MEDICAL CENTER INFORMATION

SYSTEMS ACCESS AND CONFIDENTIALITY

Adherence to the highest standards of professionalism and to the Vanderbilt University Medical Center (VUMC) information privacy and security policies is expected in the use of the electronic medical record. Maintaining and protecting the accuracy, integrity, and confidentiality of patient information entrusted to VUMC clinicians is of paramount importance to safeguard patient safety, to provide high quality care supported by evidence-based decision support, and to minimize institutional risk associated with billing and regulatory compliance. Failure to preserve the integrity of the unique user identification associated with each individual granted access for use of the clinical information systems undermines the integrity of the clinical documentation and communication, as well as the privacy and confidentiality of the patient information.

It is recognized that technology solutions must be evaluated and implemented to facilitate the user sign-on process in busy clinical settings. However, commitment to the integrity of the unique user identification must not be compromised in the interim.

Employee user IDs and passwords are equivalent to signatures. Employees should NEVER share passwords with others and never use or work under another person's ID/password. Users should always log off or lock their computer screens anytime that they walk away from a computer. This practice helps ensure others do not use the computer under the wrong user ID and see confidential information they may not be authorized to access. Employees are accountable for any action taken under their user IDs and passwords.

Clinicians may only access information related to the treatment of patients with whom they have a clinical relationship, for which they have been asked to provide a consultation, or whose records the clinician has written permission from the patient to access. **Personnel are not authorized to monitor trackboards (e.g., Emergency Department, operating rooms, and procedural areas) or other reports within the electronic medical record or other clinical applications without a specific clinical need.** Personnel are not authorized to access the medical record of co-workers, friends, or family members without written authorization (Communication with Family and Others form) from the patient unless they are directly involved in the care of that patient under the supervision of a member of the VUMC medical staff. This includes minor children's Electronic Medical Records (EMR). Please refer to https://powerdms.com/link/VanderbiltUMC/document/?id=2368640.

Every keystroke made within the electronic medical record is logged by the system. Electronic audit trails of accesses to patient information are conducted and maintained. These audit trails record the machine name, user, date, time, user action within the system, and patient identification.

Whenever a user prints a document containing patient information, it should always be placed in a shredder bin when finished. Users should never throw patient information away in a regular trash can. Users should maintain appropriate confidentiality of papers listing patient identifiable information that they possess, as the papers can easily be left in a conference room or other area utilized by non-authorized individuals, thereby putting privacy and confidentiality of the information at risk.

One of the VUMC Credo Behaviors is: "**I respect privacy and confidentiality**". Information that is obtained about a patient is strictly confidential and is legally protected from disclosure. It may be given to another employee or health care provider only when it is necessary to do so for the following reasons: (1) for the continuity of care, (2) in certain situations when required by law, or (3) when otherwise authorized by the patient. It must never be discussed with any other unauthorized person. Divulging such confidential information or any other departmental information deemed and explained by the department chair as confidential may result in disciplinary action. **HIPAA is a Federal Law and violations are FELONIES and can be tried in Federal Court, resulting in fines or potential imprisonment.**

You should assume that all information that you access, use, or disclose – in any form, verbal, electronic or physical – about patients or their relatives is subject to the law and must be safeguarded. At a minimum, the following information about a patient or a patient's relatives, employers or household members is considered PHI and must be protected:

Names;

Address, including street, city, county, precinct, zip code, and their equivalent geocodes;

All elements of dates;

Telephone numbers;

Fax numbers;

Email addresses;

Social Security Numbers;

Medical Record Numbers;

Health plan beneficiary numbers;

Account numbers;

Certificate/license numbers;

Vehicle identifiers and serial numbers, including license plate numbers;

Device identifiers and serial numbers;

Web Universal Resource Locators (URLs);

Internet Protocol (IP) address numbers;

Biometric identifiers, including finger and voice prints;

Full face photographic images and any comparable images; and

Any other unique identifying number, characteristic, or code.

De-identified data is to be used for purposes other than treatment, payment, or healthcare operations. This includes photography or recordings used for education and teaching purposes. For more information on de-identification, please see De-Identification of Protected Health Information and Use of a Limited Data Set v.5. The VUMC Patient/Visitor Photography/Recordings and Use of Recording Devices to Capture Patients and Visitors v.4 defines allowable purposes for the use of recording devices to capture or record audio, video, or images of patients or visitors.

Any violation of confidentiality and/or the terms in the **Confidentiality Agreement** may result in disciplinary action, including termination of access to the systems, and disciplinary action in accordance with Section I.V. GRADUATE MEDICAL EDUCATION EVALUATION AND DISCIPLINARY GUIDELINES of the House Staff Manual and applicable VUMC policies.

House Staff can direct questions or concerns about privacy to the Privacy Office at (615) 936-3594 or email: Privacy.Office@vumc.org.