From: Mills, G. Foster
Sent: Monday, June 29, 2009 12:13 PM
To: *ALL EXCHANGE USERS
Subject: Protection of Data

This memorandum relates to new office policies with respect to the protection of confidential data. As you know, protecting such data is very important and we we ask your cooperation in ensuring the data that comes into the possession of the Law Department remains confidential. Please read this memorandum carefully.

The Law Department is in possession of a vast amount of data. The data are contained in different media types, such as paper, hard drives, CD/DVDs, flash drives, personal digital assistants (PDAs), MP3 players, cell phones, voice mail and the memory caches of copiers and fax machines. Some of this data, such as medical records and social security numbers, are protected by law. Other data, while perhaps not protected by law, should not be left around for others to see.

We have adopted a policy with respect to data protected by the Health Insurance Portability and Accountability Act (HIPAA). That policy is in the Office Manual (you can reach it by going to the Law Department's Intranet page & coming down under Useful Links to "Office Manual" or by clicking on the following link: http://lawman-iis06/intranet/Office%20Manual/standards_of_conduct.shtml). We are now adopting additional policies and procedures that will minimize the possibility of the unauthorized disclosure of data to those for whom the data is not meant.

Data can find its way into the wrong hands in many ways. Laptops can be misplaced or stolen. E-mails can be misaddressed. Flash drives, especially, seem to disappear. All these misfortunes occur from time to time. The idea is to minimize or eliminate the damage they cause.

To that end, we are beginning to implement policies to encrypt all our data. This will allow us to use the data and share it with whomever needs to have it, but also ensure that if the data goes astray, it will be unusable by anyone not entitled to have it. Some of these policies will be transparent to you. For example, the loaner laptops in Information Technology (IT) are now encrypted. They work exactly the same way the old ones worked except that if lost or stolen, no one will be able to read the records on the hard drives.

Some of these policies will require additional steps on your part. For example, we will require that data transferred to CD/DVDs be encrypted. Many of these CD/DVDs are intended to be given to our adversaries as part of e-discovery. Encryption will involve creating a password and sharing it with the recipient. This will allow the recipient to read the CD/DVD. Someone who comes into possession of the CD/DVD without the password will not be able to de-encrypt it and read the records.

IT will send out instructions on how to encrypt data on various media over the next weeks and months. Over time, as we are funded for the technology, we will be encrypting all our data, including e-mails and their attachments, the data on flash drives and the rest. In the meantime, I want to re-emphasize the importance of protecting your data and records. Don't use flash drives unless absolutely necessary. Don't make unnecessary copies of CD/DVDs. Encrypt all data that will be send to third parties on CD/DVDs and external hard drives. IT can provide appropriate information and tools for this via the Helpdesk (helpdesk@law.nyc.gov or 212-788-0406). Wherever possible, password protect portable devices. Use Citrix rather than moving files from device to device.

Lastly, with respect to paper, reread the HIPAA policies in the Office Manual. Don't leave materials at copiers and fax machines. Put documents in file folders. Don't dump sensitive documents in the trash. ALWAYS shred them instead.

Thank you.