“Social Media/Networking”

VUMC faculty and staff can be held accountable for inappropriate social media conduct. All faculty and staff who identify themselves with VUMC and/or use their Vanderbilt email address in social media venues such as professional society blogs, LinkedIn, Facebook, or Twitter, for deliberate professional engagement or casual conversation are to follow the VUMC Credo Behaviors, Health Insurance Portability and Accountability Act (HIPAA), Conflict of Interest Policy, privacy policies and general etiquette.

Healthcare providers are prohibited from disclosing patient information without proper patient authorization. HIPAA limits the use of information that identifies a patient, including photos. A healthcare provider who discloses patient information through social media without patient authorization is in violation of HIPAA and/or state privacy laws and can be subject to fines and other penalties.

- The ability for smart phones to record images and location via the camera and GPS features pose a significant risk to patient privacy and safety. Pokémon Go renders the creatures on top of live environments using the device’s camera and should never be played in any area treating/processing patients. While the game could photograph patient records or other protected health information (PHI), simply capturing a patient’s name or face in the image could lead to a violation.
- Do not post digital images and messages containing protected health information (PHI) without written authorization from the patient. Remember facial images, recognizable markings or body parts may be PHI (i.e.: tattoos).
- Known or suspected incidents involving use or disclosure of VUMC patient PHI or Personal Information through social networking are reported to the VUMC Privacy Office and are investigated as potential HIPAA violations.
- Federal law and regulations require breach notification and reporting when a patient’s health information is accessed, used or disclosed in a way that violates the Privacy Rule of HIPAA.

Did you know?
- Protected health information (PHI) is protected as long as VUMC Retains the Patient Records or 50 years after a patient is deceased. This includes digital images and messages containing PHI without written authorization from the patient. Remember facial photos, recognizable markings or body parts are PHI.
- Facebook: The new privacy settings allow anyone to view your photos even when your settings are at the strongest level.
- Privacy office investigations: Once an investigation commences, staff members may be held accountable for all violations regardless of posting date.
- It is NOT recommended to accept or request friend requests of patients or their families.

Failure to abide by VUMC’s policies may lead to disciplinary action, up to and including termination

OP 10-10.30 Social Media
IM 10-30.12 Sanctions for Privacy and Information Security Violations
IM 10-30.02 Breach Notification: Unauthorized Access, Use, or Disclosure of Individually Identifiable Patient or Other Personal Information
HR-025 Electronic Communications and Information Technology Resources
Computing Privileges and Responsibilities: Acceptable Use Policy

For more information go to: www.mc.vanderbilt.edu/privacy or e-mail the Privacy Office at privacy.office@vanderbilt.edu

Created by the VUMC Privacy Office (936-3594) Last Revised: 7/26/2016