Photography / Videography for Clinical, Research & Teaching Purposes Policy

Approved: November 14, 2013

PURPOSE: The Washington University School of Medicine and its physicians and health professionals recognize the need to utilize photography and videography for clinical, research, and teaching purposes. At times, these images may include identifiable patient information which must be protected in accordance with applicable University policy and state and federal laws. This policy outlines the permissible purposes for obtaining digital photographs, video images and/or recordings of patients created using cameras, videography devices or other devices in WUSM clinical settings and the standards for the use, storage, and retention of the images.

POLICY:

- **Photography/Videography of Patients is Permissible:**
  - Without specific written authorization
    - For the purposes of patient identification
    - For patient care and treatment (and to document the same). This also includes patient care activities related to patient safety, care coordination, and treatment planning.
    - For Educational or Teaching Purposes – only if the image/video is completely de-identified
  - Only with specific written authorization
    - For use in Clinical Research (requires IRB approval and explicit consent to photography/videography in patient’s informed consent)
    - For Educational or Teaching Purposes – written consent to use identifiable images such as full facial photos must be obtained

  Patient identifiers, if required, should be kept to the minimum necessary and in no case should a social security number be used as an identifier. When possible, limit identifiers to procedure and/or date of service.

- **Photography/Videography Equipment – Administrative and Physical Security and Safeguards:**
  - Devices such as digital cameras used solely for photography/videography must be stored securely, in a locked cabinet or drawer in a locked office or suite. Faculty and staff using such devices are responsible for ensuring the device is secured appropriately during use and at the end of business each day.
• For other portable devices such as laptops, tablets, iPads, smart phones, external hard drives, flash drives/memory sticks, and CD/DVDs that may be used to record, store or access images, Encryption in accordance with the WUSM’s Encryption Policy is required.

• Images from all devices that store photos/videos must be promptly uploaded from the device to the patient’s medical record or a secure folder on the network drive and then wiped from the device as soon as possible and in no case more than one week from the time the image was taken. Each location where these devices are used should have designated individuals who are responsible for removing the images from the device.

**Storage and Retention of Images and/or Recordings:**

• Images taken as a part of treatment are to be promptly uploaded into the patient’s electronic medical record or a secure folder on the network, and deleted from the device. If unique circumstances exist (such as with certain radiology equipment or medical devices that retain images) alternate security measures must be implemented and agreed to by the HIPAA Privacy Officer and/or Information Security Officer to ensure the security and confidentiality of the images.

• Images containing patient information taken for research purposes will become a part of the research record, and if they are stored electronically, they must be stored in a secure file on a secure network supported by WUSM.

• Identifiable images taken for educational purposes must be stored in a secure file on a secure network supported by WUSM.

In the event that a device is lost or stolen, please notify the HIPAA Privacy Office immediately. If images are on the device, the loss or theft will be handled in accordance with the University’s Breach Notification Policy.

Workforce members who fail to comply with this policy are subject to disciplinary action in accordance with the Sanctions for Non-Compliance with HIPAA Policy.