DATE: October 29, 2009

FROM: Privacy and Information Security Office, CUMC

SUBJECT: *New notification requirements for loss or theft of patient data (Security Breach) under ARRA/HITECH Act*

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA) of 2009, has established new notification requirements to report the loss or theft of patient information (Protected Health Information – PHI) that is not protected by encryption. These requirements apply in both the clinical and research context. Examples of such security breaches include compromise of unprotected PHI through (1) Lost or stolen laptops, USB drives, CD/DVD/Zip drives, etc. with stored data; (2) A compromised account which is used to look up data, /e.g./, if it appears that someone other than the owner of the account has access to the account; (3) A compromised workstation or server that contains data; (4) Accidental disclosure of data to unauthorized recipients, /e.g./, accidentally sending an email containing data to an incorrect recipient; etc. Please note the following:

1. Columbia University Medical Center (CUMC) faculty, researchers, employees, students, and general users of CUMC patient data are required to ***immediately report any security breach*** to their supervisor and to CUMC Privacy and Information Security Officers (*/hipaa@columbia.edu/*), who will notify the University Response Team (URT). In addition, any lost or stolen equipment or devices should also be reported to Public Safety.

2. CUMC Information Security Policies require that all portable data files stored on USB, CD/DVD, and mobile laptops that include PHI be ***encrypted*** */and/* ***password-protected*** at all times.

3. All electronic transmission of patient information over the Internet must be ***encrypted***. This includes email, file transfers and other data transfer modalities.

4. Any organization that receives, stores or processes PHI on behalf of CUMC must have a ***Business Associate Agreement*** in place for protection of PHI. This means that users cannot forward their institutional email to an external account such as Gmail, Yahoo mail, etc. or use Google Docs to have PHI stored in external organizational storage, whether it is done intentionally or accidentally.

The financial cost of a data breach includes fines and penalties by the Government, the cost of notifying each individual and possibly offering free credit monitoring to each individual that is affected by a loss of data. In addition, CUMC is required to notify the Government of this loss and it will post this information on a public website. CUMC may also be required to notify media about the data loss. Finally, the individual responsible for the loss of data can be held accountable by the Government if he/she failed to follow the organizations policies and procedures.

Our recommendation on Folder, Disk and USB Encryption appears on CUMC IT web site at http://www.cumc.columbia.edu/it/about/security/encryption.html. If you have other questions, please email /*hipaa@columbia.edu*/.