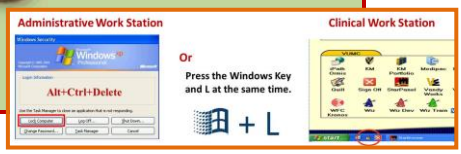
Privacy Buzz

FEBRUARY 2016



Locking and Logging Off Workstations!!!

Walking away from your computer without locking or logging off is a violation. Walking away and leaving a computer unlocked which allows someone to access Protected Health Information (PHI) or Personal information under your user ID is a ***serious*** violation.

This is what can happen:

Scenario:	You are working in StarPanel and you have a patient medical record on the screen. You leave for a meeting but you do not lock or log off your computer. After all you will only be gone for a short time.
Problem #1:	Your co-worker's neighbor has been admitted to VUMC and the co-worker is curious about the neighbor's condition. The co-worker types the neighbor's name into StarPanel (***remember you forgot to logout***) and reviews numerous documents
Problem #2:	Your co-worker's neighbor calls the Privacy Office to request an audit of their medical record looking for access by your co-worker because in conversation with your co-worker they seemed to know more than they should as to why the neighbor was in the hospital.
Problem #3:	The Privacy Office completes the audit and does not find access by your co-worker but does find access by you. Access to numerous reports, and patient demographic information (full name, date of birth, address, phone number, insurance information, and social security number). The Privacy Office notes this is the department the co-worker's neighbor provided. The Privacy Office will request for you to be interviewed and explain your access.
Problem #4:	In the interview with your (Manager/Director) regarding access to the patient record, you have no clue who this patient is and they have not been seen in the clinic where you work. You know you did not access this patient's record. You state maybe you walked away from your computer and someone else accessed the EMR and reviewed the documents.
Problem #5:	This incident could be a Level 3 and even possibly a Level 4 violation of the Sanctions for Privacy and Information Security Policy. A conference call with the Breach Response Team (BRT) will have to be completed. The BRT consist of the Privacy Office, Office of General Counsel, Human Resources, Patient Relations, Risk and Insurance Management, IT Security and your Manager/Director to determine the next steps and the potential disciplinary action that will affect ***you***.
Problem #6:	Because ***you*** failed to lock or log off your computer a patient's PHI has been compromised. The Privacy Office must now write a Breach Notification Letter to the patient detailing what happened and how we will ensure this doesn't happen again. A report of the incident will go to the Health and Human Services (HHS) Secretary. If a Social Security Number is involved then your department will pay for at least 1 year of free credit monitoring for the affected patient.
Conclusion:	***You*** have violated the Sanctions for Privacy and Information Security Policy, the Confidentiality Agreement and now have been Sanctioned with a disciplinary action in your employee record or possibly terminated from your position.

Reference: Confidentiality Agreement
Reference: VUMC Policy IM 10-30.12 *Sanctions for Privacy and Information Security*
Reference: VUMC Policy IM 10-30.02 Breach Notification: Unauthorized Access, Use, or Disclosure of Individually Identifiable Patient or Other Personal Information
Reference: VUMC Policy IM 10-30.13 Protection and Security of Protected Health Information