Published on *The National Law Review* https://natlawreview.com

This Party is BYOD--Bring Your Own Device, Part Two

Article By:

Amy D. Cubbage

The discussion in the last post focused on reasons for allowing BYOD in the work place and some traps to watch out for, which continues below.

Another pitfall that might arise in a BYOD context pertains to the nature of the information on the device itself. In addition to proprietary information of the company, certain other information is subject to additional rules and regulations. For instance, *HIPAA requirements* would apply to any employee devices that might be used to transmit patient information or data. Be aware of the consequences of data breach, and make sure BYOD policies in a health care context appropriately reach these topics. Certain information possessed by government contractors with specific clearances could also cause significant headaches for those without a sufficiently robust BYOD policy.

What will ultimately separate the wheat from the digital chaff is the adoption of a strong BYOD policy that provides guidance to both employer and employee on both the acceptable and expected use of personal devices in and out of the workplace.

The first place to start with a BYOD policy is to clarify the role of the personal device and the rights of both employer and employee. For instance, it may be important for the employee to know that the information on their devices is discoverable when the employer becomes embroiled in a lawsuit. The employer will most likely decide to reserve some rights to monitor, access and even wipe parts of the device to protect sensitive information, if necessary. The employee should also be reasonably informed of her or his rights pertaining to her or his own device should the employer have to take measures to protect employer data on the device. Clarity in defining these rights and obligations is of crucial importance.

The next step in crafting a coherent BYOD policy is to decide on the goals of such a policy. Is it merely a cost-cutting measure? Is it just a response to an influx of personal devices? Some policies fail from being overbroad, so it's important to hone in on exactly what the goals of the employer are in bringing BYOD online. What resources will the employee have access to remotely? How should personal devices be used most effectively? Where could the business and personal use of the device dovetail and possibly create conflict? Tailor your BYOD policy to the anticipated usage of the device in furtherance of company goals.

Next, clearly delineate who pays. While BYOD is seen as a cost-cutting measure, some employees may balk at the idea of conducting company business on their own dime. Employee-reimbursement

policies will become more prevalent over time as BYOD adoptions take hold, so it’s important to clarify where each party stands financially.

Finally, a strong BYOD policy will contain provisions on what will happen with the device if the employee finds him- or herself terminated. How will sensitive company data be removed? Who oversees the process?

A strong BYOD policy in the beginning will save some strong headaches down the road as employees become more and more connected to the workplace through personal devices.

National Law Review, Volume V, Number 28