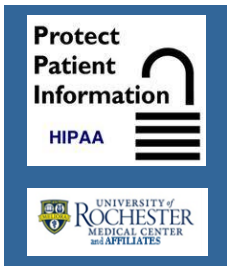
HIPAA HIGHLIGHTS



June 2021

Snooping: Curiosity Has a Cost

Snooping is when a workforce member uses access to patient information for reasons not related to his or her job for any reason, well-intended or not. A common motivation for snooping is personal interest. At its worst, snooping can be maliciously motivated, as in a domestic dispute or an attempt to commit medical or financial identity theft.

Below are a sampling of medical record snooping headlines just since the beginning of 2021.

- Former Mayo physician charged with inappropriately accessing patient medical records
- Bethesda Hospital employee fired for alleged EHR snooping, altering patient health order
- Montefiore fires employee who snooped EHRs for over 1 year
- Alaska hospital notifies patients of employee EHR snooping
- Former Froedtert Health employee wrongfully viewed 760 patient records, health system says
- Former Iowa hospital employee sentenced for 'weaponizing' patient's medical info

Patients put their trust in URMC & Affiliates to protect their privacy. They justifiably expect that their medical records will only be accessed by our staff for a job-related reason and that their information won't be inappropriately shared with others. Good intentions don't justify snooping.

If accessing a patient's record is not required by your job function, the access is not allowed.

There are many consequences for snooping. Per URMC & Affiliates policy and HIPAA, patients may need to be told of the disclosure and staff may receive disciplinary action. Before you snoop, consider this:

Audits

The Privacy Office audits patient medical records for potential inappropriate access, including snooping. eRecord logs every employee who accesses a record and their actions – your "electronic footprints" can be traced through your login. Inappropriate access can also be identified through a complaint from a patient (e.g. who hears something about his condition directly or indirectly from an employee who is not on his care team) or through "whistleblower" calls from workforce members (e.g. who hear a colleague talking about the details of a celebrity patient's medical condition). The Privacy Office investigates each report through audits and/or employee interviews.

Sanctions

Snooping in the patient record could terminate your employment or result in the loss of privileges. There have been cases where employees lost their job due to snooping, both with and without bad intent. Sanctions, per URMC & Affiliates HIPAA Policy 05, range from re-education to more severe outcomes, including notifying legal or regulatory authorities depending on the circumstances.

Your reputation and your colleagues' trust in you are also at risk with snooping.

Notifying the Patient

Snooping is a HIPAA privacy breach. When an unauthorized access or disclosure occurs, the Privacy Office will determine whether the patient needs to be notified per HIPAA Policy 31. Corrective actions taken with the employee are explained to the patient in an effort to restore the patient's trust.

Considering all of the above, is it worth it? **Snooping is never the answer!** If there's a need for a patient's family members to have access to patient care information, consider alternatives such as the MyChart proxy.

Your Privacy Officer and HIPAA Security Official are available to answer questions about HIPAA, or you may refer to URMC's HIPAA Intranet site.