Protecting Health Information

The patient portal, My Health at Vanderbilt, is the preferred mode of electronic communication between VUMC clinical staff/faculty and a specific patient. Faxing information to a patient is discouraged, but if you must send information by fax you need to know the following:

Faxing Confidential Information:

- VUMC staff should take reasonable and appropriate precautions when using fax machines to transmit confidential documents or when auto-faxing directly from an electronic system or application (e.g., using the StarPanel fax database).
- Staff should use the confirmed database to access fax numbers or confirm with the intended recipient a specific fax number before faxing any protected health information.
- The Provider Communication Wizard contains an accurate provider database and is the preferred mode for faxing patient information to and between providers.
- Before responding to a fax request to an outside individual, the fax number must be confirmed as the correct fax number by the individual making the request.
- Configure your fax machine to generate a confirmation report, if your fax machine has this option.
- Faxing of confidential information must include a cover sheet with the following:
  - Sender Name
  - Recipient Name
  - Sender Business Phone#
  - Recipient Business Phone#
  - Sender Business Fax#
  - Recipient Business Fax#
  - Transmission time and date (if not stamped by fax or computer)
  - Total number of pages (including cover sheet)
  - Confidentiality Statement:
    - See policy: Faxing Confidential Information

Social Media:

All faculty and staff who identify themselves with VUMC and/or use their Vanderbilt email address in social media venues 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.

- If you identify yourself in any online forum as a faculty/staff member of VUMC, you must make it clear you are not speaking for VUMC and all submissions represent your own personal views and comments.
- Do Not post digital images (photos) and messages containing PHI without written authorization from the patient. Remember recognizable markings or body parts are PHI.
- Remember that all content contributed on all platforms becomes immediately searchable and can be immediately shared…it immediately leaves your control forever.

Locking and Logging Off Workstations:

Staff or faculty member logs onto electronic workstations in a shared work area or an area with no patients and leaves the device allowing others to access patient information under the user identification first used:

- Workstations must be secured by locking the screen or logging off whenever the user walks away. Failure to lock the computer screen may result in others using the system under someone else’s user identification which is a data integrity concern.
- If you fail to log off a computer or lock the screen and someone else uses the computer under your user identification, you may be held accountable for any activity that results in unauthorized access to a patient’s record or inappropriate use of the Internet.

IM 10-10.03 Faxing Confidential Information
OP 10-10.30 Social Media
Vanderbilt University Medical Center - Confidentiality Agreement
IM 10-30.12 Sanctions for Privacy and Information Security Violations

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: 10/28/2016