Guidance: Snooping

SNOOPING

WHAT IS SNOOPING?

Snooping is when a workforce member accesses the record of a patient for a non-job related reason, whether or not the access was malicious or out of good will. It is the inappropriate access to patient records by a UCM employee, irrespective of whether those records are in paper or electronic format and regardless to whether the information acquired was used or disclosed for any reason. For example, if a UCM employee sees that their neighbor has come to the clinic and access's the neighbor's record to view why they are visiting the clinic, this is considered snooping. Another example would be accessing medical records of a celebrity, politician, anyone else of media interest, friends, family members and of course co-workers when there is not a work related reason.

Once an employee accesses a record that does not pertain to their work responsibilities then that access is considered snooping, even if the employee does not use the information. When accessing a record for a work related reason, employees must follow the minimum necessary standard. This means limiting access, use, disclosure or requests for protected health information to the smallest amount required to accomplish a purpose and that the information is shared only with those who have a need to know. For example, if an employee is scheduling an appointment with a patient's primary care physician then there may likely not be a need for that employee to access the patient's OB/GYN records to do their job. In this instance, the access of the OB/GYN records would not have been related to that employee's work responsibilities because the employee was supposed to only schedule the patient for their primary care visit.

Employees who leave their workstations without logging off are responsible if another employee uses their login and password to access medical records. When you step away from your workstation you should always lock your computer screen or log off to prevent unauthorized accesses that could occur under your credentials.

WHAT ARE THE CONSEQUENCES OF SNOOPING?

Absent very unusual circumstances, the penalty for snooping is termination.

This **zero-tolerance** applies to:

- Records of your spouse or domestic partner
- Records of your siblings
- Records of your children or grandchildren
- Records of co-workers
- Records of friends and neighbors
- Records of persons of media interest

Guidance: Snooping

Privacy Program Medical Record Audits

The Privacy Program audits patient medical records to determine potential for snooping. UCM utilizes an electronic tool which proactively monitors and audits for internal threats. This tool utilizes human resource, medical record, operational, and clinical data, and to identify what patient information is accessed and why that access occurred. The Department of Health and Human Services, Office for Civil Rights, requires that UCM as a HIPAA covered entity deter inappropriate access, use, and/or disclosure of protected health information through an audit program.

To help maintain patient privacy and confidentiality, follow these guidelines:

- Access patient medical records only when it is required for your job.
- Do not access medical records of co-workers, friends, family members or celebrities unless there is a job related reason.
- Remember the minimum necessary standard: only access, use and disclose the minimum necessary amount of patient protected health information to get the job done.
    - More information can be found in the HIPAA Privacy Policy: A05-31 – Minimum Necessary Requirements Policy
- Log off/lock your computer whenever you leave your workspace.

FAQ

Can I access my family member's, friend's, or co-worker's Medical Information (e.g. electronic, written)?

Employees may not access the medical record of family members, friends, or other individuals for personal or other non-work related purposes, even if written or oral patient authorization has been given by the patient. If your friend/family member/co-worker is a patient, treat him/her just like any other patient.

- If you are directly involved in the friend/family member/co-worker's treatment or care (e.g. physician, nurse):
    - Only access protected health information (PHI) related to the reason why you are involved in their care
    - Only share PHI with the treatment team
    - Do not share the information, including the fact that the friend/family member/co-worker is a patient, with anyone else who does not need to know for a work related reason

- If you are not directly involved in the friend/family member/co-worker's treatment or care:
  - Do not share information you may incidental knowledge of (e.g. room location, diagnosis) with any other individuals - including your family, friends, and co-workers
  - Do not access the patient's health information - even out of concern
  - Do not stop by to visit the patient without first checking at the nurses' station to confirm that the patient approves your visit
  - Do not ask individuals involved in the patient's care for information

WHAT IF MY CHILD OR PARENT IS A PATIENT HERE?

UCMC must first confirm and document that a person is designated as the patient's personal representative prior to any patient information being disclosed. More information can be found in the HIPAA Privacy Policy: A05-30 Personal Representatives of Patients Policy

WHAT IF I AM INVOLVED IN THE TREATMENT, BILLING OR OTHER ACTIVITY OF A PERSON WHO I KNOW?

In the circumstance when an employee's job (e.g. billing, providing treatment) requires him/her to access and/or copy the medical information of a family member, a co-worker, or other personally known individual, then the employee should immediately report the situation to his/her supervisor who will determine whether to assign a different employee to complete the task involving the specific patient

WHAT IF I AM NOT SURE IF I AM ALLOWED TO GO INTO A PATIENT'S MEDICAL RECORD?

If you have any doubts or concerns about whether you should access a patient's medical record, please contact the Privacy Program Office at 773-834-9716.

Guidance: Snooping

CAN I ACCESS MY OWN MEDICAL RECORD?

UCMC Administrative Policy A02-02, Release of Patient Medical Information and Emergency Release, gives faculty and staff permission to access, view, and print their own electronic medical records if they already have work-related access to our medical record systems. Faculty or staff who access their own record may not edit, add or make changes to any of their information; including but not limited to entering, adding or deleting demographic/registration information, scheduling, changing, cancelling, or checking in/out appointments and/or entering any notations within the health record. When accessing your own medical record, select the reason "My Health Information" when prompted by 'Break-the-Glass (BTG)'. If you do not encounter BTG on your record, contact the Privacy Program at 773-834-9716. **This access is strictly limited to the employee's own health information**.

Any questions/comments/concerns please feel free to reach out to the Privacy Program at:

773-834-9716 or hpo@bsd.uchicago.edu