Guidance to Address Cybersecurity and Data Privacy Concerns When Providing Remote Legal Services

With the current concerns regarding the spread and impact of COVID-19 (“Coronavirus”), many lawyers and law firms are moving to remote working environments. As attorneys, law firms have heightened requirements to maintain secure and private work environments, whether those be physical or virtual environments. This document is intended to provide some guidance for the transition to providing legal services on a remote basis. This document is not exhaustive. As in other contexts, lawyers should employ sound discretion and judgment in the delivery of legal services.

For general cyber and privacy concerns, the American Bar Association adopted two formal opinions that provide guidance to create and maintain secure infrastructures. ABA Formal Opinion 477R, based on the Duties of Competence (ABA Model Rule 1.1) and Confidentiality (ABA Model Rule 1.6), reiterates the affirmative duty to take reasonable measures to ensure that electronic communications with clients remain secure and confidential. ABA Formal Opinion 483, also based on Duties of Competence, Confidentiality, and Notice (ABA Model Rule 1.4), explains duties required of a lawyer in the wake of a cyberattack.

The Pennsylvania Bar Association adopted two relevant opinions. First, Formal Opinion 2010-200 requires an attorney with a virtual law office “is under the same obligation to maintain client confidentiality as is the attorney in a traditional physical office.” Second, Formal Opinion 2011-200 expressly permits the use of cloud computing services by lawyers, but placed two specific obligations on lawyers in this context:

An attorney may ethically allow client confidential material to be stored in “the cloud” provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.
What does this mean during the current COVID-19 pandemic?

Lawyers and law firms can transition to a virtual working environment. However, the obligations of confidentiality and competence must be upheld. Lawyers should understand: (i) the technology that is being used; (ii) the threats to privacy and security that accompany the use of technology; and (iii) how to create an infrastructure that promotes efficiency and access. In addition to their own work, lawyers should consider these issues to mitigate against employee error and technological risk.

Guidelines to transition to a remote working environment

**Reviewing Your Current Network Infrastructure**

For many law firms, work from home situations have been the exception, and often limited in duration, rather than the norm. With the current outbreak, companies need to ensure that their current network infrastructure can support regular and more long-term work from home options.

If your firm has a preparedness plan, consult it. In any event, attorneys should assess:

- Does my current network infrastructure allow for remote access? (i.e., can users log in via a web-browser or a virtual desktop?)
- Do I have the appropriate hardware and devices to work remotely?
- How is confidentiality of client information ensured? This may require new software that can encrypt communications and data storage, both on devices and in the cloud.
- Do my contracts with clients and suppliers provide for security and privacy? Not all cloud environments are created equal, so attorneys need to identify and understand confidentiality concerns when working in remote platforms or in the cloud.

**Creating a work-from-home set-up**

When working from home, there are additional considerations. Employees will be working in non-controlled environments that are subject to both physical and technological risks. Some items to consider:

- **Home Wi-Fi**: Employees will be connecting to your network through a home Wi-Fi connection which can be less secure and often have numerous users. Employees should be encouraged to change default router settings and passwords before connecting to the
business’ network. One solution is to provide Virtual Private Network (VPN) access to all business software and platforms. Avoid use of public Wi-Fi spots, which can be spoofed.

● **Personal Email and Devices**: Unless you already maintain a large number of business devices, you and your employees likely will be using personal devices to work remotely. Do laptops have hard drives that are encrypted-activated? Firm IT teams should work with HR teams to ensure that appropriate “Bring Your Own Device” or BYOD controls are in place, and employees are trained (most likely remotely) on those policies. Even if your organization already maintains a BYOD policy, it should be reviewed and updated to reflect a more long-term work from home requirement. For “best practices,” avoid use of personal email accounts or storing information on the hard drives of personal devices. Such practices likely violate client security requirements and could lead to the compromise of data. Avoid use of portable media devices unless data stored on them is encrypted.

● **Physical Security**: When employees are working from home, new physical security concerns arise with family members having access to critical devices. This creates an increased risk for inadvertent loss of information. For example, there are employees who may be talking loudly on the phone while working in public places, exposing their laptop’s screen for the entire crowd inside a coffee shop to see or even leave their devices unattended. Employees should be trained on best practices for ensuring both devices and paper documentation.

All of this information should be articulated within a Work-From-Home Policy that expressly outlines requirements and expectations, including security and privacy measures.

**Communication is Key**

When transitioning to a new work environment, it is critical that you communicate expectations clearly. This includes communicating to your clients, your employees, and any other stakeholders with whom you work.

● **Security Hygiene**: Make sure to communicate cybersecurity practices, both in written form and in training. If your employees have never worked with certain hardware or platforms, training becomes even more critical as it can help to ease the challenges with new technologies, while also ensuring that these technologies remain secure and confidential.
• **Identifying Tools for Remote Workers**: Remote working creates opportunities for “shadow IT” to become very prevalent. The teams need to discuss the needs of employees who are working remotely so that appropriate tools can be selected to address those needs. Further, you need to make sure to communicate to your employees regarding approved tools for communications and operations, such as cloud storage platforms, communication/videoconferencing tools, project management tools, etc.

• **Reporting account compromise**: You want to prepare for the worst, but hope for the best. It is completely reasonable that there may be a potential increase in cybercrimes. Reminding remote workers that they need to report any possible issue immediately is critical. Delayed reporting is a delayed response that leads to an increase in costs to any data incident. To do that, it is key to provide employees with steps to follow at the first signs of account compromise. This means training and daily communication. You cannot overcommunicate to your employees when working in a remote environment. Remind your employees, and provide detailed information on company protocols in the event of an actual or suspected system or account compromise. This should include clear guidelines to follow, such as how to report, where they should report, etc.

Prepared for the Pennsylvania Bar Association by the Co-Chairs of the PBA Cybersecurity and Data Privacy Committee:

**Jordan L. Fischer, Esq.**  
XPAN Law Group, LLC  
jfischer@xpanlawgroup.com  
267.536.9376  
www.xpanlawgroup.com

**Joshua A. Mooney**  
White and Williams LLP  
mooneyj@whiteandwilliams.com  
215.864.6345  
www.whiteandwilliams.com