FROM: Mark McDougle
TO: CUMC Personnel
DATE: November 29, 2012
SUBJECT: Endpoint Security Campaign

In October, CUMC experienced a breach of Protected Health Information (PHI) and Personally Identifiable Information (PII) after an unencrypted workstation was stolen from a secured office. In response, Dr. Goldman mandated that all endpoint devices be appropriately secured and encrypted. Please note that all policies below include personal devices.

We thank you in advance for your help ensuring the smooth implementation and strict enforcement of the policies outlined below.

On December 3rd, CUMC IT will launch a campaign consisting of:

- Discovery of all endpoint devices, both personal and those provided by CUMC (e.g., laptops, smart phones, tablets, mobile devices, desktop computers and workstations)
- Encryption of all endpoint devices that contain PHI or PII
- Verifying encryption through annual attestation to ensure compliance of endpoint devices
- Enhancing protection of endpoints to prevent malicious activity
- Updating pertinent policies on an ongoing basis

Policy Changes

Please review the following policies reflecting the institution?s updated security posture.

CUMC Workstation Use Policy:

- All laptops must be encrypted, regardless of whether they contain PHI or PII.
- All mobile devices must be encrypted, regardless of whether they contain PHI or PII.
- All workstations and desktops must be encrypted if they contain PHI or PII.

• All encryption will require Pre-Boot Authentication.

CUMC Information Security - Backup Devices and Media Controls Policy:

• All removable media (e.g. USB flash drives, external hard drives, backup tapes, CDs, DVDs, etc.) must be encrypted, through either software or hardware mechanisms, regardless of whether they store PHI or PII.

Sanctions Policy:

Major changes to the sanctions policy were made to assure more stringent enforcement.

• Departments will be fined for any loss of PHI or PII.
• Employees can be terminated, or appointments may not be renewed, if CUMC policies are violated.
• Examples of policy violations that can result sanctions includes: failure to encrypt PHI/PII on an endpoint device or failure to register an information system, regardless of whether it contains PHI or PII.

CUMC Email Policy:

• All email services will be consolidated into the central CUMC email; no departmental email servers will be permitted after 2013.
• All mobile devices that access central CUMC email solutions will be managed via the central mobile management platform.
• The University?s LionMail email service, offered by CUIT will not be used since it does not comply with HIPAA regulations.

Next Steps

Some of the initiatives conducted throughout this campaign are outlined below. Other initiatives may be instituted as needed.

CUMC IT User Walkup Service: Starting December 3, 2012, any

CUMC employee may visit the Hammer 2nd Floor IT Help Desk with a mobile device, such as a laptop or smartphone, to verify the security of their device and request that the device is registered and appropriately secured and encrypted. To ensure the ease of this transition, laptops brought to the Hammer 2nd Floor IT Help Desk before February 1 2013, will be encrypted free of charge. Thereafter, depending upon the effort involved, CUMC IT may levy a service charge. NOTICE - encryption services will only be performed on laptops that have been backed up. Laptops that need to be backed up can be left at the Help Desk for that service.

Discovery: Beginning January 1 2013, CUMC IT will conduct floor-by-floor discovery sweeps of all CUMC physical locations. This includes the 168th Street campus as well as remote locations, including medical practices.

Encryption: Beginning February 1 2013, CUMC IT will return to the departments that have undergone asset discovery and install encryption software on all endpoint devices that contain PHI or PII that are not already properly encrypted.

Enhanced System Discovery: Beginning February 1 2013, CUMC IT will be enhancing the discovery techniques available to further identify all assets on the CUMC network. We will conduct a robust institutional asset inventory.

Links to Policies and Other Documentation:

https://secure.cumc.columbia.edu/cumcit/secure/security/hipaa.html
- Email policy
- Workstation use and security
- Information security for backup devices and media controls

www.cumc.columbia.edu/hipaa
- Sanctions policy