Patient Privacy is Everyone’s Responsibility

**Privacy Office Investigations:** The Privacy Office is responsible for auditing access to electronic medical records and other patient information. This includes reviewing the EVE Report; (Employees reV)ewing (Employees), StarPanel alert reports, and random Audits. The *reason for the pop-up screen* is to inform users that they are accessing a medical record that will trigger an audit alert to the Privacy Office. The VUMC Privacy Office wants Medical Center workforce members, who have access to systems or databases that contain patient information, to keep in mind that access to a patient’s information continues to be closely audited for potential privacy violations. Audits reveal the following: the user’s ID, date and time(s) of access, the IP address and the specific documents that have been viewed. **Confirmed unauthorized access** to a patient’s EMR by workforce members will result in disciplinary action up to and including termination of employment.

*You are about to retrieve an electronic medical record that will be monitored for unauthorized access.*

*A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment.*

**Please designate your reason for access to this record:**

- I am accessing this EMR to provide patient care.
- I am accessing this EMR in support of financial services (Billing, Coding, etc.).
- I am accessing this EMR for administrative reasons (IT, Quality Review, Research, Teaching, Training, etc.).
- I am accessing this EMR for other reasons. My reason is described in the Comments below.

**Privacy Office Investigations include (but are not limited to):**

- **Accessing & viewing the EMR for reasons other than job related reasons;**
  - Accessing the EMR of a co-worker or other patient out of curiosity, concern or other unauthorized reason.
- **Accessing clinical/registration/appointment (EPIC/MEDIPAC) systems;**
  - Looking up an address or phone number of a sick co-worker/friend to send a get well card or to call her.
  - Looking up identification information about a patient out of curiosity or for a personal, non-work related reason.
  - Checking to see if an employee really has a doctor’s appointment to verify their FMLA or other purposes.
  - Checking to get a room number or clinic location of a co-worker/friend or another patient.

**Violations for Unauthorized access to patients’ EMR are considered Level 3 and Level 4 violations. These violations will result in a written warning, final warning or termination of employment.**

**Federal Government enforcement of HIPAA has stepped up significantly over the past year:**

- **Civil monetary penalties (paying a fine) for a HIPAA breach, which are from $100 up to $50,000 per incident.**
- **Criminal penalties may also apply in some circumstances and may lead to imprisonment.**

Information Management Policy, 10-30.12 “Sanctions for Privacy and Information Security Violations”

For more information go to: [www.mc.vanderbilt.edu/privacy](http://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: 12/30/2015