur via an encrypted session. Here is how I feel about it. If you or anyone on your staff has no idea how to tell if the signal that you or they are about to connect to is from a trusted source versus a viral peer-to-peer network, then neither of you has any business using wireless for work-related purposes. If you wish to risk your own identity, that's your own choice. Client confidences are another matter. Further, I don't care if it is a free WiFi hotspot at your favorite local coffee shop or your own home router for that matter. Just because it's convenient doesn't mean it's safe. In simple terms, always use a VPN (Virtual Private Network) connection when working over a wireless connection. Always!

Yes, just about everything in the cellular service world is now digital, which we all equate with being secure. That's a positive development; but so what. What I don't understand is why so many continue to walk around with Bluetooth headsets always on and/or having private conversations in public places. Making matters worse, I continue to laugh at those folks who seem to believe that because the mike is back by their ear they must speak QUITE LOUDLY in order to be heard. I must have missed this in science class; but apparently sound doesn't travel around the side of one's head very well. Again, Bluetooth's convenience doesn't make it secure. To me, that blinking blue light says "victim here." When not in use, turn the Bluetooth functionality off, and for goodness sake, stop talking at full voice and find a private place to make all work-related calls. The guy sitting next to you at Starbucks doesn't want to be forced to hear all about your client's problems.

This list could go on and on, but hopefully you begin to get the point. As attorneys, we have an affirmative duty to preserve and maintain client confidences and this duty requires more of us than simply keeping quite when outside the office. Lock doors and/or file cabinets. Put files away and log off computers if a cleaning service or others will have access to the space after hours. Properly secure closed file storage areas; password protect all tech (and you might also consider encrypting those drives); and take steps to make certain that conversations are not able to be overheard by others, even those clients sitting in a conference room that happens to be next to your office. These things are not something that can be an afterthought. A client, whose information ultimately finds its way to the Internet, isn't going to be pacified with a statement along the lines of "We didn't anticipate that this kind of thing would ever happen and we'll make certain that from here on out it won't happen again." From their perspective, it should never have happened in the first place and I couldn't agree more. If that client were me, I'd be looking for a new attorney who gets how to maintain client confidences with tech post haste and when I do, trust me, she'll be in touch.

ALPS Risk Manager Mark Bassingthwaighte, Esq. has conducted over 1,000 law firm risk management assessment visits, presented numerous continuing legal education seminars throughout the United States, and written extensively on risk management and technology. Check out Mark's recent seminars to assist you with your solo practice by visiting our on-demand CLE library at alps.inreachce.com. Mark can be contacted at: mbass@alpsnet.com.

Disclaimer: