GLASER & WEINER, LLP

ATTORNEYS AT LAW

BYOD

What's Your Policy?

It started with the BlackBerry. Companies welcomed the idea that employees could maintain productivity and responsiveness even while they were away from the office. They purchased units and distributed them to employees needing to be constantly "connected". The BlackBerry enterprise server was popular with CIOs and IT departments because it gave them the ability to control the company's data and dictate and scale its IT infrastructure and information security. For several reasons, including BlackBerry's loss of market share due to its failure to keep pace with the market's innovators, and businesses' recognition that they could eliminate the cost of purchasing smartphones for their employees, more and more businesses have started adopting a "Bring Your Own Device" (BYOD) strategy. As a result, employees are increasingly using personal devices to access, store and process their employers' data and confidential information.

While the use of mobile devices may increase productivity and be crucial to the success of a business, companies who allow employees to bring their own devices lose the security, consistency, scalability and efficiency they enjoyed when they owned their hardware and controlled their data. As technology continues to proliferate throughout our society, BYOD, for better or worse, is here to stay. But companies beware - a BYOD strategy carries with it substantial risks.

On December 12, 2012, the U.S. Department of Health and Human Services (HHS) launched an initiative to offer health care providers practical tips on ways to safeguard protected health information when using mobile devices such as laptops, tablets and smartphones. These tips should be carefully considered by health care providers subject to HIPAA and, because the State of New York has its own Data Breach Notification Law, businesses in all industries. HHS advises taking the following steps to secure information on mobile devices:

- Use a password or other user authentication.
- Install and enable encryption.
- Install and activate remote wiping and/or remote disabling.
- Disable and do not install or use file sharing applications.
- Install and enable a firewall.
- Install and enable security software.
- Keep security software up to date.
- Restrict download of mobile applications.

- Maintain physical control of the device.
- Use adequate security to send or receive information over public Wi-Fi networks.
- Delete all stored information before discarding or reusing the mobile device.

Companies that have or are implementing a BYOD strategy should carefully analyze their existing policies to determine whether these sufficiently cover employees' use of their personal devices for business purposes, or establish new policies to address these issues. Further, companies that are subject to regulatory requirements, such as HIPAA, must ensure that their business associates also have appropriate policies in place.

Companies should have policies that address the following: mobile device security, password usage, encryption, data classification, acceptable use, antivirus software, wireless access, remote disabling and wiping, incident response, remote working and privacy. While having these policies in place is important, it is even more important that the company is committed to consistently monitoring and enforcing them, as well as informing, educating and training employees concerning the policies and the implications of using their own devices for work purposes. Companies with a BYOD policy should also have their employees sign a written consent that addresses some of the more sensitive issues that come along with a BYOD strategy (e.g. privacy, investigations and device and data access, responsibility for loss, damage, loss of use and remote disabling and wiping of a lost or stolen device).

BYOD has created complex questions regarding data management and information security that companies must confront. Employees using unsecured networks, downloading viruses or losing a device with confidential information or trade secrets can be devastating to a company and can also result in significant costs and/or fines when companies are required to notify people that their confidential or protected information has been compromised. As a result, these issues should be carefully considered when implementing a BYOD strategy and companies should prepare a comprehensive set of policies, procedures and agreements that will help them navigate their way through this evolving strategy with greater clarity.

DISCLAIMER: The information contained herein is provided by Glaser & Weiner, LLP for informational purposes only. These materials should not be considered as, or as a substitute for, legal advice and they are not intended to nor do they create an attorney-client relationship. Because the materials included here are general, they may not apply to your individual legal or factual circumstances. This document contains information that may be modified or rendered incorrect by future legislative or judicial developments. You should not take (or refrain from taking) any action based on the information you obtain from this document without first obtaining professional counsel. It is possible that under the laws, rules or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.