WASHINGTON UNIVERSITY DEPARTMENT OF MEDICINE
USE OF CAMERAS FOR PATIENT INTERACTIONS

Statement of Policy

The Department of Medicine is committed to safeguarding the privacy of our patients and their families in compliance with all applicable laws, regulations and WU policies. Due to the nature of the Department of Medicine and its educational mission, we have adopted a policy for handling the use of camera and any electronic media during patient interactions.

All Washington University Department of Medicine physicians and staff are required to do the following:

- Providers and all medical personnel are to minimize the potential risk of exposure of protected health information (PHI) by downloading pictures or images from a camera or other device onto a secure network supported by IMCSS at least once per week.

- Encryption is required for all laptops and portable devices that may be used to store or access PHI. Portable devices may include, but are not limited to the following: laptops, tablets, external hard drives, flash drives/memory sticks, and CD/DVDs.

- If a mobile phone that receives emails from your DOM email system is lost or misplaced, the phone must be wiped immediately. Please contact the IMCSS Help Desk (314) 362-2165. IMCSS needs to wipe the phone first before you call the service provider to cancel the service. The service provider cannot wipe the data that is stored on the phone if they do not have the device.

- Once images are downloaded, providers are required to delete the material from the original source (camera, CD/DVD, flashdrive/flash drive, etc.).

- Cameras must be stored behind 2-keys (locked cabinet in locked suite) at the end of each use.

- Collection of identifiers on the pictures should be limited to indirect identifiers, such as dates of service, zip codes, patient’s initials or abbreviations. Providers should never take pictures of patient demographic face sheets, wrist bands or documents originating from the patient health record. We ask providers to avoid taking photographic images of medical monitors, which may include identifiers. For example, a heart monitor with the name of the patient included in the picture.

- Full face photographic images should be avoided unless there is a true educational purpose and the patient is aware of the potential risks and a proper consent form is completed.

- This policy applies to photos taken in the outpatient setting. The BJH policy for photos taken in the inpatient setting is attached.

The Department of Medicine will share this policy with their providers during their initial orientation process, as well as regular communication of WUSM HIPAA policies (including this one).

Draft as of February 27, 2013